Roberto Conti
1942

LUIGI BIANCHI

LEZIONI SULLA TEORIA DELLE FUNZIONI DI VARIABILE COMPLESSA

E DELLE

FUNZIONI ELLITTICHE

PARTE SECONDA

FUNZIONI ELLITTICHE

TERZA EDIZIONE

BOLOGNA

NICOLA ZANICHELLI

EDITORE

Firenze - Tipografia Ariani - VII-1930

PARTE SECONDA

TEORIA DELLE FUNZIONI ELLITTICHE

CAPITOLO IX.

Le funzioni fondamentali σu, $\wp u$ di Weierstrass. — Le funzioni generali ellittiche espresse per la σu. — Equazione differenziale per la $\wp u$: $\wp'^2 u = 4\,\wp^3 u - g_2\,\wp u - g_3$.

§ 93. — Cenni storici.

Un problema di calcolo integrale ha dato origine alla teoria delle funzioni ellittiche. Denoti $f(x, y)$ una funzione razionale dei due argomenti x, y e si consideri l' integrale (Abeliano)

$$\int f(x, \sqrt{P(x)})\, dx, \tag{1}$$

dove $P(x)$ è un polinomio razionale intero in x. Se $P(x)$ è di primo o secondo grado, con note sostituzioni si riporta questa quadratura a quella di una funzione razionale di una variabile ausiliaria e l' integrale stesso si esprime per ordinarie funzioni, algebriche e logaritmiche. Ma appena $P(x)$ supera il secondo grado, diventa, *in generale*, impossibile una simile riduzione e la funzione di x che nasce dall' integrazione rappresenta *una nuova trascendente*, non riducibile alle trascendenti ordinarie. Se in particolare il polinomio $P(x)$ è di terzo o quarto grado, l' integrale (1) dicesi un *integrale ellittico*. Quando il polinomio è di grado superiore al quarto, si hanno gli integrali *iperellittici* (§ 91). La denominazione di integrale ellittico ha un'origine geometrica, perchè appunto per un integrale di questa specie si esprime la lunghezza di un arco di ellisse.

Una fondamentale scoperta nella teoria degli integrali ellittici è dovuta ad *Eulero*, che trovò il così detto *teorema d'addizione* per gli integrali di 1ª specie, nel quale sono inclusi, come casi particolari, i risultati già prima trovati da *Fagnani* sugli archi di lemniscata di Bernoulli.

Ma Legendre fu il primo che costruì sistematicamente la teoria, classificando e riducendo a tre specie essenziali distinte gli integrali ellittici. Egli studiò le proprietà di queste nuove trascendenti, cui diede il nome di funzioni ellittiche, oggidì riserbato ad altre specie di funzioni che nascono, come ora diremo, da un problema d' inversione.

Le geniali ricerche di Abel e di Jacobi cangiarono totalmente l'aspetto della teoria di Legendre ed arricchirono l'analisi di nuove ed importanti conquiste.

Due sono le principali idee che guidarono Abel e Jacobi nelle loro scoperte. L' una consiste nell'estendere la considerazione dei nuovi enti analitici ai valori complessi delle variabili, l'altra nel sostituire allo studio diretto degli integrali ellittici quello delle funzioni che nascono dall' inversione degli integrali stessi (di 1ª specie). S' intenderà facilmente l' importanza del *principio d' inversione*, ove si consideri, con Jacobi, in qual modo la teoria delle funzioni circolari, se già non fosse stata prima nota, si sarebbe introdotta in un problema analogo di calcolo integrale. Si consideri l' integrale

$$y = \int_0^x \frac{dx}{\sqrt{1 - x^2}},$$

che porta alla funzione circolare inversa arc sen x. Seguendo il metodo di Legendre, dovremmo qui studiare la y come funzione della x. Ma ben più semplici ed importanti sono, come sappiamo, le proprietà della *funzione inversa*: $x = \operatorname{sen} y$; e la ragione principale sta in ciò che mentre y considerata come funzione della x è infinitiforme, la inversa $x = \operatorname{sen} y$ è invece una funzione *uniforme* e periodica del suo argomento.

Analogamente si consideri l' integrale ellittico di 1ª specie della forma normale di Legendre:

$$y = \int_0^x \frac{dx}{\sqrt{(1 - x^2)(1 - k^2 x^2)}},$$

essendo k una costante (modulo), e in luogo di considerare y come funzione di x, si consideri il limite superiore x dell' integrale come funzione del valore y dell' integrale stesso. Servendoci delle nozioni acquistate nello studio generale delle funzioni di variabile complessa, possiamo esprimere il risultato fondamentale di Abel, Jacobi, dicendo che la funzione x di y così definita è uniforme in tutto il piano y, con sole singolarità polari, e partecipando ad un tempo della natura delle funzioni circolari ed esponenziali, possiede una *doppia periodicità*. È questa la prima funzione ellittica di Jacobi, da lui indicata col simbolo

$$\text{sen am } y \text{ (seno amplitudine).}$$

Della medesima natura sono le due altre funzioni ellittiche di Jacobi

$$\cos \text{am } y = \sqrt{1 - \text{sen am}^2 y} \quad \text{(coseno amplitudine)}$$

$$\Delta \text{ am } y = \sqrt{1 - k^2 \text{ sen am}^2 y} \quad \text{(delta amplitudine).}$$

Oggi si indicano più brevemente queste tre funzioni coi simboli di Gudermann

$$\text{sn } y, \quad \text{cn } y, \quad \text{dn } y.$$

Sotto il nome generale di *funzioni ellittiche* si comprendono ora tutte le funzioni uniformi, con sole singolarità polari, a distanza finita, dotate di una doppia periodicità; le funzioni ottenute per inversione dell'integrale ellittico di 1ª specie ne offrono il primo esempio.

Un'altra idea di Jacobi, di cui si trova traccia anche nelle memorie di Abel, è di capitale importanza per la teoria. Le funzioni ellittiche di Jacobi

$$\text{sn } y, \quad \text{cn } y, \quad \text{dn } y$$

essendo uniformi in tutto il piano, prive di singolarità essenziali, e diventando infinite nei medesimi punti, possono esprimersi (ciò che risulta per noi dal teorema di Weierstrass al Cap. VI, § 66) come quozienti di trascendenti intere, il denominatore essendo nei tre casi il medesimo. Queste trascendenti intere, senza essere doppiamente periodiche, offrono però evidentemente una doppia periodicità rispetto alla distribuzione dei loro infinitesimi. Esse sono le funzioni ϑ (theta) di Jacobi, che si riducono in sostanza ad una sola trascendente, mediante la quale possono esprimersi tutte le funzioni che si incontrano nella teoria delle funzioni e degli integrali ellittici.

Un perfezionamento notevole è stato portato alle teorie di Jacobi da Weierstrass. Alle tre funzioni di Jacobi

$$\text{sn } y, \quad \text{cn } y, \quad \text{dn } y$$

egli ha sostituito un' unica funzione ellittica, che per molti riguardi si comporta più semplicemente. È questa la funzione indicata da Weierstrass col simbolo

$$\wp u$$

e per mezzo di questa e della sua derivata prima $\wp' u$ si possono esprimere razionalmente, come si vedrà, tutte le funzioni ellittiche dell'argomento u (coi medesimi periodi). Così pure alle funzioni ϑ di Jacobi Weierstrass ha sostituito un' unica trascendente intera, la funzione

$$\sigma u,$$

che gode di proprietà analoghe alle ϑ, ma più semplici e simmetriche. La funzione σu è appunto l'elemento col quale si possono esprimere tutte le funzioni e gli integrali ellittici nella teoria di Weierstrass.

Noi ci occuperemo principalmente in questo corso delle funzioni di Weierstrass σu, $\wp u$, senza trascurare lo studio delle funzioni di Jacobi, e particolarmente delle ϑ, che oltre l' importanza storica offrono grande interesse per l'eleganza dei loro sviluppi in serie a rapidissima convergenza. Cominceremo dal costruire la funzione elementare σu e da essa dedurremo tutte le altre.

Questo modo di sviluppare la teoria, che procede in senso inverso all'effettivo sviluppo storico, ha per noi il vantaggio di essere semplice e rapido, senza esigere altre nozioni che quelle della teoria delle funzioni monodrome.

§ 94. — **Costruzione della funzione σu di Weierstrass.**

Nella funzione sen z abbiamo l'esempio di una trascendente intera, i cui infinitesimi sono distribuiti a regolari intervalli sopra una retta (asse reale).

La trascendente intera

$$\text{sen}\left(\frac{\pi z}{2\omega}\right),$$

dove ω è una costante complessa, ha similmente i suoi infinitesimi distribuiti a regolari intervalli sulla retta che unisce l'origine al punto 2ω; essi sono infatti nei punti

$$z_0 = m \cdot 2\omega,$$

percorrendo m tutti i valori interi positivi e negativi.

La trascendente intera

$$\sigma u$$

di Weierstrass, dove ora indichiamo con u la variabile complessa (argomento), ha proprietà simili, ma i suoi infinitesimi hanno una ricorrenza *doppiamente* periodica. Indichiamo con

$$\omega, \quad \omega'$$

due costanti fondamentali complesse e domandiamoci in primo luogo: È possibile costruire una trascendente intera che divenga infinitesima del primo ordine in tutti e soli i punti del piano dati dalla formola

$$u_0 = m\, 2\omega + n\, 2\omega',$$

dove m, n percorrono tutti gli interi positivi o negativi? Osserviamo che, rispetto al gruppo lineare di sostituzioni paraboliche (vol. I, cap. II, § 17):

$$u' = u + 2m\omega + 2n\omega', \tag{2}$$

i punti in questione formano un sistema completo di punti equivalenti all'origine $u_0 = 0$. Le ricerche del citato paragrafo ci portano subito ad escludere il caso in cui il rapporto $\frac{\omega'}{\omega}$ sia reale. E infatti se $\frac{\omega'}{\omega}$ fosse reale commensurabile, i due periodi 2ω, $2\omega'$ sarebbero multipli di un medesimo periodo fondamentale 2Ω e la trascendente domandata non potrebbe differire dalla funzione elementare

$$\operatorname{sen}\left(\frac{\pi u}{2\Omega}\right)$$

che per un fattore esponenziale, caso per noi senza importanza. Se poi $\frac{\omega'}{\omega}$ fosse reale ed incommensurabile, nell' intorno di ogni

infinitesimo della funzione da costruirsi si addenserebbero infiniti altri infinitesimi, ciò che esclude la possibilità dell'esistenza per la funzione richiesta.

Il rapporto $\frac{\omega'}{\omega}$ deve dunque essere una costante complessa

$$\frac{\omega'}{\omega} = \alpha + i\beta, \quad \beta \neq 0,$$

e, siccome possiamo cangiare di segno l' uno o l'altro dei periodi, non alteriamo la generalità supponendo al coefficiente β dell' immaginario un segno determinato. E noi facciamo la convenzione fondamentale per il seguito: *Il coefficiente dell' immaginario nel rapporto dei periodi* $\tau = \frac{\omega'}{\omega}$ *deve essere positivo.*

Questa convenzione induce una conseguenza, che importa subito notare. Costruiamo la rete parallelogrammica (vol. I, § 17, pag. 53) relativa al gruppo (2) di traslazioni situando un vertice in $u_0 = 0$, sicchè i quattro vertici del parallelogrammo fondamentale saranno i punti

$$0, \quad 2\omega, \quad 2\omega + 2\omega', \quad 2\omega'.$$

Il supporre $R\left(\frac{\omega'}{i\omega}\right) > 0$ [1]), come abbiamo fatto, porta che percorrendo il contorno del parallelogrammo nel verso positivo si incontrino, a partire dall'origine, i vertici nell'ordine sopra scritto [2]). La trascendente intera da costruirsi deve avere i suoi infinitesimi, del primo ordine, nei vertici della nostra rete parallelogrammica e poichè le distanze fra questi punti non scendono al disotto del minimo fra i moduli delle quattro quantità 2ω, $2\omega'$, $2\omega + 2\omega'$,

[1]) Col simbolo $R(\Omega)$ indichiamo la parte reale di una quantità complessa Ω.

[2]) Posto infatti $\omega = \varrho e^{i\theta}$, $\omega' = \varrho' e^{i\theta'}$, si ha

$$\frac{\omega'}{\omega} = \frac{\varrho'}{\varrho} \left\{ \cos(\theta' - \theta) + i \operatorname{sen}(\theta' - \theta) \right\}$$

onde

$$\operatorname{sen}(\theta' - \theta) > 0,$$

ciò che dimostra che per un osservatore collocato in 0, che guardi nella direzione da 0 a 2ω, la direzione da 0 a $2\omega'$ resta alla sinistra.

$2\omega - 2\omega'$, il teorema del cap. VI, § 69 (vol. I), ci fornisce subito la trascendente cercata nel doppio prodotto infinito

$$u \mathop{\Pi'}_{m,n}\left(1 - \frac{u}{2m\omega + 2n\omega'}\right) e^{\frac{u}{2m\omega+2n\omega} + \frac{1}{2}\frac{u^2}{(2m\omega+2n\omega')^2}}$$

esteso a tutti i valori interi positivi e negativi di m, n, l'accento nel prodotto infinito indicando che viene esclusa la combinazione $m = 0$, $n = 0$. Questo prodotto infinito, in ogni campo finito, converge indipendentemente dall'ordine dei fattori ed in egual grado e rappresenta, senza alcuna aggiunta di fattore esponenziale esterno $e^{G(u)}$, appunto la funzione σu di Weierstrass. Ponendo per brevità

$$w = 2m\omega + 2n\omega',$$

notazione che conserveremo in seguito, abbiamo dunque per la σu la prima espressione analitica

$$\text{(I)} \qquad \sigma u = u \mathop{\Pi'}_{m,n}\left(1 - \frac{u}{w}\right) . \; e^{\frac{u}{w} + \frac{u^2}{2w^2}} .$$

Questa trascendente intera dipende, oltre che dall'argomento u, anche dalle costanti fondamentali 2ω, $2\omega'$, rispetto alle quali è costruita, che si dicono i *periodi*. Volendo porre in evidenza anche i periodi coi quali la σu è costruita, si scriverà con Weierstrass:

$$\sigma(u \mid \omega, \omega') .$$

§ 95. — **Proprietà fondamentali della σu.**

Una prima proprietà della σu si rileva subito dalla sua espressione analitica (I): *La σu è una funzione dispari, cioè si ha*

$$\text{(3)} \qquad \sigma(-u) = -\sigma u .$$

E infatti dalla (I) si ha

$$\sigma(-u) = -u \mathop{\Pi'}_{m,n}\left(1 + \frac{u}{w}\right) e^{-\frac{u}{w} + \frac{u^2}{2w^2}},$$

e poichè il prodotto infinito non cangia mutando m, n in $-m$, $-n$, cioè w in $-w$, ne risulta subito la formola scritta.

Similmente dalla (I) vediamo subito che si ha

$$\text{(3*)} \qquad \lim_{u=0} \frac{\sigma u}{u} = 1 ,$$

ossia $\sigma' 0 = 1$.

Ancora dalla espressione analitica risulta dimostrata una proprietà di *omogeneità* della σ, espressa dalla formola

$$\text{(4)} \qquad \sigma(\lambda u \mid \lambda\omega, \lambda\omega') = \lambda \sigma(u \mid \omega, \omega') ,$$

dove λ indica un fattore costante arbitrario.

Troviamo un'altra proprietà importantissima della funzione σu, proponendoci la questione seguente:

Possono due funzioni

$$\sigma(u \mid \omega, \omega'), \qquad \sigma(u \mid \Omega, \Omega'),$$

costruite con periodi diversi, coincidere?

Poichè gli infinitesimi della prima debbono essere anche infinitesimi della seconda e viceversa, dovranno ω, ω' esprimersi linearmente ed omogeneamente, con coefficienti interi, per Ω, Ω' e inversamente Ω, Ω' per ω, ω' in modo analogo.

Si dovrà quindi avere

$$\begin{cases} \omega = \alpha\Omega + \beta\Omega' \\ \omega' = \gamma\Omega + \delta\Omega' \end{cases} \qquad \begin{cases} \Omega = \alpha'\omega + \beta'\omega' \\ \Omega' = \gamma'\omega + \delta'\omega' , \end{cases}$$

i coefficienti $\alpha, \beta, \gamma, \delta$; $\alpha', \beta', \gamma', \delta'$ essendo interi. Se sostituiamo nelle prime due formole i valori di Ω, Ω' dati dalle seconde, dobbiamo ottenere delle identità, poichè $\frac{\omega'}{\omega}$ non è reale. Ne deduciamo

$$\begin{cases} \alpha\alpha' + \beta\gamma' = 1, & \alpha\beta' + \beta\delta' = 0 \\ \gamma\alpha' + \delta\gamma' = 0, & \gamma\beta' + \delta\delta' = 1, \end{cases}$$

onde

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \cdot \begin{vmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{vmatrix} = 1 ,$$

e però

$$\alpha\delta - \beta\gamma = \pm 1 \;[1]).$$

L' incertezza del segno si toglie osservando che, per ipotesi, i coefficienti dell' immaginario nei due rapporti

$$\frac{\omega'}{\omega}, \quad \frac{\Omega'}{\Omega},$$

legati dalla relazione lineare

$$\frac{\omega'}{\omega} = \frac{\delta\dfrac{\Omega'}{\Omega} + \gamma}{\beta\dfrac{\Omega'}{\Omega} + \alpha},$$

debbono essere ambedue positivi, il che porta che si abbia

$$\alpha\delta - \beta\gamma = +1.$$

Inversamente, se supponiamo

$$\begin{cases} \omega = \alpha\Omega + \beta\Omega' \\ \omega' = \gamma\Omega + \delta\Omega', \end{cases}$$

con α, β, γ, δ interi e $\alpha\delta - \beta\gamma = 1$, risolvendo avremo

$$\begin{cases} \Omega = \delta\omega - \beta\omega' \\ \Omega' = -\gamma\omega + \alpha\omega', \end{cases}$$

onde gli infinitesimi

$$w = 2m\omega + 2n\omega'$$
$$\overline{w} = 2m\Omega + 2n\Omega'$$

delle due σ coincideranno, salvo l'ordine, e le loro espressioni analitiche (I), a causa della convergenza assoluta del prodotto infinito, coincideranno altresì. Abbiamo dunque il teorema :

Condizione necessaria e sufficiente affinchè due funzioni σ, costruite con diversi periodi :

$$\sigma(u \mid \omega, \omega'), \quad \sigma(u \mid \Omega, \Omega')$$

[1]) Cfr. vol. I, cap. II, § 17, pag. 56 nota.

coincidano, è che i periodi siano legati da relazioni lineari, intere ed omogenee

$$\begin{cases} \omega = \alpha\Omega + \beta\Omega' \\ \omega' = \gamma\Omega + \delta\Omega' \end{cases}$$

a coefficienti interi α, β, γ, δ e a determinante

$$\alpha\delta - \beta\gamma = +1.$$

§ 96. — Le funzioni ζu e $\wp u$ e la doppia periodicità di $\wp u$, $\wp' u$.

Consideriamo la derivata logaritmica della σ, funzione indicata da Weierstrass col simbolo ζu, sicchè

$$\zeta u = \frac{\sigma' u}{\sigma u}. \tag{5}$$

L' espressione analitica della ζu risulta immediatamente dalla (I) per la σu, derivando logaritmicamente, e si ha

$$\zeta u = \frac{1}{u} + \sum_{m,n}{}' \left\{ \frac{1}{u-w} + \frac{1}{w} + \frac{u}{w^2} \right\} \;[1]), \tag{II}$$

le serie del secondo membro essendo convergente in egual grado in ogni campo finito, dal quale siano esclusi i punti

$$u_0 = 2m\omega + 2n\omega',$$

che sono per ζu i punti singolari, e precisamente poli del primo ordine col residuo $+1$.

La funzione ζu è, come la σu, una funzione dispari :

$$(-\zeta u) = -\zeta u.$$

La funzione

$$\wp u$$

di Weierstrass si definisce semplicemente come la derivata della ζu, cangiata di segno :

$$\wp u = -\zeta' = -\frac{d^2 \log \sigma u}{d u^2}. \tag{6}$$

[1]) L'accento nella somma indica l' omissione del termine corrispondente a $m = 0$, $n = 0$.

La $\wp\, u$ è evidentemente una funzione pari, cioè:

$$\wp(-u) = \wp\, u\,. \tag{7}$$

La sua espressione analitica si ottiene per derivazione (vol. I, cap. IV, § 47) dalla (II); risulta così:

$$\wp u = \frac{1}{u^2} + \sum_{m,n}{}' \left\{ \frac{1}{(u - 2m\omega - 2n\omega')^2} - \frac{1}{(2m\omega + 2n\omega')^2} \right\}. \tag{III}$$

Una nuova derivazione ci dà

$$\wp' u = -\frac{2}{u^3} - 2\sum_{m,n}{}' \frac{1}{(u - 2m\omega - 2n\omega')^3}\,,$$

che si può anche scrivere semplicemente

$$\wp' u = -2\sum_{m,n} \frac{1}{(u - 2m\omega - 2n\omega')^3}\,, \tag{IV}$$

attualmente con inclusione del termine corrispondente a $m = 0$, $n = 0$. La convergenza delle serie (III), (IV) è assoluta ed in egual grado in ogni campo finito, esclusi i punti

$$u_0 = 2m\omega + 2n\omega'\,,$$

ove le $\wp\, u$, $\wp'\, u$ diventano rispettivamente infinite del secondo e del terzo ordine coi termini d' infinito

$$\frac{1}{(u - 2m\omega - 2n\omega')^2}\,, \quad \frac{-2}{(u - 2m\omega - 2n\omega')^3}\,.$$

Ma l' espressione (IV) della $\wp'\, u$ pone in evidenza una proprietà di capitale importanza, e cioè la sua *doppia periodicità*. Se cangiamo infatti nella (IV) u in $u + 2\omega$, o in $u + 2\omega'$, i termini della serie non fanno che cangiar di posto e si ha quindi

$$\begin{cases} \wp'(u + 2\omega) = \wp' u \\ \wp'(u + 2\omega') = \wp' u\,, \end{cases}$$

e più in generale naturalmente

$$\wp'(u + 2m\omega + 2n\omega') = \wp' u\,,$$

essendo m, n interi qualunque. Anche la funzione $\wp\, u$ è doppiamente periodica, coi periodi fondamentali 2ω, $2\omega'$, sebbene la cosa non riesca subito evidente dallo sviluppo (III) in serie. Integrando le precedenti (8), si ottiene infatti

$$\wp(u + 2\omega) - \wp\, u = c$$
$$\wp(u + 2\omega') - \wp\, u = c'\,,$$

con c, c' costanti. Ma se in queste facciamo rispettivamente $u = -\omega$, $u = -\omega'$ (osservando che $\wp\,\omega$, $\wp\,\omega'$ non sono infinite) otteniamo subito, a causa della parità della $\wp\, u$:

$$c = 0\,,\ c' = 0$$

e quindi

$$\begin{cases} \wp(u + 2\omega) = \wp\, u \\ \wp(u + 2\omega') = \wp\, u\,. \end{cases} \tag{9}$$

Ne concludiamo: *La funzione $\wp\, u$ e tutte le sue successive derivate*

$$\wp' u\,,\ \wp'' u\,,\ \wp''' u \ldots.$$

sono funzioni uniformi in tutto il piano complesso e sono doppiamente periodiche, coi periodi fondamentali 2ω, $2\omega'$.

I loro punti singolari si trovano unicamente nei punti $u_0 = 2m\omega + 2n\omega'$, vertici della rete parallelogrammica, ove hanno dei poli. Si noti poi che la $\wp\, u$ e tutte le sue derivate d'ordine pari $\wp'' u$, $\wp^{IV} u$, ... sono funzioni pari, mentre le derivate d' ordine dispari $\wp' u$, $\wp''' u$, ... sono tutte funzioni dispari.

§ 97. — Effetto dell'aggiunta di periodi all'argomento di σu.

Vediamo ora come si comporta la funzione σu, quando all' argomento u si aggiunga 2ω o $2\omega'$. Dalle (9) integrando, si ha

$$\begin{cases} \dfrac{\sigma'(u + 2\omega)}{\sigma(u + 2\omega)} = \dfrac{\sigma' u}{\sigma u} + 2\eta \\[2ex] \dfrac{\sigma'(u + 2\omega')}{\sigma(u + 2\omega')} = \dfrac{\sigma' u}{\sigma u} + 2\eta'\,, \end{cases} \tag{10}$$

essendo η, η' due costanti d' integrazione.

Per determinarle si faccia nelle precedenti rispettivamente $u = -\omega$, $u = -\omega'$ e, rammentando che $\dfrac{\sigma' u}{\sigma u} = \zeta u$ è una funzione dispari, si avrà subito

$$\eta = \frac{\sigma'\omega}{\sigma\omega} = \zeta\,\omega\,, \quad \eta' = \frac{\sigma'\omega'}{\sigma\omega'} = \zeta\,\omega'\,. \tag{11}$$

Integrando nuovamente le (10) e passando dai logaritmi ai numeri, deduciamo

$$\begin{cases} \sigma(u+2\omega) = C\,e^{2\eta u}\,\sigma u \\ \sigma(u+2\omega') = C' e^{2\eta' u}\,\sigma u\,, \end{cases}$$

con C, C' nuove costanti, che si determinano subito facendo in queste ultime formole rispettivamente $u = -\omega$, $u = -\omega'$; si trovano così le formole

$$\begin{cases} \sigma(u+2\omega) = -\,e^{2\eta(u+\omega)}\,.\,\sigma u \\ \sigma(u+2\omega') = -\,e^{2\eta'(u+\omega')}\,.\,\sigma u\,. \end{cases} \tag{12}$$

Come si vede, aumentando l'argomento u della σ di un periodo, la funzione si riproduce, moltiplicata per un fattore esponenziale *con esponente di primo grado nella* u [1]).

Le costanti 2η, $2\eta'$ si dicono anche i periodi di *seconda specie*, per distinguerli dai periodi 2ω, $2\omega'$, che si dicono di *prima specie*. Fra i periodi di prima e seconda specie ha luogo l'importante relazione:

$$\eta\,\omega' - \eta'\omega = \frac{\pi i}{2}\ ^{2)}\,, \tag{V}$$

che dimostriamo nel modo seguente.

Consideriamo nel piano complesso u il parallelogrammo $A\,B\,C\,D$ i cui vertici sono nei punti

$$A \equiv -(\omega+\omega'),\quad B \equiv \omega - \omega'\,,\quad C \equiv \omega + \omega'\,,\quad D \equiv -\omega + \omega'.$$

[1]) Che si dovesse riprodurre a meno di un fattore esponenziale, risultava subito dall'osservare che $\sigma\,(u+2\omega)$. $\sigma\,(u+2\omega')$ hanno i medesimi infinitesimi di σu.

[2]) Che debba essere $\eta\,\omega' - \eta'\omega$ un *multiplo* di $\dfrac{\pi i}{2}$ si riconosce anche subito così. Nella prima delle (12) si cangi u in $u+2\omega'$ e nella seconda u in $u+2\omega$ e si paragonino i risultati, che debbono essere eguali.

Sul contorno e nell'interno di esso la funzione $\zeta\,u = \dfrac{\sigma' u}{\sigma u}$ non ha alcuna singolarità, salvo in $u = 0$, ove ha un polo del primo ordine col residuo $+1$; si ha quindi

$$2\pi i = \int_{ABCD} \zeta u \; du\,,$$

l'integrale essendo esteso al contorno nel senso positivo, che è appunto il senso $A\,B\,C\,D$ (cfr. § 94). Possiamo scrivere in altro modo, riunendo le parti dell'integrale estese ai tratti paralleli $A\,B$, $C\,D$; $B\,C$, $D\,A$, e cioè:

$$2\pi i = \int_{AB} \{\,\zeta u - \zeta(u+2\omega')\,\}\,d\,u + \int_{DA} \{\,\zeta u - \zeta(u+2\omega)\,\}\,d\,u\,,$$

onde, per le formole fondamentali (10), essendo

$$\zeta(u+2\omega) = \zeta u + 2\eta\,, \qquad \zeta(u+2\omega') = \zeta u + 2\eta'\,,$$

ricaviamo

$$2\pi i = -\int_{AB} 2\eta'\;d\,u + \int_{AD} 2\eta\;d\,u = 4\,\eta\,\omega' - 4\,\eta'\omega\,,$$

il che dimostra appunto la (V).

Ciò premesso, possiamo dalle (12) dedurre la formola generale che dà l'effetto sulla $\sigma\,u$ dell'aggiunta di un qualsiasi periodo $2\,m\,\omega + 2\,n\,\omega'$ all'argomento u.

Dalla prima delle (12) si ha intanto, per qualunque m intero e positivo, cangiandovi u in $u + 2\,(m-1)\,\omega$

$$\sigma(u+2\,m\,\omega) = -\,e^{2\eta\,[u+2(m-1)\omega+\omega]}\,.\,\sigma(u+2\,(m-1)\,\omega)\,.$$

Cangiando in questa successivamente m in $m-1$, $m-2$, ..., 2, 1 e moltiplicando insieme tutte le formole, otteniamo:

$$\sigma\,(u+2\,m\,\omega) = (-1)^m\,e^{2m\eta(u+m\omega)}\,.\,\sigma\,u\,. \tag{13}$$

Se in questa si cangia u in $u - 2\,m\,\omega$, si ottiene la formola stessa per m negativo. Similmente avremo per qualunque n intero:

$$\sigma(u+2\,n\,\omega') = (-1)^n\,e^{2n\eta'(u+n\omega')}\,.\,\sigma\,u\,. \tag{14}$$

Cangiamo nella (13) u in $u + 2n\omega'$, sostituendo nel secondo membro a $\sigma(u + 2n\omega')$ il valore (14); troveremo

$$\sigma(u + 2m\omega + 2n\omega') = (-1)^{m+n}\, e^{(2m\eta + 2n\eta')(u + m\omega + n\omega') + 2mn(\eta'\omega - \eta\omega')}$$

ovvero per la (V):

$$\text{(VI)}\quad \sigma(u + 2m\omega + 2n\omega') = (-1)^{m+n+mn} \cdot e^{(2m\eta + 2n\eta')(u + m\omega + n\omega')} \cdot \sigma u.$$

È questa la formola generale richiesta.

§ 98 [1]. — Proprietà generali delle funzioni ellittiche.

Nella $\wp u$ e nelle sue derivate abbiamo riconosciuto delle funzioni uniformi in tutto il piano, aventi a distanza finita soltanto singolarità polari e dotate di due periodi indipendenti 2ω, $2\omega'$. In generale, come già si è detto al § 93, si comprendono oggidì sotto il nome di *funzioni ellittiche* tutte le funzioni doppiamente periodiche, con sole singolarità polari a distanza finita. Se chiamiamo 2ω, $2\omega'$ i periodi della funzione, possiamo anche dire che le funzioni ellittiche rimangono invariate eseguendo sull'argomento tutte le sostituzioni lineari del gruppo parabolico

$$u' = u + 2m\omega + 2n\omega'.$$

Esse offrono, dopo le funzioni semplicemente periodiche, il più semplice esempio di quella classe generale di funzioni uniformi nel loro campo d'esistenza che si dicono *automorfe* (*Fuchsiane-Kleiniane* secondo Poincaré) e che godono della proprietà di riprodursi, quando sul loro argomento si eseguiscono le sostituzioni lineari di un gruppo fondamentale. È chiaro, che nel campo di esistenza della funzione, il gruppo deve essere *propriamente discontinuo* (cap. II, § 14). E, per restare al caso nostro speciale, i due periodi 2ω, $2\omega'$ di ogni funzione ellittica debbono essere in rapporto complesso; altrimenti, se fossero indipendenti, nell'intorno di ogni punto del piano si addenserebbero infiniti punti equivalenti, nei quali la funzione ellittica dovrebbe riprendere il medesimo valore, ciò che è incompatibile coll'uniformità della funzione. Si osservi ancora che le nostre ricerche sui gruppi di traslazioni (vol. I, cap. II, § 17) ci assicurano che *non esistono funzioni uniformi con tre o più periodi indipendenti*.

[1] Le proprietà generali delle funzioni ellittiche, che si studiano nel presente paragrafo e nel seguente, non sono che un caso particolare delle proprietà delle funzioni razionali sopra una superficie Riemanniana di cui abbiamo trattato al § 89, e corrispondono precisamente al caso ellittico $p = 1$.

Cominciamo lo studio delle proprietà generali delle funzioni ellittiche colla dimostrazione del seguente teorema:

Ogni funzione ellittica deve ammettere dei poli a distanza finita. In caso contrario infatti, se consideriamo un parallelogrammo fondamentale dei periodi, il cui primo vertice collochiamo in un punto arbitrario a del piano, ivi il modulo della nostra funzione, che sarebbe una trascendente intera, si manterrebbe inferiore ad un numero fisso K e lo stesso avverrebbe quindi, a causa della doppia periodicità, in qualunque campo finito. Il teorema dimostrato al cap. VI, § 59 (vol. I), ci assicura allora che la funzione si ridurrebbe ad una costante.

Da questo teorema seguono due corollari importanti, di continuo uso nella teoria, e cioè:

1° *Se due funzioni ellittiche $f(u)$, $f_1(u)$ coi medesimi periodi 2ω, $2\omega'$ hanno i medesimi punti di infinito e di infinitesimo, coi medesimi ordini, non possono differire che per un fattore costante.*

E infatti il quoziente $\dfrac{f(u)}{f_1(u)}$ sarebbe ancora una funzione ellittica coi periodi 2ω, $2\omega'$ e non diventerebbe più infinito (nè zero), onde sarebbe una costante.

2° *Se due funzioni ellittiche $f(u)$, $f_1(u)$, coi medesimi periodi, hanno a comune i poli e i relativi termini d'infinito, l'una non può differire dall'altra che per una costante additiva.*

E infatti la differenza $f_1(u) - f(u)$ sarebbe doppiamente periodica e senza poli, e perciò una costante.

§ 99. — Ordine di una funzione ellittica e teorema d'Abel.

Sia $f(u)$ una funzione ellittica coi periodi $(2\omega, 2\omega')$ e consideriamo un parallelogrammo fondamentale $ABCD$ dei periodi coi vertici nei punti

$$A \equiv a, \quad B \equiv a + 2\omega, \quad C \equiv a + 2\omega + 2\omega', \quad D \equiv a + 2\omega',$$

essendo a un punto arbitrario del piano, scelto però in guisa che sul contorno $A\,B\,C\,D$ la $(f\,u)$ non divenga infinita, ciò che evidentemente è sempre possibile, gli infiniti di $f(u)$ in un campo finito essendo in numero finito. Allora la $f(u)$ diventerà certamente infinita in qualche punto interno del parallelogrammo e noi vogliamo dimostrare l'importante teorema :

La somma dei residui di una funzione ellittica nell'interno del parallelogrammo dei periodi è nulla.

Questa somma è data infatti da

$$\frac{1}{2\pi i}\int\limits_{ABCD} f(u)\,du\,;$$

e se riuniamo nell'integrale le parti relative ai lati paralleli, ricordando che $f(u+2\,\omega)=f(u)$, $f(u+2\,\omega')=f(u)$, vediamo subito che l'integrale stesso è nullo (cfr. § 97).

Supponiamo ora di più che il parallelogrammo fondamentale dei periodi sia collocato in guisa da non contenere sul contorno nemmeno infinitesimi della $f(u)$, come è lecito ammettere. Se applichiamo il teorema precedente alla derivata logaritmica $\dfrac{f'(u)}{f(u)}$, che è anch'essa manifestamente una funzione ellittica, e ricordiamo che la somma dei residui di $\dfrac{f'(u)}{f(u)}$ è data da

$$N_0 - N_\infty\,,$$

indicando con N_0 il numero degli infinitesimi e con N_∞ il numero degli infiniti [1]) nel parallelogrammo, ne risulta

$$N_0 = N_\infty\,,$$

cioè il teorema: *Ogni funzione ellittica diventa nel parallelogrammo dei periodi tante volte zero quante volte infinita.* Possiamo intendere che questo teorema valga anche quando capitino infinitesimi o poli sul contorno, purchè dei due infinitesimi o poli equivalenti sui lati se ne conti uno solo. Ed ora se osserviamo che,

[1]) Ben inteso, computando ciascun infinitesimo o infinito tante volte quante unità sono nel suo ordine.

essendo c una costante qualunque, anche $f(u)-c$ è una funzione ellittica, possiamo enunciare il teorema generale :

Una funzione ellittica prende nel parallelogrammo dei periodi ogni valore fissato ad arbitrio sempre lo stesso numero di volte.

Questo numero fisso, che dice quante volte una funzione ellittica riprende in un parallelogrammo dei periodi ogni suo valore, si chiama l'*ordine* della funzione ellittica. Si vede subito che *non esistono funzioni ellittiche di primo ordine*. Una tale funzione dovrebbe invero possedere un solo polo del primo ordine con residuo nullo, ciò che è assurdo. Dunque : *Le funzioni ellittiche di minimo ordine sono quelle di secondo ordine.* Tale è per esempio la funzione elementare di Weierstrass $\wp\,u$.

Per una funzione ellittica $f(u)$ d'ordine n siano

$$\alpha_1\,,\quad \alpha_2\,,\ \ldots,\quad \alpha_n$$

i punti di infinitesimo, e

$$\beta_1\,,\quad \beta_2\,,\ \ldots,\quad \beta_n \;{}^{1)}$$

i poli nel parallelogrammo fondamentale dei periodi $A\,B\,C\,D$, che supponiamo nuovamente non contenga sul contorno nè punti α nè punti β. Fra le posizioni degli zeri α e degli infiniti β passa una relazione, che è un caso particolare di un celebre teorema d'*Abel* e che consiste nella formola

$$\sum\alpha - \sum\beta = 2\,m\,\omega + 2\,n\,\omega' \quad (m, n \text{ interi}), \tag{15}$$

o, come si suol scrivere anche più semplicemente :

$$\sum\alpha \equiv \sum\beta,\ (2\,\omega\,,\ 2\,\omega').$$

Per dimostrare la (15), si estenda al contorno $A\,B\,C\,D$ del parallelogrammo l'integrale

$$\frac{1}{2\pi i}\int\limits_{ABCD} u\,\frac{f'(u)}{f(u)}\,du\,,$$

[1]) Se vi sono infinitesimi o poli d'ordine superiore, intendiamo che altrettante α o altrettante β coincidano.

il cui valore sarà la somma dei residui della funzione sotto il segno, cioè appunto $\Sigma\alpha - \Sigma\beta$. D'altra parte, decomponendo l'integrale come al § 97, abbiamo

$$\frac{1}{2\pi i}\int_{ABCD} u\,\frac{f'(u)}{f(u)}\,du = \frac{1}{2\pi i}\int_{AB}\left\{u\,\frac{f(u)}{f'(u)} - (u+2\omega')\,\frac{f'(u+2\omega')}{f(u+2\omega')}\right\}du$$

$$+\frac{1}{2\pi i}\int_{DA}\left\{u\,\frac{f'(u)}{f(u)} - (u+2\omega)\,\frac{f'(u+2\omega)}{f(u+2\omega)}\right\}du =$$

$$= -\frac{2\omega'}{2\pi i}\int_{AB}\frac{f'(u)}{f(u)}\,du + \frac{2\omega}{2\pi i}\int_{AD}\frac{f'u}{f(u)}\,du\,.$$

Ora l'integrale indefinito $\int \frac{f'(u)}{f(u)}\,du$ è $\log f(u)$ e poichè in B, D la $f(u)$ ha lo stesso valore che in A, i due valori ottenuti in B, D per $\log f$ lungo i cammini rettilinei AB, AD non possono differire da $\log f_A$ che per multipli di $2\pi i$, ciò che dimostra la (15).

§ 100. — Espressione di una funzione ellittica con infinitesimi ed infiniti assegnati.

Procediamo ora alla effettiva costruzione delle più generali funzioni ellittiche. Riferendoci ai teoremi dimostrati alla fine del § 98, risolveremo successivamente i due problemi:

A) *costruire una funzione ellittica, assegnati nel parallelogrammo fondamentale i suoi infinitesimi ed i suoi poli;*

B) *costruire una funzione ellittica, assegnati i suoi poli ed i suoi termini d'infinito.*

Nel presente capitolo ci occupiamo del primo problema, esprimendo la funzione ellittica cercata per mezzo della σ. Siano nel parallelogrammo fondamentale

$$\alpha_1,\ \alpha_2,\ \dots,\ \alpha_n$$

gli infinitesimi, e

$$\beta_1,\ \beta_2,\ \dots,\ \beta_n$$

i poli della funzione ellittica cercata dove, al solito, se si avranno infinitesimi o poli d'ordine superiore al primo, altrettante α o β dovranno coincidere fra loro.

Pel teorema d'Abel, l'esistenza della funzione è subordinata al verificarsi della relazione

$$(15^*)\qquad \sum\alpha - \sum\beta = 2r\omega + 2s\omega' \qquad (r,\ s \text{ interi}),$$

ma ora dimostreremo che, soddisfatta questa condizione, esiste effettivamente la funzione ellittica cercata $f(u)$.

Consideriamo la funzione

$$(16)\qquad \frac{\sigma(u-\alpha_1)\ \sigma(u-\alpha_2)\ \dots,\ \sigma(u-\alpha_n)}{\sigma(u-\beta_1)\ \sigma(u-\beta_2)\ \dots,\ \sigma(u-\beta_n)},$$

che è uniforme in tutto il piano ed ha a comune colla $f(u)$ da costruirsi gli infinitesimi ed i poli. La $f(u)$ richiesta non può dunque differire dalla (16) che per un fattore esponenziale

$$e^{G(u)},$$

il cui esponente $G(u)$ sia una trascendente intera. Avremo dunque:

$$f(u) = e^{G(u)}\,\frac{\sigma(u-\alpha_1)\ \sigma(u-\alpha_2)\ \dots.\ \sigma(u-\alpha_n)}{\sigma(u-\beta_1)\ \sigma(u-\beta_2)\ \dots.\ \sigma(u-\beta_n)}$$

e resterà da determinare, se sarà possibile, la $G(u)$ in guisa che il secondo membro ammetta i periodi 2ω, $2\omega'$. Servendoci delle formole fondamentali (12) § 97, troviamo che $G(u)$ deve soddisfare le condizioni seguenti

$$(17)\qquad \begin{cases} G(u+2\omega) - 2\eta\left[\sum\alpha - \sum\beta\right] = G(u) + 2k\pi i \\ G(u+2\omega') - 2\eta'\left[\sum\alpha - \sum\beta\right] = G(u) + 2k'\pi i, \end{cases}$$

dove k, k' debbono essere interi. Da queste, derivando, segue che la trascendente intera $G'(u)$ deve ammettere i periodi 2ω, $2\omega'$, onde sarà una costante (§ 98), ed avremo

$$G(u) = A\,u + B$$

con A, B costanti. Le (17) diventano

$$(18)\qquad \begin{cases} A\,\omega - \eta\,(2\,r\,\omega + 2\,s\,\omega') = k\,\pi\,i \\ A\,\omega' - \eta'\,(2\,r\,\omega + 2\,s\,\omega') = k'\,\pi\,i \end{cases}$$

da cui

$$A\,(\eta\,\omega' - \eta'\,\omega) = (k'\eta - k\,\eta')\,\pi\,i\,.$$

Ma, per la (V), pag. 15, è $\eta\,\omega' - \eta'\,\omega = \dfrac{\pi\,i}{2}$ e però

$$A = 2\,k'\,\eta - 2\,k\,\eta'.$$

Sostituendo nella prima delle (18), abbiamo

$$(2\,k'\eta - 2\,k\,\eta')\,\omega - \eta\,(2\,r\,\omega + 2\,s\,\omega') = k\,\pi\,i$$

ovvero, poichè $\eta'\omega = \eta\,\omega' - \dfrac{\pi\,i}{2}$:

$$2\,(k' - r)\,\eta\,\omega - 2\,(k + s)\,\eta\,\omega' = 0\,,$$

e similmente dalla seconda delle (18):

$$2\,(k' - r)\,\eta'\omega - 2\,(k + s)\,\eta'\,\omega' = 0\,.$$

Non potendo essere $\eta = \eta' = 0$, ne deduciamo

$$k' = r\,,\quad k = -s\,,$$

e però

$$\mathrm{A} = 2\,r\,\eta + 2\,s\,\eta'$$

e con questo valore di A le (18) sono effettivamente soddisfatte.

Per la funzione ellittica cercata $f\,(u)$ avremo dunque l'espressione analitica

$$(\mathrm{VI})\qquad f\,(u) = C\,e^{(2r\eta + 2s\eta')\,u}\,\frac{\sigma\,(u - a_1)\quad \sigma\,(u - a_2)\,\ldots.\,\sigma\,(u - a_n)}{\sigma\,(u - \beta_1)\quad \sigma\,(u - \beta_2)\,\ldots.\,\sigma\,(u - \beta_n)}\,,$$

restando C costante arbitraria. Ne concludiamo: *Dati ad arbitrio nel parallelogrammo dei periodi gli infinitesimi a e gli infiniti β*

di una funzione ellittica da determinarsi, purchè sia soddisfatta la condizione

$$(15^*)\qquad \sum a - \sum \beta = 2\,r\,\omega + 2\,s\,\omega' \qquad (r,\ s \text{ interi})\,,$$

la funzione esiste ed è data, a meno di un fattore costante, dalla (VI).

Osserviamo che nella (VI) non importa che i punti a, β siano tutti in un medesimo parallelogrammo, ma basta che le a formino un sistema *completo* di infinitesimi non equivalenti e le β similmente un sistema completo di poli della funzione. In particolare potremo alterare le a e le β di periodi, in guisa che risulti

$$\sum a = \sum \beta\,,$$

e allora la (VI) diventerà più semplicemente:

$$(\mathrm{VI}^*)\quad f(u) = C\,\frac{\sigma\,(u - a_1)\quad \sigma\,(u - a_2)\,\ldots.\,\sigma\,(u - a_n)}{\sigma\,(u - \beta_1)\quad \sigma\,(u - \beta_2)\,\ldots.\,\sigma\,(u - \beta_n)}\,,\quad \left(\sum a = \sum \beta\right).$$

§ 101. — Funzioni doppiamente periodiche di 1ª, 2ª e 3ª categoria.

Per mezzo della σ si esprimono, come si è visto, tutte le funzioni ellittiche, mediante la (VI) o (VI*). Ma insieme a queste funzioni, che offrono una doppia periodicità assoluta, possiamo esprimere più generalmente per la σ tutte quelle funzioni uniformi, senza singolarità essenziali tranne in $u = \infty$, *i cui infinitesimi ed infiniti sono distribuiti in modo doppiamente periodico nel piano, senza che lo siano gli altri valori* [1]).

Dati infatti ad arbitrio un sistema completo di infinitesimi

$$a_1\,,\quad a_2\,,\ \ldots,\ a_n\,,$$

ed un sistema completo di poli

$$\beta_1\,,\quad \beta_2\,,\ \ldots,\ \beta_m\,,$$

per la funzione cercata $\varphi\,(u)$, questa non potrà differire dal quoziente

$$\frac{\sigma\,(u - a_1)\quad \sigma\,(u - a_2)\,\ldots.\,\sigma\,(u - a_n)}{\sigma\,(u - \beta_1)\quad \sigma\,(u - \beta_2)\,\ldots.\,\sigma\,(u - \beta_m)}$$

[1]) La σ stessa offre il più semplice esempio di una tale specie di funzioni.

che per un fattore esponenziale

$$e^{G(u)},$$

nel quale la trascendente $G(u)$ resterà affatto arbitraria, sicchè

$$\varphi(u) = e^{G(u)} \frac{\sigma(u-a_1) \,....\, \sigma(u-a_n)}{\sigma(u-\beta_1) \,....\, \sigma(u-\beta_m)}.$$

Si avrà allora

$$\frac{\varphi(u+2\omega)}{\varphi(u)} = e^{G(u+2\omega)-G(u)+2\eta(n-m)u+2\eta'(\Sigma a-\Sigma\beta)+(n-m)\pi i}$$

$$\frac{\varphi(u+2\omega')}{\varphi(u)} = e^{G(u+2\omega')-G(u)+2\eta'(n-m)u+2\eta'(\Sigma\beta-\Sigma a)+(n-m)\pi i}.$$

Possiamo determinare $G(u)$ in guisa che i fattori esponenziali, per cui $\varphi(u+2\omega)$, $\varphi(u+2\omega')$ differiscono da $\varphi(u)$, abbiano esponenti lineari in u, come accade per la σu. Sarà perciò necessario e sufficiente che $G(u)$ sia un polinomio di secondo grado in u:

$$G(u) = a u^2 + b u + c,$$

dopo di che per la funzione

(VII) $$\varphi(u) = e^{a u^2+bu+c} \frac{\sigma(u-a_1) \,....\, \sigma(u-a_n)}{\sigma(u-\beta_1) \,....\, \sigma(u-\beta_m)}$$

risulterà:

(19) $$\begin{cases} \varphi(u+2\omega) = e^{Au+B} \cdot \varphi(u) \\ \varphi(u+2\omega') = e^{A'u+B'} \cdot \varphi(u), \end{cases}$$

dove si è posto

$$A = 4a\omega + 2\eta(n-m), \qquad A' = 4a\omega' + 2\eta'(n-m)$$

$$\begin{cases} B = 4a\omega^2 + 2b\omega + 2\eta\left(\sum\beta - \sum a\right) + (n-m)\pi \\ B' = 4a\omega'^2 + 2b\omega' + 2\eta'\left(\sum\beta - \sum a\right) + (n-m)\pi i. \end{cases}$$

Si noti che fra le costanti A, A' ha luogo la relazione

(20) $$A\omega' - A'\omega = (n-m)\pi i.$$

Diremo funzioni periodiche di prima categoria quelle $\varphi(u)$, date dalla (VII), per le quali si possono determinare a, b in guisa che ne risulti

$$A = A' = B = B' = 0,$$

cioè in modo da avere una funzione ellittica. Per ciò è necessario e sufficiente che si abbia insieme

(21) $$n - m = 0, \quad \sum a \equiv \sum \beta.$$

Le funzioni periodiche di prima categoria coincidono dunque colle ordinarie funzioni ellittiche, o ne differiranno soltanto per un fattore esponenziale con esponente di secondo grado.

Diremo periodiche di seconda categoria quelle $\varphi(u)$ per le quali possiamo determinare a, b in guisa che risultino ancora

$$A = A' = 0,$$

ma non simultaneamente $B = B' = 0$. In tal caso delle due condizioni (21) sarà soddisfatta solo la prima, e la funzione $\varphi(u)$ acquisterà fattori costanti per aggiunta di periodi all'argomento.

Attribuiamo in fine alla terza categoria tutte le altre funzioni $\varphi(u)$, per le quali adunque non è possibile determinare a, b in guisa da rendere $A = A' = 0$. Per le funzioni di terza categoria sarà quindi $n \neq m$.

§ 102. — Formola $\wp u - \wp v = \frac{\sigma(v+u)\,\sigma(v-u)}{\sigma^2 u\; \sigma^2 v}$ ed equazione ai tre termini per la σ.

Applichiamo subito i risultati generali del § 100 alla ricerca di alcune formole fondamentali. Sia v un punto fisso nel primo parallelogrammo dei periodi $(0, 2\omega, 2\omega+2\omega', 2\omega')$ e si consideri la differenza

$$\wp u - \wp v.$$

Considerata come funzione di u, è questa una funzione ellittica di secondo ordine con un unico infinito in $u = 0$ e col termine d' infinito $\frac{1}{u^2}$. Essa avrà dunque due infinitesimi nel parallelogrammo, che sono evidentemente nei punti

$$u_0 = v\,,\quad u_0 = 2\,\omega + 2\,\omega' - v\ ^{1)}\,;$$

questi infinitesimi saranno del primo ordine salvo quando siano equivalenti, il che accade soltanto per

$$v = \omega\,,\quad \omega',\quad \omega + \omega'\ ^{2)}.$$

La (VI*) ci dà quindi subito

$$\wp\, u - \wp\, v = C\frac{\sigma(u-v)\,\sigma(u+v)}{\sigma^2(u)}\,,$$

essendo C una costante rispetto ad u, cioè una funzione di v.

Per determinare C basta moltiplicare per u^2 e passare al limite per $u = 0$, osservando che

$$\lim_{u=0} u^2 \wp\, u = 1\,,\qquad \lim_{u=0} \frac{\sigma\, u}{u} = 1$$

e si trova $C = -\sigma^2 v$. Abbiamo così la formola fondamentale:

$$\text{(VIII)}\qquad \wp\, u - \wp\, v = \frac{\sigma(u+v)\,\sigma(v-u)}{\sigma^2 u\ \sigma^2 v}\,.$$

Di qui possiamo dedurre un'altra formola importante per la σ. Essendo

$$a\,,\ b\,,\ c\,,\ d$$

quattro valori qualsiasi dell'argomento u, e posto

$$A = \wp\, a\,,\quad B = \wp\, b\,,\quad C = \wp\, c\,,\quad D = \wp\, d\,,$$

[1]) A causa di $\wp(-v) = \wp\, v$.

[2]) Che le differenze

$$\wp u - \wp\omega\,,\quad \wp u - \wp\omega'\,,\quad \wp u - \wp(\omega + \omega')$$

abbiano rispettivamente in $u = \omega,\ \omega',\ \omega + \omega'$ un infinitesimo di secondo ordine risulta anche da ciò che ivi si annulla $\wp'$. Infatti, essendo $\wp'$ dispari, si ha per es.

$$\wp'(2\,\omega - u) = -\wp' u\,,$$

indi $\wp'\omega = -\wp'\omega = 0$ e così $\wp'\omega' = 0$, $\wp'(\omega + \omega') = 0$.

si ha l' identità

$$(A - B)\ (C - D) + (A - C)\ (D - B) + (A - D)\ (B - C) = 0\ ^{1)},$$

ossia

$$(\wp a - \wp b)(\wp c - \wp d) + (\wp a - \wp c)(\wp d - \wp b) + (\wp a - \wp d)(\wp b - \wp c) = 0.$$

Se alle differenze $\wp a - \wp\, b$, $\wp c - \wp d$ ecc. sostituiamo le loro espressioni date dalla (VIII), e togliamo i denominatori, otteniamo la formola domandata:

$$\text{(IX)}\qquad \begin{aligned} &\sigma(a-b)\,\sigma(a+b)\,\sigma(c-d)\,\sigma(c+d) + \\ &+ \sigma(a-c)\,\sigma(a+c)\,\sigma(d-b)\,\sigma(d+b) + \\ &+ \sigma(a-d)\,\sigma(a+d)\,\sigma(b-c)\,\sigma(b+c) = 0. \end{aligned}$$

che si dice l' *equazione ai tre termini* per la σ.

§ 103. — Equazione differenziale per la $\wp u$: $\wp'^2 = 4\,\wp^3 - g_2\,\wp - g_3$.

Un' altra formula importantissima otteniamo esprimendo la derivata $\wp' u$ per la σ. Si osservi che la $\wp' u$ è una funzione ellittica di terzo ordine, che diventa infinita nell'origine come $-\frac{2}{u^3}$ ed infinitesima del primo ordine nei tre punti non equivalenti

$$\omega\,,\quad \omega'\,,\quad -(\omega + \omega')\ ^{2)}$$

Per la (VI*), pag. 24, avremo dunque

$$\wp' u = C\,\frac{\sigma(u-\omega)\,\sigma(u-\omega')\,\sigma(u+\omega+\omega')}{\sigma^3 u}\,.$$

[1]) Basta sviluppare il determinante identicamente nullo

$$\begin{vmatrix} A & A & A \\ B & C & D \\ 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} A-B & A-C & A-D \\ B & C & D \\ 1 & 1 & 1 \end{vmatrix}.$$

[2]) Si prende $-(\omega + \omega')$ in luogo di $\omega + \omega'$, perchè sia $\Sigma\alpha = 0$ come $\Sigma\beta$ (cfr. § 100).

Per determinare la costante C si moltiplichi per u^3 e si passi al limite per $u = 0$; troviamo

$$C = -\frac{2}{\sigma\omega\;\sigma\omega'\;\sigma(\omega+\omega')},$$

indi

$$\text{(X)}\qquad \wp' u = -2\,\frac{\sigma(u-\omega)\,\sigma(u-\omega')\,\sigma(u+\omega+\omega')}{\sigma\omega\;\sigma\omega'\;\sigma(\omega+\omega')\,\sigma^3 u}.$$

Cangiando in questa u in $-u$ e moltiplicando le due formole fra loro, si ha:

$$\wp'^2 u = 4\,\frac{\sigma(\omega-u)\,\sigma(\omega+u)}{\sigma^2\omega\;\sigma^2 u}\cdot\frac{\sigma(\omega'-u)\,\sigma(\omega'+u)}{\sigma^2\omega'\;\sigma^2 u}\cdot\frac{\sigma(\omega+\omega'-u)\,\sigma(\omega+\omega'+u)}{\sigma^2(\omega+\omega')\,\sigma^2 u}$$

ossia per la (VIII)

$$\text{(XI)}\qquad \wp'^2 u = 4\,(\wp u - \wp\omega)\,(\wp u - \wp\omega')\,(\wp u - \wp(\omega+\omega')),$$

formola che potremmo anche stabilire direttamente, osservando che le due funzioni ellittiche dei due membri hanno a comune infinitesimi e poli.

Da questa formola (XI) deriviamo importanti conseguenze, cercando di determinare i coefficienti del polinomio di terzo grado in $\wp u$ del secondo membro. Possiamo a tale scopo servirci degli sviluppi di $\wp u$, $\wp' u$ nell'intorno dell'origine $u = 0$. La formola (III), pag. 13, ci dà per lo sviluppo di $\wp u$ nell'intorno dell'origine

$$\text{(22)}\qquad \wp u = \frac{1}{u^2} + \sum_{m,n}{}' \left\{ \frac{1}{(u-w)^2} - \frac{1}{w^2} \right\}$$

$$(w = 2m\omega + 2n\omega').$$

Secondo i teoremi sulle serie di funzioni analitiche (vol. I, cap. IV, §§ 47, 48), si può sviluppare la serie del secondo membro in una serie di potenze di u nel modo seguente. Abbiamo

$$\frac{1}{(u-w)^2} = \frac{1}{w^2}\left(1-\frac{u}{w}\right)^{-2}$$

e quando $|u| < |w|$ (per il che basta che $|u|$ sia minore della più piccola delle quantità $2|\omega|$. $2|\omega'|$ $2|\omega+\omega'|$ $2|\omega-\omega'|$), sviluppando colla serie binomiale, abbiamo

$$\left(1-\frac{u}{w}\right)^{-2} = \sum_{r=0}^{r=\infty}(r+1)\,\frac{u^r}{w^r},$$

indi

$$\frac{1}{(u-w)^2} - \frac{1}{w^2} = \sum_{r=1}^{r=\infty}(r+1\,\frac{u^r}{w^{r+2}}$$

e sostituendo nella (22):

$$\wp u = \frac{1}{u^2} + \sum_{m,n}{}' \sum_{r=1}^{r=\infty} \frac{(r+1)\,u^r}{w^{r+2}}.$$

Ordiniamo la serie tripla per le potenze di u, osservando che tutte le somme doppie

$$\sum_{m,n}{}' \frac{1}{(2m\omega+2n\omega')^{r+2}}$$

per r dispari sono nulle [1]). Ponendo

$$\text{(23)}\qquad c_r = \sum_{m,n}{}' \frac{1}{(2m\omega+2n\omega')^{2r+2}}\quad (r = 1, 2, 3, \ldots),$$

avremo per lo sviluppo domandato

$$\text{(24)}\qquad \wp u = \frac{1}{u^2} + \sum_{r=1}^{r=\infty}(2r+1)\,c_r u^{2r},$$

quindi

$$\wp' u = -\frac{2}{u^3} + 2\sum_{r=1}^{r=\infty} r\,(2r+1)\,c_r u^{2r-1}.$$

Ora, facendo uso con Weierstrass delle notazioni

$$\text{(25)}\qquad e_1 = \wp\omega,\quad e_2 = \wp(\omega+\omega'),\quad e_3 = \wp\omega',$$

[1]) Ciò risulta anche dalla parità di $\wp u$

e ponendo

(26) $g_1 = 4(e_1 + e_2 + e_3), \quad g_2 = -4(e_1 e_2 + e_2 e_3 + e_3 e_1), \quad g_3 = 4 e_1 e_2 e_3,$

potremo scrivere la (XI) così:

$$\wp'^2 u = 4\wp^3 u - g_1 \wp^2 u - g_2 \wp u - g_3 .$$

Moltiplichiamo questa per u^6 e sostituendo ad $u^3 \wp' u$, $u^2 \wp u$ i loro sviluppi, dati dalle (24), (24*):

$$u^3 \wp' u = -2 + 6 c_1 u^4 + 20 c_2 u^6 + \ldots$$
$$u^2 \wp u = 1 + 3 c_1 u^4 + 5 c_2 u^6 + \ldots,$$

avremo l'identità:

$$(-2 + 6 c_1 u^4 + 20 c_2 u^6 + \ldots)^2 = 4(1 + 3 c_1 u^4 + 5 c_2 u^6 + \ldots)^3 -$$
$$- g_1 u^2 (1 + 3 c_1 u^4 + \ldots)^2 - g_2 u^4 (1 + 3 c_1 u^4 + \ldots) - g_3 u^6,$$

e paragonando da una parte e dall'altra i coefficienti di u^2, u^4, u^6, otteniamo

$$g_1 = 0, \quad g_2 = 60 c_1 = 60 \sum_{m,n}' \frac{1}{(2m\omega + 2n\omega')^4},$$

$$g_3 = 140 c_2 = 140 \sum_{m,n}' \frac{1}{(2m\omega + 2n\omega')^6}.$$

Di qui vediamo intanto che si ha

(27) $$e_1 + e_2 + e_3 = 0,$$

cioè

$$\wp\omega + \wp\omega' + \wp(\omega + \omega') = 0$$

e per ciò

$$\begin{cases} g_2 = -4(e_1 e_2 + e_2 e_3 + e_3 e_1) = 2(e_1^2 + e_2^2 + e_3^2) \\ g_3 = 4 e_1 e_2 e_3 . \end{cases}$$

La relazione fra $\wp' u$ e $\wp u$ resta dunque

(XII) $$\wp'^2 u = 4\wp^3 u - g_2 \wp u - g_3 .$$

§ 104. — Gli invarianti g_2 g_3 e gli sviluppi di $\wp u$, ξu, σu nell'intorno di $u = 0$.

Le costanti g_2, g_3, che dipendono dai periodi 2ω, $2\omega'$ nel modo trascendente espresso dalle formole

(XIII) $$\begin{cases} g_2 = 60 \sum_{m,n}' \dfrac{1}{(2m\omega + 2n\omega')^4} \\ g_3 = 140 \sum_{m,n}' \dfrac{1}{(2m\omega + 2n\omega')^6}, \end{cases}$$

diconsi gli *invarianti* della funzione $\wp u$. Una prima ragione di tale denominazione la troviamo in questo che, comunque si cangino i periodi, purchè la $\wp u$ rimanga la stessa, le costanti g_2, g_3 non cangiano. È evidente infatti che, come per la σu (§ 95), così per la $\wp u$, *condizione necessaria e sufficiente perchè due* $\wp u$ *costruite con diversi periodi*

$$\wp(u \mid \omega, \omega'), \quad \wp(u \mid \Omega, \Omega')$$

coincidano, è che i loro periodi siano legati da una sostituzione lineare omogenea

$$\begin{cases} \omega' = \alpha\Omega + \beta\Omega' \\ \omega = \gamma\Omega + \delta\Omega' \end{cases}$$

a coefficienti interi e determinante $\alpha\delta - \beta\gamma = 1$. In conseguenza i punti (poli) $2m\omega + 2n\omega'$ coincidono, salvo l'ordine, cogli altri $2m\Omega + 2n\Omega'$ e perciò, secondo le (XIII), i corrispondenti invarianti sono identici.

Osserviamo poi che dalla espressione analitica (22) della $\wp u$ discende immediatamente la formola di omogeneità

$$\wp(\lambda u \mid \lambda\omega, \lambda\omega') = \frac{1}{\lambda^2} \wp(u \mid \omega, \omega').$$

Si vedrà poi più tardi che la denominazione di invarianti, data a g_2, g_3, corrisponde anche ad una proprietà algebrica.

Ritorniamo ora allo sviluppo di $\wp u$ nell'intorno di $u = 0$:

$$\wp u = \frac{1}{u^2} + \sum_{r=1}^{r=\infty} (2r+1)\, c_r u^{2r} = \frac{1}{u^2} + \frac{g_2}{20} u^2 + \frac{g_3}{28} u^4 + \dots$$

per dimostrare l'importante teorema:

Tutti i coefficienti di questa serie sono funzioni razionali intere, a coefficienti razionali, degli invarianti g_2, g_3.

Per dimostrarlo osserviamo che, derivando la (XII), si ottiene

$$\wp'' u = 6\wp^2 u - \frac{1}{2} g_2 \tag{29}$$

e, se sostituiamo da una parte e dall'altra gli sviluppi di $\wp u$, $\wp'' u$ nell'intorno di $u = 0$, otterremo delle formole ricorrenti per i coefficienti, che porranno in evidenza la proprietà enunciata.

Pongasi per brevità $u^2 = v$ e inoltre

$$a_0 = 1, \quad a_1 = 0, \quad a_n = (2n-1)\, c_{n-1} \quad (\text{per } n > 1);$$

avremo

$$\wp u = \frac{1}{v} \sum_0^\infty a_n v^n$$

e quindi

$$\wp^2 u = \frac{1}{v^2} \sum_{n=0}^{n=\infty} \left(\sum_{r=0}^{r=n} a_r a_{n-r} \right) \cdot v^n$$

$$\wp'' u = \frac{1}{v^2} \sum_{n=0}^{n=\infty} (2n-2)\,(2n-3)\, a_n v^n.$$

Sostituendo nella (29) e paragonando da una parte e dall'altra i coefficienti di v^{n-2} (per $n > 2$), otteniamo

$$(2n-2)\,(2n-3)\, a_n = 6\,(a_0 a_n + a_1 a_{n-1} + \dots + a_{n-1} a_1 + a_n a_0)$$

ovvero, supposto $n > 3$:

$$(n-3)\,(2n+1)\, a_n = 3 \sum_{r=2}^{r=n-2} a_r a_{n-r}. \tag{30}$$

Da questa formola ricorrente a coefficienti interi potremo calcolare successivamente

$$a_4, \quad a_5, \quad a_6, \dots$$

per funzioni razionali ed intere, a coefficienti razionali, di a_2, a_3, ossia di g_2, g_3. Per i primi termini dello sviluppo si trova così:

$$\wp u = \frac{1}{u^2} + \frac{g_2}{20} u^2 + \frac{g_3}{28} u^4 + \frac{g_2^2}{2^4 \cdot 3 \cdot 5^2} u^6 + \frac{3 g_2 g_3}{2^4 \cdot 5 \cdot 7 \cdot 11} u^8 + \tag{31}$$

$$+ \frac{1}{2^4 \cdot 13} \left(\frac{g_3^2}{7} + \frac{g_2^3}{2 \cdot 3 \cdot 5^3} \right) u^{10} + \frac{g_2^2 g_3}{2^5 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11} u^{12} + \dots$$

Risulta dal teorema dimostrato che due funzioni $\wp u$, le quali abbiano i medesimi invarianti, coincidono, giacchè coincidendo i loro sviluppi (31) nell'intorno dell'origine, le due funzioni sono identiche. Siccome la $\wp u$ resta individuata dagli invarianti g_2, g_3, come dai periodi, si scriverà

$$\wp\,(u;\; g_2,\; g_3),$$

quando si vogliano porre in evidenza gli invarianti.

Con ciò però non è ancora dimostrato che *agli invarianti g_2, g_3 si possano dare valori arbitrari*. Questa proprietà importante effettivamente sussiste; ma nel nostro metodo di esposizione della teoria non lo potremo dimostrare che più tardi (vedi cap. XI).

Dallo sviluppo (31) di $\wp u$ facilmente si deduce integrando quello di ζu:

$$\zeta u = \frac{1}{u} - \frac{g_2}{20} \frac{u^3}{3} - \frac{g_3}{28} \frac{u^5}{5} - \frac{g_2^2}{2^4 \cdot 3 \cdot 5^2} \frac{u^7}{7} + \dots, \tag{32}$$

i cui coefficienti sono evidentemente funzioni razionali intere, a coefficienti razionali, di

$$g_2, \quad g_3.$$

Osserviamo in fine che, anche per la trascendente intera σu, nello sviluppo in serie

$$\sigma u = u + a u^3 + b u^5 + c u^7 + \dots,$$

i coefficienti a, b, c .... saranno della medesima natura. E infatti poichè

$$\sigma u \, . \, \zeta u = \sigma' u\,,$$

avremo

$$1 + 3\,a u^2 + 5\,b u^4 + 7\,c u^6 + \ldots = $$

$$= \left(\frac{1}{u} - \frac{g_2}{20}\,\frac{u^3}{3} - \frac{g_3}{28}\,\frac{u^5}{5} + \ldots\right)(u + a u^3 + b u^5 + c u^7 + \ldots)\,,$$

e paragonando dall' una parte e dall'altra i coefficienti delle medesime potenze di u, ne risulta subito la proprietà enunciata. Si avrà in particolare

$$a = 0\,, \quad b = -\frac{g_2}{240}\,, \quad c = -\frac{g_3}{840} \ldots$$

$$\sigma u = u - \frac{g_2}{240}\,u^5 - \frac{g_3}{840}\,u^7 + \ldots$$

CAPITOLO X.

Decomposizione di una funzione ellittica in elementi semplici. — Teorema d'addizione per la ζu e la $\wp u$. — Le funzioni ellittiche espresse razionalmente per $\wp u$, $\wp' u$. — Moltiplicazione e divisione dell'argomento nella $\wp u$.

§ 105. — Costruzione di una funzione ellittica con poli e termini d'infinito assegnati.

Ritornando alle funzioni generali ellittiche, occupiamoci ora di risolvere il secondo problema B enunciato al § 100 : *costruire una funzione ellittica, di cui siano assegnati nel parallelogrammo dei periodi i poli ed i termini d' infinito.* Sia $u = \beta$ uno qualunque dei poli assegnati e siano

$$(1) \qquad \frac{A_0}{u-\beta} + \frac{A_1}{(u-\beta)^2} + \frac{A_2}{(u-\beta)^3} + \ldots + \frac{A_{n-1}}{(u-\beta)^n}$$

i relativi termini d' infinito. La somma dei residui

$$\sum A_0\,,$$

estesa a tutti i poli nel parallelogrammo, o ad un sistema completo qualunque di poli, dovrà essere nulla (§ 99) : viceversa, soddisfatta questa condizione, esiste una corrispondente funzione ellittica, come ora dimostreremo costruendola effettivamente.

Per ciò cominciamo dall'osservare che le funzioni

$$\zeta u = \frac{\sigma' u}{\sigma u}\,, \quad \wp u, \quad \wp' u, \quad \wp'' u, \;\ldots,\; \wp^{(n-2)} u$$

diventano infinite in $u = 0$ e nei punti equivalenti coi termini rispettivi di infinito

$$\frac{1}{u}\,, \quad \frac{1}{u^2}\,, \quad -\frac{2}{u^3}\,, \quad \frac{2\,.\,3}{u^4} \;\ldots\; (-1)^n \frac{\pi(n-1)}{u^n}\,.$$

L'espressione

$$(2) \quad A_0 \zeta(u-\beta) + A_1 \wp(u-\beta) - \frac{1}{2} A_2 \wp'(u-\beta) + \frac{A_3}{2\,.\,3} \wp''(u-\beta + \ldots$$

$$+ \frac{(-1)^n A_{n-1}}{\pi(n-1)} \wp^{n-2}(u-\beta)$$

diventa quindi infinita in $u = \beta$ precisamente coi termini d' infinito (1).

Se facciamo la somma delle espressioni (2), estesa ai punti β nel parallelogrammo dei periodi, ovvero ad un sistema completo di poli della funzione ellittica cercata $f(u)$, ed osserviamo che la somma

$$\sum A_0 \zeta(u-\beta)$$

ammette i periodi $2\,\omega$, $2\,\omega'$, a causa di

$$\sum A_0 = 0\,,$$

avremo subito

$$\text{(I)}\quad f(u) = C + \sum \Big\{ A_0 \zeta(u-\beta) + A_1 \wp(u-\beta) - \frac{A_2}{2}\wp'(u-\beta) + $$
$$+ \frac{A_3}{2\,.\,3}\wp''(u-\beta) + \ldots + \frac{(-1)^n A_{n-1}}{\pi(n-1)}\wp^{(n-2)}(u-\beta)\Big\},$$

essendo C una costante additiva arbitraria. Il secondo membro è effettivamente una funzione ellittica coi periodi 2ω, $2\omega'$, coi poli e i termini d'infinito assegnati. Dunque vediamo che : *Di una funzione ellittica $f(u)$ si possono assegnare ad arbitrio un sistema completo di poli e i loro termini d'infinito, purchè sia nulla la somma dei residui ; e la funzione cercata è data, a meno di una costante additiva, dalla* (I).

§ 106. — Formole d'addizione degli argomenti nella ζu e nella $\wp u$.

Il secondo membro della formola (I) si può cangiare, come ci proponiamo di dimostrare, in una funzione razionale di $\wp u$, $\wp' u$. A questo si arriva trasformando la (I) mediante le così dette *formole d'addizione* degli argomenti.

Cominciamo dallo stabilire la formola d'addizione per la funzione ζu. Perciò prendiamo la formola (§ 102) :

$$\frac{\sigma(u+v)\ \sigma(u-v)}{\sigma^2 u\ \sigma^2 v} = \wp v - \wp u$$

e derivandola logaritmicamente rapporto ad u otteniamo

$$\zeta(u+v) + \zeta(u-v) - 2\zeta u = \frac{\wp' u}{\wp u - \wp v},$$

da cui, permutando u con v e sommando, abbiamo :

$$\text{(II)}\qquad \zeta(u+v) = \zeta u + \zeta v + \frac{1}{2}\,\frac{\wp' u - \wp' v}{\wp u - \wp v}.$$

Questa esprime, come si vede, la ζ della somma di due argomenti per la ζ, la $\wp$ e la $\wp'$ degli argomenti semplici e dicesi la *formola d'addizione* per la ζ.

Deduciamo subito dalla (II) una conseguenza che importa notare. Facendovi

$$u = \omega, \qquad v = \omega'$$

e ricordando che $\wp'\omega = 0$ $\wp'\omega' = 0$, ne risulta

$$\zeta(\omega + \omega') = \zeta\omega + \zeta\omega' = \eta + \eta'$$

Più in generale se r, s sono due interi che non siano ambedue pari, ne risulta

$$\zeta(r\omega + s\omega') = r\eta + s\eta'.$$

Ciò posto, supponiamo di cangiare i periodi fondamentali 2ω, $2\omega'$ in altri due fondamentali $2\overline{\omega}$, $2\overline{\omega}'$ colla sostituzione lineare (§ 95)

$$\begin{cases} \overline{\omega} = \alpha\omega + \beta\omega' \\ \overline{\omega}' = \gamma\omega + \delta\omega' \end{cases}$$

con $\alpha, \beta, \gamma, \delta$ interi e $\alpha\delta - \beta\gamma = 1$, e chiamiamo $2\overline{\eta}$, $2\overline{\eta}'$ i nuovi periodi di seconda specie. Siccome la nuova funzione ζ è eguale all'antica, pel medesimo valore dell'argomento, avremo

$$\begin{cases} \overline{\eta} = \zeta(\overline{\omega}) = \zeta(\alpha\omega + \beta\omega') = \alpha\eta + \beta\eta' \\ \overline{\eta}' = \zeta(\overline{\omega}') = \zeta(\gamma\omega + \delta\omega') = \gamma\eta + \delta\eta'. \end{cases}$$

Se ne conclude il teorema : *Se i periodi di prima specie subiscono una sostituzione lineare* $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ *a coefficienti interi e a determinante* $= 1$, *anche i periodi di seconda specie subiscono la medesima sostituzione.*

Ritorniamo alla formola generale (II) d'addizione per la ζ e deriviamola rapporto ad u ; otteniamo :

$$\text{(III)}\qquad \wp(u+v) = \wp u - \frac{1}{2}\,\frac{\partial}{\partial u}\,\frac{\wp' u - \wp' v}{\wp u - \wp v},$$

che è una prima forma del *teorema d'addizione per la* $\wp$.

Se eseguiamo nel secondo membro della (III) la derivazione, e sostituiamo a

$$\wp'^2 u, \quad \wp'' u$$

i loro rispettivi valori

$$4\wp^3 u - g_2 \wp u - g_3\,, \quad 6\wp^2 u - \frac{1}{2} g_2\,,$$

la poniamo sotto l'altra forma

$$\wp(u+v) = \frac{2\left(\wp u\, \wp v - \frac{1}{4} g_2\right)(\wp u + \wp v) - g_3 - \wp' u\, \wp' v}{2(\wp u - \wp v)^2}\,,$$

mediante la quale esprimiamo $\wp(u+v)$ razionalmente per $\wp u$, $\wp' u$, $\wp v$, $\wp' v$. Compendiando la formola precedente con quella che se ne ottiene cangiando v in $-v$, possiamo scrivere

$$\text{(IV)} \qquad \wp(u \pm v) = \frac{2\left(\wp u\, \wp v - \frac{1}{4} g_2\right)(\wp u + \wp v) - g_3 \mp \wp' u\, \wp' v}{2(\wp u - \wp v)^2}\,.$$

Notiamo altre forme semplici ed utili del teorema d'addizione per la $\wp$. Dalla (III) si ha

$$\wp(u+v) = \wp u - \frac{6\wp^2 u - \frac{1}{2} g_2}{2(\wp u - \wp v)} + \frac{1}{2}\, \frac{\wp'^2 u - \wp' u\, \wp' v}{(\wp u - \wp v)^2}\,.$$

Permutando in questa u con v, sommando e dividendo per 2, abbiamo la formola equivalente

$$\text{(V)} \qquad \wp(u+v) = \frac{1}{4}\left(\frac{\wp' u - \wp' v}{\wp u - \wp v}\right)^2 - \wp u - \wp v$$

e perciò anche

$$\wp(u-v) = \frac{1}{4}\left(\frac{\wp' u + \wp' v}{\wp u - \wp v}\right)^2 - \wp u - \wp v\,,$$

da cui

$$\text{(VI)} \qquad \wp(u+v) - \wp(u-v) = -\frac{\wp' u\, \wp' v}{(\wp u - \wp v)^2}\,.$$

Meritano speciale menzione quei casi particolari del teorema d'addizione in cui l'argomento v è un *semiperiodo* ω, ω' ovvero $\omega + \omega'$, perchè allora il secondo membro si esprime per una fun-

zione lineare della sola $\wp u$. Se facciamo per es. nella (V) $v = \omega$, otteniamo

$$\wp(u+\omega) = -\wp u - e_1 + \frac{1}{4}\, \frac{\wp'^2 u}{(\wp u - e_1)^2} = -(\wp u + e_1) + \frac{(\wp u - e_2)(\wp u - e_3)}{\wp u - e_1}\,.$$

Ora si ha, eseguendo la divisione:

$$\frac{(\wp u - e_2)(\wp u - e_3)}{\wp u - e_1} = \wp u + e_1 - e_2 - e_3 + \frac{(e_1 - e_2)(e_1 - e_3)}{\wp u - e_1}$$
$$= \wp u + 2e_1 + \frac{(e_1 - e_2)(e_1 - e_3)}{\wp u - e_1}$$

e quindi:

$$\wp(u+\omega) = e_1 + \frac{(e_1 - e_2)(e_1 - e_3)}{\wp u - e_1}\,.$$

Con un calcolo analogo per $v = \omega + \omega'$, $v = \omega'$, otteniamo le formole richieste

$$\text{(VII)} \qquad \left\{\begin{aligned} \wp(u+\omega) &= e_1 + \frac{(e_1 - e_2)(e_1 - e_3)}{\wp u - e_1} \\ \wp(u+\omega+\omega') &= e_2 + \frac{(e_2 - e_3)(e_2 - e_1)}{\wp u - e_2} \\ \wp(u+\omega') &= e_3 + \frac{(e_3 - e_1)(e_3 - e_2)}{\wp u - e_3} \end{aligned}\right.$$ [1]).

[1]) Queste formole si possono anche stabilire direttamente così. Le funzioni ellittiche

$$\wp(u+\omega) - \wp\omega\,, \quad \wp(u+\omega+\omega') - \wp(\omega+\omega')\,, \quad \wp(u+\omega') - \wp\omega'$$

hanno rispettivamente per infinitesimi ed infiniti gli infiniti ed infinitesimi delle differenze

$$\wp u - \wp\omega\,, \quad \wp u - \wp(\omega+\omega')\,, \quad \wp u - \wp\omega'\,,$$

dalle cui inverse differiscono quindi solo per fattori costanti. Questi si determinano subito facendo successivamente, nelle tre formole

$$u = \omega'\,, \quad u = \omega\,, \quad u = \omega.$$

§ 107. — Espressione di ogni funzione ellittica in funzione razionale di $\wp u$, $\wp' u$.

Trovate nel paragrafo precedente le formole d'addizione per la $\wp u$, facilmente ne deduciamo quelle per le successive derivate, osservando che si ha

$$\wp'^2 u = 4\wp^3 u - g_2 \wp u - g_3$$

$$\wp'' u = 6\wp^2 u - \frac{1}{2} g_2$$

$$\wp''' u = 12 \wp u \, \wp' u$$

$$\wp^{IV} u = 12\left(10\wp^3 u - \frac{3}{2} g_2 \wp u - g_3\right)$$

. . . . :

e in generale che ogni derivata d'ordine pari è un polinomio razionale intero in $\wp u$, mentre ogni derivata d'ordine impari è il prodotto di $\wp' u$ per un tale polinomio [1]). Ne segue che in generale

$$\wp^{(n)}(u+v)$$

si esprime razionalmente per

$$\wp u, \quad \wp v, \quad \wp' u, \quad \wp' v.$$

Ciò posto, riprendiamo la formola generale (I) § 105, che dà la decomposizione di una qualsiasi funzione ellittica $f(u)$ in elementi semplici e modifichiamo il secondo membro, servendoci del teorema d'addizione. Abbiamo in primo luogo

$$\zeta(u-\beta) = \zeta u - \zeta \beta + \frac{1}{2} \frac{\wp' u + \wp' \beta}{\wp u - \wp \beta},$$

[1]) Supposto infatti verificata la legge fino alle derivate

$$\wp^{(2n-2)} u, \qquad \wp^{(2n-1)} u,$$

facilmente si vede che vale per le successive

$$\wp^{(2n)}, \qquad \wp^{(2n+1)} u.$$

onde, a causa di $\Sigma A_0 = 0$

$$C + \sum A_0 \zeta(u-\beta) = C' + \frac{1}{2} \sum A_0 \frac{\wp' u + \wp' \beta}{\wp u - \wp \beta}.$$

La (I) può quindi scriversi anche così

$$\text{(VIII)} \qquad f(u) = C' + \frac{1}{2} \sum A_0 \frac{\wp' u + \wp' \beta}{\wp u - \wp \beta} +$$

$$+ \sum \left\{ A_1 \wp(u-\beta) - \frac{A_2}{2} \wp'(u-\beta) + \dots + \right.$$

$$\left. + \frac{(-1)^n A_{n-1}}{\pi(n-1} \wp^{(n-2)}(u-\beta) \right\}.$$

Però è da osservarsi che se uno dei poli della $f(u)$ fosse in $\beta = 0$, il corrispondente termine nella prima somma del secondo membro deve essere tralasciato. Se nessun polo di $f(u)$ è in $u = 0$, il termine apparente d'infinito in $u = 0$ nella (VIII) sparisce in effetto, a causa di $\Sigma A_0 = 0$.

Ora è evidente che nella (VIII) possiamo, colle formole d'addizione, cangiare anche gli altri termini della somma in altrettante funzioni razionali di $\wp u$, $\wp' u$. Perveniamo così all'importante teorema:

Qualunque funzione ellittica coi periodi 2ω, $2\omega'$ è esprimibile razionalmente per la $\wp u$, $\wp' u$ costruite coi medesimi periodi.

La funzione $\wp u$ e la sua derivata $\wp' u$ sono dunque le funzioni elementari ellittiche, colle quali si possono comporre razionalmente tutte le altre.

Osserviamo poi che, siccome il quadrato di $\wp'$ è esprimibile razionalmente per la $\wp$, potremo porre ogni funzione ellittica $f(u)$ sotto la forma

$$f(u) = A(\wp u) + \wp' u \, B(\wp u),$$

essendo A, B funzioni razionali di $\wp u$. Così ogni funzione ellittica $f(u)$ risulta decomposta in due parti l'una pari, l'altra dispari. Mancherà la seconda parte se $f(u)$ è pari, la prima se $f(u)$ è dispari.

Segue inoltre che: *per ogni funzione ellittica* $f(u)$ *si avrà un teorema d'addizione e cioè fra*

$$f(u), \quad f(v), \quad f(u+v)$$

sussisterà, qualunque siano gli argomenti u, v, *una relazione algebrica*

$$G(f(u), f(v), f(u+v)) = 0, \tag{3}$$

dove G *è un polinomio razionale intero nei suoi tre argomenti.*

E infatti, se dalle formole

$$\begin{cases} f(u) = A(\wp u) + \wp' u\, B(\wp u) \\ f(v) = A(\wp v) + \wp' v\, B(\wp v) \\ f(u+v) = A(\wp(u+v)) + \wp'(u+v)\, B(\wp(u+v)), \end{cases}$$

mediante le formole d'addizione e le formole

$$\wp'^2 u = 4\wp^3 u - g_2 \wp u - g_3$$

$$\wp'^2 v = 4\wp^3 v - g_2 \wp v - g_3,$$

eliminiamo $\wp u$, $\wp' u$, $\wp v$, $\wp' v$, otterremo appunto fra $f(u)$, $f(v)$, $f(u+v)$ una relazione della forma (3).

Se consideriamo due funzioni ellittiche $f(u)$, $f_1(u)$ coi medesimi periodi, avremo

$$f(u) = A(\wp u) + \wp' u\, B(\wp u)$$

$$f_1(u) = A_1(\wp u) + \wp' u\, B_1(\wp u)$$

e fra queste due e la

$$\wp'^2 u = 4\wp^3 u - g_2 \wp u - g_3,$$

eliminando $\wp u$, $\wp' u$, ne segue una relazione algebrica fra $f(u)$, $f_1(u)$. Abbiamo dunque il teorema: *Due funzioni ellittiche coi medesimi periodi sono sempre legate da un'equazione algebrica.*

§ 108. — Nuovo modo di stabilire i risultati dei due paragrafi precedenti.

I risultati stabiliti nei due paragrafi precedenti sono d'importanza così fondamentale per la teoria delle funzioni ellittiche che sarà bene darne una seconda dimostrazione. Cominciamo perciò dallo stabilire in altro modo semplicissimo la formola (V) d'addizione, della quale tutte le altre sono conseguenze.

Indichiamo con u_1, u_2 due valori fissi dell'argomento, che non siano però multipli di periodi, nè congrui fra loro, e supponiamo di più che *non* sia

$$u_1 + u_2 \equiv 0.$$

Il determinante

$$\psi(u) = \begin{vmatrix} 1 & \wp u & \wp' u \\ 1 & \wp u_1 & \wp' u_1 \\ 1 & \wp u_2 & \wp' u_2 \end{vmatrix}$$

è una funzione ellittica del terzo ordine con un polo del terzo ordine in $u = 0$, ed avrà quindi tre infinitesimi non equivalenti, due dei quali sono evidentemente in $u = u_1$, $u = u_2$ e il terzo u_0 sarà quindi in

$$u_0 \equiv -(u_1 + u_2).$$

Avremo dunque l'identità

$$\begin{vmatrix} 1 & \wp(u_1+u_2) & -\wp'(u_1+u_2) \\ 1 & \wp u_1 & \wp' u_1 \\ 1 & \wp u_2 & \wp' u_2 \end{vmatrix} = 0,$$

formola che contiene appunto l'indicato teorema d'addizione. Sviluppando abbiamo

$$\wp u_1 \wp' u_2 - \wp u_2 \wp' u_1 + \wp(u_1+u_2)(\wp' u_1 - \wp' u_2) =$$
$$= \wp'(u_1+u_2)(\wp u_2 - \wp u_1),$$

ed elevando al quadrato col porre $\wp(u_1 + u_2) = x$ otterremo

$$(4) \qquad (4x^3 - g_2 x - g_3)(\wp u_1 - \wp u_2)^2 - \\ \{(\wp' u_1 - \wp' u_2)x + \wp u_1 \, \wp' u_2 - \wp u_2 \, \wp' u_1\}^2 = 0.$$

Le radici di questa equazione del terzo grado sono, oltre $x = \wp(u_1 + u_2)$, le $x = \wp u_1$, $x = \wp u_2$, giacchè il determinante $\psi(u)$ si annulla per $u = u_1$, $u = u_2$. Il primo membro della (4) sarà dunque identicamente eguale al prodotto

$$4(\wp u_1 - \wp u_2)^2 (x - \wp(u_1 + u_2))(x - \wp u_1)(x - \wp u_2)$$

e, se paragoniamo i coefficienti di x^2, troviamo precisamente la formola (V)

$$\wp(u_1 + u_2) + \wp u_1 + \wp u_2 = \frac{1}{4}\left(\frac{\wp' u_1 - \wp' u_2}{\wp u_1 - \wp u_2}\right)^2.$$

Dimostriamo ora nuovamente il teorema che: *Ogni funzione ellittica coi periodi* 2ω, $2\omega'$ *è una funzione razionale di* $\wp u$, $\wp' u$.

Per questo cominciamo dall'osservare che dalla formola fondamentale (I) pag. 37 risulta subito il teorema: *Ogni funzione ellittica d'ordine n, che diventa infinita solo nell'origine* (*e nei punti equivalenti*), *è una funzione lineare intera di*

$$\wp u, \quad \wp' u, \quad \wp'' u, \quad \dots, \quad \wp^{(n-2)} u$$

e quindi esprimibile sotto la forma

$$f(u) = \alpha(\wp u) + \wp' u \, \beta(\wp u),$$

dove α, β *sono polinomî razionali interi in* $\wp u$.

Ora è ben facile vedere che qualsiasi funzione ellittica $\psi(u)$ è sempre il quoziente di due tali funzioni speciali $f_1(u)$, $f(u)$.

Siano infatti $a_1, a_2, \dots, a_n$ gli infinitesimi (non equivalenti) di $\psi(u)$ e $b_1, b_2, \dots, b_n$ i poli; avremo $\Sigma a \equiv \Sigma b$. Supposto dapprima che sia $\Sigma b \equiv 0$, potremo costruire una funzione ellittica d'ordine n, sia $f(u)$, che diventi infinitesima in $b_1, b_2, \dots, b_n$ ed infinita (d'ordine n) nell'origine, onde il prodotto $f(u) \cdot \psi(u)$ diventerà infinito solo nei vertici della rete, e sarà per ciò una

funzione $f_1(u)$ della specie voluta, *c. d. d.* Se poi $\Sigma b \not\equiv 0$, prendasi $b_{n+1} \equiv -\Sigma b$ e si costruisca la $f(u)$ d'ordine $n + 1$ cogli infinitesimi $b_1, b_2, \dots, b_n, b_{n+1}$ e un infinito d'ordine $n + 1$ nell'origine, e si proceda come sopra.

§ 109. — Funzioni uniformi che ammettono un teorema d'addizione.

Le funzioni ellittiche sono, come abbiamo dimostrato, funzioni uniformi che ammettono un teorema d'addizione.

Queste proprietà caratterizzano perfettamente le funzioni ellittiche e due altre classi di funzioni, che possono del resto riguardarsi come casi limiti delle ellittiche. Sussiste infatti il seguente teorema, dovuto a Weierstrass:

Se una funzione $f(u)$, *uniforme in tutto il piano complesso, possiede un teorema d'addizione, in guisa che, essendo u, v due valori qualunque dell'argomento, fra* $f(u)$, $f(v)$, $f(u + v)$ *abbia luogo l'equazione algebrica*

$$(a) \qquad G(f(u), f(v), f(u + v)) = 0,$$

la $f(u)$ *potrà presentare i tre casi seguenti: 1° la* $f(u)$ *è una funzione razionale di u; 2° la* $f(u)$ *è una funzione razionale dell'esponenziale* $e^{\alpha u}$ (*a costante*)*; 3°* $f(u)$ *è una funzione ellittica e quindi razionale nelle due funzioni elementari* $\wp u$, $\wp' u$ [1]).

Questo importante teorema è per Weierstrass il punto di partenza per la sua trattazione della teoria delle funzioni ellittiche (cfr. Lezioni manoscritte).

Dimostreremo il teorema enunciato seguendo il metodo di Phragmèn (loc. cit., in nota). In primo luogo se la $f(u)$, uniforme in tutto il piano complesso, non ha alcuna singolarità essenziale, sarà una funzione razionale di u (vol. I, cap. VI, § 61). Che inversamente ogni funzione razionale di u possegga un teorema d'addizione è subito evidente.

Abbia ora la $f(u)$ almeno una singolarità essenziale; dimostreremo allora in primo luogo che la $f(u)$ dovrà essere almeno una

[1]) Per le generali funzioni analitiche sussiste un teorema analogo, sostituendo alla qualifica di funzione *razionale* quella di funzione *algebrica* (vedi la dimostrazione di PHRAGMÈN, *Acta Mathematica*, Bd. 7, pag. 33.

volta periodica e per ciò partiremo dal fatto che, essendo N un numero intero grande quanto si voglia, vi sarà qualche valore che la $f(u)$ riprenderà N volte o più. Utilizzando un teorema di Picard, enunciato al cap. VI, § 60 (vol. I), la cosa riesce di immediata evidenza; ma possiamo facilmente dimostrare il nostro lemma riferendoci soltanto ai risultati di Weierstrass, relativi alle singolarità essenziali, dimostrati al citato § 60. Sia b un valore preso da $f(u)$ un certo numero m di volte in m punti regolari

$$u_1, \quad u_2, \ \ldots, \ u_m.$$

Se consideriamo m intorni sufficientemente piccoli di $u_1, u_2, \ldots, u_m$, sappiamo che $f(u)$ prenderà in questi intorni *tutti* i valori sufficientemente prossimi a b.

D'altronde, in vicinanza di una singolarità essenziale, la $f(u)$ prende *dei* valori prossimi a b più di qualunque quantità assegnabile. Se ne conclude che esisterà qualche valore c prossimo a b, che $f(u)$ riprenderà almeno $m + 1$ volte, e cioè una volta nell' intorno di ciascun punto $u_1, u_2, \ldots, u_m$ ed una volta nell' intorno della singolarità essenziale. Partendo ora da c, troveremo almeno un valore d, che $f(u)$ dovrà riprendere almeno $m + 2$ volte e così di seguito.

Ciò premesso, supponiamo che, nella supposta formula d'addizione

$$(a) \qquad G(f(u), f(v), f(u+v)) = 0,$$

la funzione razionale intera G sia di grado m in $f(u+v)$ e sia b un valore che $f(u)$ riprenda almeno $m + 1$ volte nei punti distinti

$$v_1, \quad v_2, \ \ldots, \ v_{m+1}.$$

L'equazione

$$G(f(u), b, x) = 0$$

ammetterà le $m + 1$ radici in x

$$f(u+v_1), \quad f(u+v_2), \ \ldots, \ f(u+v_{m+1})$$

e fra queste ve ne saranno quindi almeno due eguali, per es. sarà *con qualunque* u:

$$f(u+v_1) = f(u+v_2),$$

od anche

$$f(u + v_1 - v_2) = f(u),$$

ossia, posto $v_1 - v_2 = 2\omega$:

$$f(u + 2\omega) = f(u).$$

Dunque intanto: *la* $f(u)$ *è almeno una volta periodica*. Supponiamo dapprima che sia semplicemente periodica, e sia 2ω il periodo di modulo minimo, del quale adunque tutti gli altri saranno multipli. Se poniamo

$$z = e^{\frac{\pi i u}{\omega}},$$

e consideriamo $f(u)$ come funzione di z

$$f(u) = \varphi(z),$$

sarà $\varphi(z)$ funzione uniforme di z, poichè, per ogni cammino chiuso descritto da z,

$$u = \frac{\omega}{\pi i} \log z$$

aumenta di un multiplo di 2ω ed $f(u)$ si riproduce. Ora se $\varphi(z)$ non ha, rispetto a z, alcuna singolarità essenziale, sarà una funzione razionale di z, diciamo $R(z)$, quindi

$$f(u) = R\left(e^{\frac{\pi i u}{\omega}}\right).$$

Che viceversa ogni funzione razionale dell'esponenziale possegga un teorema d'addizione è subito evidente.

Se poi $\varphi(z)$ possiede qualche singolarità essenziale, dovrà, per quanto si è visto sopra, riprendere il medesimo valore per $m + 1$ valori distinti di z e quindi per $m + 1$ valori di u incongrui rispetto al periodo 2ω. La $f(u)$ ammetterà dunque un secondo periodo distinto.

Resta in fine che consideriamo il caso in cui la $f(u)$ possegga due periodi distinti 2ω, $2\omega'$ (in rapporto necessariamente complesso) e possiamo supporre 2ω, $2\omega'$ già scelti in guisa che ogni altro periodo, non indipendente da questi, sia un loro aggregato lineare omogeneo a coefficienti interi. Se proviamo che $f(u)$ non può avere singolarità essenziali a distanza finita, sarà provato che è una funzione ellittica, quindi razionale in $\wp u$, $\wp' u$. Ora, se vi fosse nel parallelogrammo $(2\omega, 2\omega')$ una singolarità essenziale, dalla formola supposta d'addizione seguirebbe, come sopra, che per due certi punti v_1, v_2 situati nel parallelogrammo dei periodi $(2\omega, 2\omega')$ si avrebbe, per qualunque valore dell'argomento u,

$$f(u+v_1) = f(u+v_2)$$

e però $v_1 - v_2$ sarebbe un *nuovo* periodo, indipendente da 2ω, $2\omega'$, ciò che è impossibile (§ 98). Così l'enunciato teorema di Weierstrass è completamente dimostrato.

§ 110. — Formole di moltiplicazione dell'argomento per la $\wp u$.

Passiamo ora a studiare le *formole di moltiplicazione* dell'argomento per la $\wp u$. Essendo n un numero intero qualunque, la funzione $\wp(nu)$ è evidentemente una funzione ellittica coi periodi 2ω, $2\omega'$ ed è una funzione pari, come la $\wp u$, onde avremo (§ 95): *La $\wp(nu)$, per qualunque valore del numero intero n, è una funzione razionale di $\wp u$.* Si tratta ora di studiare più da vicino la composizione di questa funzione razionale $F(\wp u)$. Ricorriamo perciò alle formole di addizione (§ 106), e dalla (IV) deduciamo

$$\wp(u+v)+\wp(u-v) = \frac{2\left(\wp u\, \wp v - \frac{1}{4} g_2\right)(\wp u + \wp v) - g_3}{(\wp u - \wp v)^2}.$$

Se cangiamo in questa u in $(n-1)u$ e v in u, otteniamo la formola ricorrente:

$$\wp(nu)+\wp((n-1)u) = \tag{5}$$
$$= \frac{2\left[\wp((n-1)u)\,\wp u - \frac{1}{4} g_2\right](\wp(n-1)u + \wp u) - g_3}{(\wp(n-1)\;u - \wp u)^2}$$

mediante la quale, facendovi

$$n = 3,\ 4,\ 5,\ \ldots,$$

si calcoleranno successivamente

$$\wp(3u),\quad \wp(4u),\quad \wp(5u),\ \ldots,$$

in funzione razionale di $\wp u$, $\wp(2u)$. Se poi nella formola (V) § 106:

$$\wp(u+v) = \frac{1}{4}\left(\frac{\wp' u - \wp' v}{\wp u - \wp v}\right)^2 - \wp u - \wp v,$$

poniamo $u = v$, osservando che, al limite per $u = v$,

$$\frac{\wp' u - \wp v}{\wp u - \wp v}$$

diventa

$$\frac{\wp'' u}{\wp' u} = \frac{6\wp^2 u - \frac{1}{2} g_2}{\wp' u}$$

otteniamo

$$\wp(2u) = \frac{\left(6\wp^2 u - \frac{1}{2} g_2\right)^2}{4\wp'^2 u} - 2\wp u.$$

È utile dare a questa formola l'altra forma

$$\wp(2u) - \wp u = \frac{-3\wp^4 u + \frac{3}{2} g_2 \wp^2 u + 3 g_3 \wp u + \frac{1}{16} g_2^2}{\wp'^2 u}. \tag{6}$$

Dalle (5), (6) risulta che: *nella funzione razionale $F(\wp u) = \wp(nu)$ il numeratore ed il denominatore sono polinomî a coefficienti interi nelle quantità g_3, $\frac{1}{4} g_2$.*

§ 111. — La funzione $\psi_n(u) = \dfrac{\sigma(nu)}{\sigma^{n^2} u}$.

Il calcolo successivo di $\wp(2u)$, $\wp(3u)$, $\wp(4u)$ .... dalla formola ricorrente (5) riuscirebbe molto complicato. Si ottiene una notevole semplificazione del processo introducendo una funzione ellittica ausiliaria $\psi_n(u)$, che definiamo ponendo:

$$\psi_n(u) = \frac{\sigma(n\,u)}{\sigma^{n^2} u}. \tag{6*}$$

Le formole fondamentali per la σu (§ 97) dimostrano subito che la $\psi_n(u)$ è effettivamente una funzione ellittica coi periodi 2ω, $2\omega'$. Essa diventa infinita d'ordine $n^2 - 1$ in $u = 0$; i suoi $n^2 - 1$ infinitesimi nel parallelogrammo dei periodi sono nei punti

$$\frac{2r\omega + 2s\omega'}{n},$$

dove r, s percorrono tutti i valori $0, 1, 2, \ldots; n-1$, *esclusa la combinazione* $(r, s) = (0, 0)$. Ne segue che, se si considera il prodotto

$$\Pi'_{r,s}\left(\wp u - \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)\right),$$

ove r, s percorrono gli indicati valori, questa funzione avrà a comune con $\psi_n^2(u)$ periodi, infiniti ed infinitesimi, e sarà quindi

$$\psi_n^2(u) = C\,\Pi'_{r,s}\left(\wp u - \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)\right). \tag{7}$$

Ora, se osserviamo che

$$\wp\left(\frac{2(n-r)\omega + 2(n-s)\omega'}{n}\right) = \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)$$

e che le coppie *opposte* (r, s) $(n-r, n-s)$ sono sempre distinte *se n è dispari*, vediamo che per n dispari il secondo membro della (7) è il quadrato perfetto di un polinomio in $\wp u$ e si ha perciò

$$\psi_n(u) = C'\,\Pi''_{r,s}\left(\wp u - \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)\right), \text{ per } n \equiv 1 \pmod 2, \tag{8}$$

ove nel prodotto Π'' i numeri r, s percorrono $\frac{n^2-1}{2}$ coppie incongrue di valori (mod n) tali che colle opposte $(-r, -s)$ formino un sistema completo (mod n), con esclusione della coppia $(0, 0)$. Per queste $\frac{n^2-1}{2}$ coppie si potranno prendere, per es., le combinazioni seguenti

$$\begin{cases} r = 1, 2, 3, \ldots \frac{n-1}{2}, \text{ con } s = 0 \\ r = 0, 1, 2, \ldots n-1, \text{ con } s = 1, 2, 3, \ldots \frac{n-1}{2}. \end{cases}$$

Per determinare infine la costante C' in (8) si moltiplichi dall'una parte e dall'altra per u^{n^2-1} e si passi al limite per $u = 0$, osservando che

$$\lim_{u=0} (u^2 \wp u) = 1, \qquad \lim_{u=0} \{ u^{n^2-1} \psi_n(u) \} = n;$$

si avrà così la formola definitiva

$$\psi_n(u) = n\,\Pi''\left(\wp u - \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)\right), \quad (n \equiv 1 \pmod 2). \tag{9}$$

Se n è pari, vi sono soltanto le tre coppie

$$\left(\frac{n}{2}, 0\right), \quad \left(0, \frac{n}{2}\right), \quad \left(\frac{n}{2}, \frac{n}{2}\right)$$

che coincidono colle proprie opposte, e i corrispondenti fattori in (7) si riuniscono in

$$(\wp u - \wp\omega)\ (\wp u - \wp\omega')\ (\wp u - \wp(\omega + \omega')) = \frac{1}{4}\wp'^2 u,$$

mentre le residue $n^2 - 4$ coppie (r, s) si distribuiscono nuovamente due a due in coppie opposte; si avrà quindi

$$\psi_n(u) = C'\,\wp' u\,\overline{\Pi}_{r,s}\left(\wp u - \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)\right) \quad (n \equiv 0 \bmod 2),$$

ove nel prodotto $\overline{\Pi}$ le coppie r, s percorrono per es. i valori seguenti:

$$\begin{cases} r = 1, 2, 3, \ldots \frac{n}{2} - 1, \text{ con } s = 0, \ s = \frac{n}{2} \\ r = 0, 1, 2, \ldots n-1, \text{ con } s = 1, 2, 3 \ldots \frac{n}{2} - 1 \end{cases}$$

e determinando in fine la C' col solito processo avremo:

$$\psi_n(u) = -\frac{n}{2}\wp' u\,\overline{\Pi}_{r,s}\left(\wp u - \wp\left(\frac{2r\omega + 2s\omega'}{n}\right)\right), \ (n \equiv 0 \pmod 2). \tag{10}$$

Per mezzo delle funzioni $\psi_n(u)$ possiamo esprimere le formole di moltiplicazione dell'argomento per la $\wp u$, partendo dalla formola (§ 102)

$$\wp(nu) - \wp u = \frac{\sigma(n-1)u \, . \, \sigma(n+1)u}{\sigma^2(nu) \, . \, \sigma^2 u},$$

che scriviamo

$$\wp(nu) - \wp u = - \frac{\frac{\sigma(n-1)u}{\sigma^{(n-1)^2} u} \, . \, \frac{\sigma(n+1 u}{\sigma^{(n+1)^2} u}}{\left(\frac{\sigma n u}{\sigma^{n^2} u}\right)^2}$$

od anche per la (6*)

$$\wp(nu) - \wp u = - \frac{\psi_{n-1}(u)\, \psi_{n+1}(u)}{\psi_n^2(u)}. \tag{11}$$

Si osserverà poi che, secondo le formole (9), (10): *La funzione* $\psi(u)$ *per n dispari è un polinomio di grado* $\frac{n^2-1}{2}$ *in* $\wp u$ e *per n pari è il prodotto di* $\wp' u$ *per un polinomio di grado* $\frac{n^2-4}{2}$ *in* $\wp u$.

§ 112. — Calcolo delle funzioni $\psi_n(u)$ per mezzo di formole ricorrenti.

La formola (11) riduce la costruzione delle formole di moltiplicazione dell'argomento della $\wp u$ al calcolo delle funzioni $\psi_n(u)$. Dalla (6*) abbiamo subito intanto

$$\psi_1(u) = 1$$

e dalla (10)

$$\psi_2(u) = - \wp' u.$$

Poi, dal confronto della (*C*) § 110 colla formola

$$\wp(2u) - \wp u = - \frac{\psi_1 \psi_3}{\psi_2^2},$$

deduciamo

$$\psi_3(u) = 3\wp^4 u - \frac{3}{2} g_2 \wp^2 u - 3 g_3 \wp u - \frac{1}{16} g_2^2.$$

Per calcolare anche $\psi_4(u)$, ricorriamo alla (5), pag. 49, facendovi $n = 3$, e ne deduciamo:

$$\wp(3u) + \wp u = \frac{\left(2\wp(2u)\wp u - \frac{1}{2} g_2\right)\left(\wp(2u) + \wp u\right) - g_3}{\left(\wp(2u) - \wp u\right)^2},$$

sottraendo dai due membri $2\wp u$ e sostituendo per $\wp(2u)$ il suo valore $\wp u - \frac{\psi_3(u)}{\wp'^2 u}$, troviamo

$$\wp(3u) - \wp u = \frac{\wp'^2 u\,(\wp'^4 - \psi_3(u)\,\wp'' u)}{\psi_3^2(u)}$$

e paragonando questa colla

$$\wp(3u) - \wp u = - \frac{\psi_2 \psi_4}{\psi_3^2},$$

che segue dalla (11), abbiamo in fine:

$$\psi_4(u) = \wp' u\,(\wp'^4 u - \psi_3 \wp'' u) = \wp' u \left\{ -2\wp^6 u + \frac{5}{2} g_2 \wp^4 u + \right.$$
$$\left. + 10 g_3 \wp^3 u + \frac{1}{2} g_2 g_3 \wp u + g_3^2 + \frac{1}{32} g_2^3 \right\}.$$

Calcolate così le prime funzioni ψ_n:

$$\psi_1 = 1, \quad \psi_2 = - \wp' u, \tag{12}$$

$$\psi_3 = 3\wp^4 u - \frac{3}{2} g_2 \wp^2 u - 3 g_3 \wp u - \frac{1}{16} g_2^2, \quad \psi_4 = \wp' u\,(\wp'^4 u - \psi_3 \wp'' u),$$

possiamo calcolare le successive

$$\psi_5, \quad \psi_6, \quad \psi_7, \ldots$$

per mezzo di due formole ricorrenti, che ora andiamo a stabilire.

Partiamo perciò dall' equazione ai tre termini per la σu (§ 102):

$$\sigma(a-b)\ \sigma(a+b)\ \sigma(c-d)\ \sigma(c+d) + \sigma(a-c)\ \sigma(a+c)\ \sigma(d-b)\ \sigma(d+b) +$$
$$+ \sigma(a-d)\ \sigma(a+d)\ \sigma(b-c)\ \sigma(b+c) = 0$$

e facciamo in questa

$$a = mu, \qquad b = nu, \qquad c = u, \qquad d = 0,$$

onde avremo

$$\sigma(m+n)u \,.\, \sigma(m-n)u \,.\, \sigma^2 u = \sigma(m-1)u \,.\, \sigma(m+1)u \,.\, \sigma^2 nu -$$
$$- \sigma(n-1)u \,.\, \sigma(n+1)u \,.\, \sigma^2 mu \,.$$

Dividendo per

$$\sigma^{2m^2+2n^2+2} u = \sigma^{(m+n)^2+(m-n)^2+2} u = \sigma^{(m-1)^2+(m+1)^2+2n^2} =$$
$$= \sigma^{(n-1)^2+(n+1)^2+2m^2},$$

otteniamo

$$(a) \qquad \psi_{m+n}\,\psi_{m-n} = \psi_{m-1}\,\psi_{m+1}\,\psi_n^2 - \psi_{n-1}\,\psi_{n+1}\,\psi_m^2 \,.$$

Se facciamo in questa $m = n+1$ coll' osservare che $\psi_1(u) = 1$, abbiamo

$$(13) \qquad \psi_{2n+1} = \psi_{n+2}\,\psi_n^3 - \psi_{n-1}\,\psi_{n+1}^3 \,.$$

Cangiando nella (a) n in $n-1$ ed m in $n+1$ e ricordando che $\psi_2 = -\wp' u$ risulterà

$$(13^*) \qquad \psi_{2n} = \frac{\psi_n}{\wp' u}\,(\psi_{n-2}\,\psi_{n+1}^2 - \psi_{n+2}\,\psi_{n-1}^2) \,.$$

Le (13), (13*) sono le formole ricorrenti richieste. La prima a partire da $n = 2$, e la seconda da $n = 3$, esprimono ψ_{2n+1}, ψ_{2n} per le ψ con indice inferiore e risolvono quindi la questione proposta.

Si osservi che si ottiene un'altra formola ricorrente pel calcolo delle ψ_n, ove si derivi due volte logaritmicamente la (6*), ciò che dà

$$\frac{\psi''_n\,\psi_n - \psi'^2_n}{\psi_n^2} = n^2\,[\wp u - \wp nu],$$

e confrontando con (11) si ha la seguente formola ricorrente:

$$\psi_{n-1}\,\psi_{n+1} = \frac{1}{n^2}\,(\psi''_n\,\psi_n - \psi'^2_n) \,.$$

Da questa facendo $n = 2$, $n = 3$, troviamo i valori di ψ_3, ψ_4 già calcolati nelle (12) coll' uso delle formole d'addizione.

§ 113. — **Divisione dell'argomento nella $\wp u$.**

Data $\wp u$, la $\wp(nu)$ si calcola razionalmente. Se supponiamo invece data $\wp(nu)$ e cerchiamo $\wp u$, dalla (11) abbiamo per determinare $\wp u$ l'equazione

$$(14) \qquad \wp(nu) \,.\, \psi_n^2 - \wp u\, \psi_n^2 + \psi_{n-1}\,\psi_{n+1} = 0 .$$

Tenendo conto dei gradi in $\wp u$ di ψ_n, $\psi_{n-1}\,\psi_{n+1}$ si vede che in ogni caso questa equazione è del grado n^2 in $\wp u$, poichè il termine di questo più alto grado ha un coefficiente non nullo, come risulta subito dalle (9), (10). La (14) è irriducibile, perchè il polinomio ψ_n non ha fattori comuni nè con ψ_{n-1}, nè con ψ_{n+1}.

Cangiando nella (14) u in $\frac{u}{n}$, e ponendo

$$x = \wp u \,, \quad y = \wp\left(\frac{u}{n}\right),$$

le ψ_n^2, ψ_{n-1}, ψ_{n+1} diventeranno polinomi in y; e per determinare y dato x, avremo l'equazione di grado n^2

$$(15) \qquad x\,\psi_n^2 - y\,\psi_n^2 + \psi_{n-1}\,\psi_{n-1} = 0,$$

che è *l'equazione per la divisione dell'argomento della* $\wp u$.

Dimostriamo ora l' importante teorema: *L' equazione* (15) *per la divisione dell'argomento è risolubile per radicali.*

Cominciamo per ciò dall'esprimere tutte le radici in y della (15), osservando che questa relazione fra $\wp u$, $\wp\left(\frac{u}{n}\right)$ sussiste qualunque sia u e perciò anche mutando u in $u + 2r\omega + 2s\omega'$, con r, s

interi qualunque. Con ciò $x = \wp u$ non muta; ma $y = \wp\left(\frac{u}{n}\right)$ si cangia in

$$\wp\left(\frac{u+2r\omega+2s\omega'}{n}\right);$$

e poichè si ha

$$\wp\left(\frac{u+2r\omega+2s\omega'}{n}\right) = \wp\left(\frac{u+2r_1\omega+2s_1\omega'}{n}\right)$$

solo quando sia

$$r \equiv r_1, \quad s \equiv s_1 \pmod{n},$$

ciò che esprimiamo più brevemente scrivendo

$$(r, s) \equiv (r_1, s_1) \bmod n),$$

così vediamo che: *Le n^2 radici della equazione* (15) *per la divisione dell'argomento sono date dalle espressioni*

$$y_{r,s} = \wp\left(\frac{u+2r\omega+2s\omega'}{n}\right),$$

percorrendo (r, s) *un sistema completo di n^2 coppie incongrue* (mod n).

Ora, per le formole d'addizione

$$y_{r,s} = \wp\left(\frac{u+2r\omega+2s\omega'}{n}\right)$$

si esprime razionalmente per

$$\wp\left(\frac{u}{n}\right), \quad \wp'\left(\frac{u}{n}\right), \quad \wp\left(\frac{2r\omega+2s\omega'}{n}\right), \quad \wp'\left(\frac{2r\omega+2s\omega'}{n}\right),$$

e d'altronde per le formole di moltiplicazione

$$\wp u = F\left(\wp\left(\frac{u}{n}\right)\right),$$

dove F è il simbolo di una funzione razionale, e quindi derivando si ha:

$$\wp'\left(\frac{u}{n}\right) = \wp' u \,\Phi\left(\wp\left(\frac{u}{n}\right)\right),$$

essendo Φ razionale. Vediamo quindi che se, oltre $x = \wp u$, consideriamo come nota anche $\sqrt{4x^3 - g_2 x - g_3} = \wp' u$, ogni radice $y_{r,s}$ della (15) è una funzione razionale della prima radice $y_{00} = \wp\left(\frac{u}{n}\right)$ i cui coefficienti, oltre g_2, g_3, contengono razionalmente i valori delle $\wp$, $\wp'$ per le parti aliquote dei periodi

$$\wp\left(\frac{2r\omega+2s\omega'}{u}\right), \quad \wp'\left(\frac{2r\omega+2s\omega'}{n}\right).$$

Ora, se si pone

$$y_{r,s} = \psi(y_{00}), \text{ cioè } \wp\left(\frac{u+2r\omega+2s\omega'}{n}\right) = \psi\left(\wp\left(\frac{u}{n}\right)\right)$$

$$y_{r_1,s_1} = \psi_1(y_{00}), \text{ cioè } \wp\left(\frac{u+2r_1\omega+2s_1\omega'}{n}\right) = \psi_1\left(\wp\left(\frac{u}{n}\right)\right),$$

essendo ψ, ψ_1 simboli di due funzioni razionali della specie indicata, e si osserva che queste relazioni sussistono *qualunque sia* u, cangiando nella prima u in $u + 2r_1\omega + 2s_1\omega'$ e nella seconda u in $u + 2r\omega + 2s\omega'$, ne dedurremo

$$\psi(\psi_1(y_{00})) = \psi_1(\psi(y_{00})).$$

Di più si vede che, ove uno almeno dei due numeri r, s sia primo con n, il *periodo* della corrispondente operazione ψ è precisamente n, e se ne conclude:

L'equazione (15) *per la divisione dell'argomento è un'equazione Abeliana composta di grado n^2, che si risolve coll'estrazione di due radicali d'indice n.*

A questo risultato possiamo pervenire anche direttamente, ricercando il *gruppo di monodromia* (§ 81) della (15). Perciò dobbiamo far percorrere ad $x = \wp u$, nel suo piano complesso, un cammino chiuso qualunque, cioè cangiare u in

$$\pm u + 2\mu\omega + 2\nu\omega' \quad (\mu, \nu \text{ interi})$$

ed esaminare la sostituzione indotta sulle radici

$$y_{r,s} = \wp\left(\frac{u+2r\omega+2s\omega'}{n}\right).$$

Si vede subito che la $y_{r,s}$ si porta per tale sostituzione nella $y_{r',s'}$, dove gli indici r', s' sono determinati dalle congruenze

$$(16) \qquad \left\{ \begin{array}{l} r' \equiv \pm r + \mu \\ s' \equiv \pm s + \nu \end{array} \right. \pmod{n}.$$

Queste sostituzioni (16) formano appunto il gruppo di monodromia per la nostra equazione. Il gruppo (16) contiene evidentemente $2n^2$ sostituzioni e in esso è contenuto, come sottogruppo invariante d'indice 2, il gruppo

$$(16^*) \qquad \left\{ \begin{array}{l} r' \equiv r + \mu \\ s' \equiv s + \nu \end{array} \right. \pmod{n},$$

corrispondente ai segni superiori. Il gruppo di monodromia (16) si abbassa a (16*) coll'aggiunta di un radicale quadratico, che si vede subito essere

$$\sqrt{4x^3 - g_2 x - g_3} = \wp' u ,$$

giacchè le sostituzioni (16) corrispondenti ai segni inferiori lasciano bensì invariato $\wp u$, ma cangiano $\wp' u$, in $-\wp' u$.

Se consideriamo dunque come data anche $\wp' u$, il gruppo di monodromia è il gruppo (16) d'ordine n^2, generato dalle due sostituzioni elementari

$$(r', s') \equiv (r + 1, s) \pmod{n}$$
$$(r', s') \equiv (r, s + 1) \pmod{n}.$$

Anche di qui vediamo, come sopra, che l'equazione si risolve coll'estrazione di due radicali d'indice n.

Ma il primo metodo ha il vantaggio di farci riconoscere quali sono gli irrazionali numerici (rispetto agli invarianti g_2, g_3 supposti dati), la cui aggiunta fa scendere il gruppo algebrico al gruppo di monodromia. Sono questi i valori della $\wp$, $\wp'$ per le parti aliquote dei periodi.

§ 114. — **Equazione per la divisione dei periodi.**

Esaminiamo ora l'equazione da cui dipende la ricerca degli irrazionali

$$\wp\left(\frac{2r\omega + 2s\omega'}{n}\right), \qquad \wp'\left(\frac{2r\omega + 2s\omega'}{n}\right).$$

Basterà che ci occupiamo di determinare

$$\wp\left(\frac{2r\omega + 2s\omega'}{n}\right),$$

perchè

$$\wp'\left(\frac{2r\omega + 2s\omega'}{n}\right)$$

si otterrà successivamente estraendo una radice quadrata. Osserviamo poi che, se n è un numero composto $n = q \cdot q'$, basta saper risolvere l'equazione proposta pei divisori q, q' dopo di che, per quanto si è visto al paragrafo precedente, si otterrà

$$\wp\left(\frac{2r\omega + 2s\omega'}{qq'}\right)$$

con estrazione di radicali. *Ci possiamo dunque limitare al caso di n numero primo.*

Ora per $n = 2$ i corrispondenti valori

$$\wp\omega, \quad \wp\omega', \quad \wp(\omega + \omega')$$

sono le radici e_1, e_2, e_3 dell'equazione di terzo grado

$$4e^3 - g_2 e - g_3 = 0 .$$

Consideriamo dunque il caso di n numero primo dispari. Siccome

$$\wp\left(\frac{2r\omega + 2s\omega'}{n}\right) = \wp\left(\frac{-2r\omega - 2s\omega'}{n}\right),$$

basterà far percorrere a (r, s) $\frac{n^2-1}{2}$ coppie incongrue (mod n), tali che colle opposte $(-r, -s)$ formino un sistema completo (mod n) esclusa $(0, 0)$.

Questi $\frac{n^2-1}{2}$ valori

$$\wp\left(\frac{2r\omega+2s\omega'}{n}\right)$$

sono le radici della equazione

$$\text{(17)} \qquad \psi_n(y)=0\,,$$

che è appunto di grado $\frac{n^2-1}{2}$ ed ha coefficienti razionali interi in g_3, $\frac{1}{4}g_2$ con coefficienti numerici interi. Per ciò l'*equazione* (17) $\psi_n(y)=0$ *si dice l'equazione per la divisione dei periodi.*

Osserviamo ora che tutte le radici della (17) in cui $s=0$ si ordinano nelle serie

$$\text{(A)} \quad \wp\left(\frac{2\omega}{n}\right), \quad \wp\left(2\,.\,\frac{2\omega}{n}\right), \quad \wp\left(3\,.\,\frac{2\omega}{n}\right) \;\ldots\; \wp\left(\frac{n-1}{2}\,.\,\frac{2\omega}{n}\right)$$

e, per le formole di moltiplicazione dell'argomento, tutte le radici di questa serie sono funzioni razionali della prima $\wp\left(\frac{2\omega}{n}\right)$ con coefficienti razionali in g_2, g_3. Le rimanenti radici della (17) possono egualmente ordinarsi in serie, contenenti ciascuna $\frac{n-1}{2}$ radici, e dotate delle proprietà stesse della serie (A). E infatti, per $s \not\equiv 0 \pmod n$, possiamo determinare un numero ν dalla congruenza

$$s\nu \equiv r \pmod n$$

e scrivere

$$\wp\left(\frac{2r\omega+2s\omega'}{n}\right)=\wp\left(s\,\frac{2\nu\omega+2\omega'}{n}\right).$$

Tenendo fermo ν e ponendo

$$s=1,\ 2,\ \ldots\ \frac{n-1}{2}\,,$$

abbiamo una nuova serie di radici

$$\text{(B)} \qquad \wp\left(\frac{2\nu\omega+2\omega'}{n}\right),$$

$$\wp\left(2\,.\,\frac{2\nu\omega+2\omega'}{n}\right) \ldots \wp\left(\frac{n-1}{2}\,.\,\frac{2\nu\omega+2\omega'}{n}\right),$$

dotata delle proprietà della serie (A). Ora se diamo successivamente a ν i valori

$$\nu = 0,\ 1\ ,\ 2\ ,\ \ldots\ ,\ n-1$$

le n serie (B), insieme colla serie (A), contengono una ed una sola volta tutte le radici della (17), come subito si vede.

Poniamo per semplicità

$$\bar\omega_\nu = \frac{2\nu\omega+2\omega'}{n}\,,$$

e introducendo l'indice ∞ per ν nel primo caso di $s=0$, poniamo altresì

$$\bar\omega_\infty=\frac{2\omega}{n};$$

le $\frac{n^2-1}{2}$ radici della (17) si ordineranno così nel quadro:

$$\left.\begin{array}{llll}
\wp\,\bar\omega_\infty, & \wp(2\bar\omega_\infty), & \wp(3\bar\omega_\infty) & \ldots\ \wp\left(\frac{n-1}{2}\,\bar\omega_\infty\right)\\
\wp\,\bar\omega_0, & \wp(2\bar\omega_0), & \wp(3\bar\omega_0) & \ldots\ \wp\left(\frac{n-1}{2}\,\bar\omega_0\right)\\
\ldots & \ldots & \ldots & \ldots\\
\wp(\bar\omega_{n-1}), & \wp(2\bar\omega_{n-1}), & \wp(3\bar\omega_{n-1}) & \ldots\ \wp\left(\frac{n-1}{2}\,\bar\omega_{n-1}\right)
\end{array}\right\} \quad \begin{array}{l}\bar\omega_\infty=\frac{2\omega}{n}\\[2ex] \bar\omega_\nu=\frac{2\nu\omega+2\omega'}{n}\end{array}$$

contenente $n+1$ orizzontali di $\frac{n-1}{2}$ radici ciascuna. In ogni orizzontale possiamo poi ordinare in modo più conveniente le radici così. Sia g una radice primitiva (mod n), e con r_ϵ si indichi il resto di g^s (mod n), o il suo complemento a n, secondo che il resto stesso è $\leqq \frac{n-1}{2}$ ovvero $> \frac{n-1}{2}$; talchè i numeri r_0, r_1, r_2, ..., $r_{\frac{n-1}{2}}$ saranno in altro ordine i numeri

$$1,\ 2,\ 3 \ldots. \frac{n-1}{2}\ ^{1)}.$$

Se ordiniamo le radici della (17) nel nuovo quadro :

$$(\mathrm{C})\quad \left.\begin{array}{l} \wp(\tilde\omega_\infty),\quad \wp(g\tilde\omega_\infty),\quad \wp(g^2\tilde\omega_\infty)\ \ldots.\ \wp\left(g^{\frac{n-1}{2}-1}\tilde\omega_\infty\right) \\ \wp(\tilde\omega_0),\quad \wp(g\tilde\omega_0),\quad \wp(g^2\tilde\omega_0)\ \ldots.\ \wp\left(g^{\frac{n-1}{2}-1}\tilde\omega_0\right) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \wp(\tilde\omega_{n-1}),\ \wp(g\tilde\omega_{n-1}),\ \wp(g^2\tilde\omega_{n-1})\ \ldots.\ \wp\left(g^{\frac{n-1}{2}-1}\tilde\omega_{n-1}\right) \end{array}\right\}\quad \begin{array}{l} \tilde\omega_\infty = \dfrac{2\omega}{n} \\ \tilde\omega_\nu = \dfrac{2\nu\omega+2\omega'}{n} \end{array}$$

vediamo che, per le formole di moltiplicazione si ha :

$$\wp\,(g\,u = \Theta\,(\wp\,u)\,,$$

dove Θ è il simbolo di una funzione razionale con coefficienti razionali in g_2, g_3; si avrà quindi :

$$\wp\,(g\,\tilde\omega_\nu) = \Theta\,(\wp\,\tilde\omega_\nu)\,,\quad \wp\,(g^2\tilde\omega_\nu) = \Theta\,(\Theta(\wp\,\tilde\omega_\nu)) = \Theta^2\,(\wp\,\tilde\omega_\nu)\ \ldots.$$

$$\wp\left(g^{\frac{n-1}{2}-1}\tilde\omega_\nu\right) = \Theta^{\frac{n-1}{2}-1}\,(\wp\,\tilde\omega_\nu)\,,$$

indi

$$\wp\left(g^{\frac{n-1}{2}-1}\tilde\omega_\nu\right) = \wp\,(\tilde\omega_\nu) = \Theta^{\frac{n-1}{2}-1}\,\wp\,\tilde\omega_\nu).$$

Dunque : *Le radici di una medesima orizzontale nel quadro* (C) *sono tutte funzioni razionali della prima e formano, così ordinate, un unico periodo.*

1) E infatti da $g^s \equiv \pm\, g^{s_1}$ seguirebbe $g^{s-s_1} \equiv \pm\, 1$ quindi $s - s_1$ multiplo di $\frac{n-1}{2}$.

§ 115. — **Risolventi di grado $n+1$ dell'equazione per la divisione dei periodi e loro gruppo.**

Dal risultato precedente, pei teoremi generali della teoria delle equazioni secondo Galois, segue l'importante teorema : *La equazione per la divisione dei periodi possiede nel caso di n primo (dispari) risolventi di grado $n+1$.*

Prendasi infatti una funzione razionale (intera) e simmetrica delle radici di una medesima orizzontale del quadro (C) e sia

$$z_\nu = \Phi\left(\wp\,\tilde\omega_\nu,\ \wp\,(g\,\tilde\omega_\nu)\ \ldots.\ \wp\left(g^{\frac{n-1}{2}-1}\tilde\omega_\nu\right)\right)\qquad \nu = \infty,\ 0,\ 1,\ \ldots,\ n-1.$$

Gli $n+1$ valori di z

$$z_\infty,\quad z_0,\quad z_2,\ \ldots,\ z_{n-1}$$

sono radici di una equazione risolvente in grado $n+1$ in z

$$(18)\qquad\qquad F_{n+1}\,(z) = 0\,,$$

con coefficienti razionali in g_2, g_3. Quando sia risoluta la risolvente (18), la proposta (17) si risolve con estrazioni di radicali d'indice $\frac{n-1}{2}$. Anzi basta nel nostro caso l'estrazione di due tali radicali che ci diano

$$\wp\left(\frac{2\omega}{n}\right)\quad \wp\left(\frac{2\omega'}{n}\right),$$

e dei due radicali quadratici che danno

$$\wp'\left(\frac{2\omega}{n}\right),\quad \wp'\left(\frac{2\omega'}{n}\right),$$

le altre radici

$$\wp\left(\frac{2\,r\,\omega + 2\,s\,\omega}{n}\right)$$

potendosi poi calcolare razionalmente mediante le formole d'addizione.

La risoluzione dell'equazione per la divisione dei periodi si riduce dunque in sostanza a quella della (18) e ad estrazioni di radicali. Resta dunque che esaminiamo la risolvente (18) e ne determiniamo il gruppo di Galois. La equazione (18) contiene, razionalmente nei coefficienti, le quantità g_2, g_3 che riguardiamo come parametri [1]), e vogliamo innanzi tutto determinare il gruppo di monodromia della (18) rispetto a g_2, g_3. Perciò dobbiamo far variare i periodi 2ω, $2\omega'$ per tali cammini che g_2, g_3 riprendano alla fine i medesimi valori ed esaminare la sostituzione indotta sulle radici

$$z_\infty,\quad z_0,\quad z_1,\quad \ldots,\quad z_{n-1}.$$

Dal § 104 sappiamo che, a fine di riprodurre i medesimi valori di g_2, g_3, dobbiamo far subire ad ω, ω' la sostituzione lineare

$$\begin{pmatrix} \alpha\,\omega+\gamma\,\omega' & \beta\,\omega+\delta\,\omega' \\ \omega & \omega' \end{pmatrix}$$

a coefficienti interi α, β, γ, δ e a determinante $\alpha\delta-\beta\gamma=1$. Per tale sostituzione una radice qualunque della (17)

$$\wp\,(k\,\tilde{\omega}_\nu)=\wp\left(k\,\frac{2\,\nu\,\omega+2\,\omega'}{n}\right),$$

per ν finito, si trasporta nella radice

$$\wp\left(k\,\frac{2\,\nu\,(\alpha\,\omega+\gamma\,\omega')+2\,(\beta\,\omega+\delta\,\omega')}{n}\right)=\wp\left(k\,(\gamma\nu+\delta)\,\frac{2\,\nu'\omega+2\,\omega'}{n}\right),$$

posto

$$(19)\qquad \nu'\equiv\frac{\alpha\,\nu+\beta}{\gamma\,\nu+\delta}\pmod{n},$$

cioè in una radice $\wp\,(r\tilde{\omega}_{\nu'})$, e la medesima formola vale per $\nu=\infty$, giacchè

$$\wp\,(k\,\tilde{\omega}_\infty)=\wp\left(k\,\frac{2\,\omega}{n}\right)$$

[1]) In ciò facciamo uso della proprietà, che si dimostrerà nel seguente capitolo, che gli invarianti g_2, g_3 della $\wp$ possano darsi affatto arbitrariamente.

si trasporta in

$$\wp\left(k\gamma\,\frac{2\,\frac{\alpha}{\gamma}\,\omega+2\,\omega'}{n}\right)=\wp\left(r\,\frac{2\,\nu'\,\omega+2\,\omega'}{n}\right)$$

con $\nu'\equiv\frac{\alpha}{\gamma}\pmod{n}$. Tutte le radici di una orizzontale nel quadro (C) si trasportano dunque nelle radici di un'altra orizzontale, colla legge espressa dalla (19) e per ciò ogni radice z_ν della (18) si cangia nella radice $z_{\nu'}$ secondo la sostituzione lineare (19) sull'indice.

Ne concludiamo: *Il gruppo di monodromia della equazione* (18) *è il gruppo di* $\frac{n(n^2-1)}{2}$ *sostituzioni, rappresentato analiticamente dalla formola*

$$(19)\qquad \nu'\equiv\frac{\alpha\,\nu+\beta}{\gamma\,\nu+\delta}\pmod{n},\quad \alpha\delta-\beta\gamma\equiv1.$$

Si sa che questo gruppo (gruppo semimodulare) è *semplice* appena $n>3$ e perciò l'equazione (18) non è ulteriormente riducibile ad equazioni più semplici; in particolare *essa non è risolubile per radicali.*

Il gruppo algebrico dell'equazione (18), dovendo contenere come sottogruppo invariante il gruppo semimodulare (19), non può essere che il gruppo stesso o il gruppo totale lineare di $n(n^2-1)$ sostituzioni

$$\nu'\equiv\frac{\alpha\,\nu+\beta}{\gamma\,\nu+\delta},\quad \alpha\delta-\beta\gamma\not\equiv0\pmod{n}.$$

Ritornando più tardi, nella teoria della trasformazione delle funzioni ellittiche, su queste risolventi di grado $n+1$ dell'equazione per la divisione dei periodi, vedremo che è quest' ultimo caso che si presenta e l' irrazionalità numerica che si deve aggiungere per ridurre il gruppo algebrico al gruppo di monodromia è precisamente la radice quadrata

$$\sqrt{(-1)^{\frac{n-1}{2}}\cdot n}.$$

§ 116. — Risolubilità per radicali della equazione per la divisione dei periodi nelle funzioni lemniscatiche.

Ciò che abbiamo detto nel paragrafo precedente relativamente al gruppo di Galois dell'equazione per la divisione dei periodi suppone che gli invarianti g_2, g_3 (o i periodi 2ω, $2\omega'$) abbiano valori arbitrari. Ma per valori particolari dei periodi, o degli invarianti, può darsi benissimo che il gruppo si abbassi ad un suo sottogruppo fino anche ad ottenere un gruppo risolubile, ed allora per queste speciali funzioni ellittiche l'equazione per la divisione dei periodi risulterà risolubile per radicali.

Un esempio semplice di una tale classe di funzioni ellittiche si ha nelle *funzioni lemniscatiche*. Portano questo nome le funzioni ellittiche nelle quali il rapporto dei periodi $\frac{\omega'}{\omega}$ è $= i$ [1]). Per la funzione lemniscatica $\wp(u \mid \omega, i\omega)$ ha luogo la formola di *moltiplicazione complessa*

$$\wp(iu) = -\wp u, \tag{20}$$

che si deduce come caso particolare dalla formola d'omogeneità (§ 104)

$$\wp(\lambda u \mid \lambda\omega, \lambda\omega') = \frac{1}{\lambda^2}\wp(u \mid \omega, \omega'),$$

ove si faccia

$$\omega' = i\omega, \quad \lambda = i \text{ }^{2)}.$$

Confrontando nella (20) gli sviluppi di $\wp(iu)$, $\wp u$ nell'intorno dell'origine si vede subito che: *per la funzione lemniscatica $\wp u$ il secondo invariante g_3 è nullo.*

[1]) Il nome di lemniscatiche proviene da ciò che la rettificazione di un arco di lemniscata dipende appunto da funzioni di questa specie.

[2]) La (20) si stabilisce anche subito osservando che le due funzioni ellittiche $\wp(iu)$, $-\wp u$ hanno a comune periodi ed infiniti coi termini d'infinito.

Dimostriamo ora che per la nostra speciale $\wp u$ sussiste una formola generale di moltiplicazione complessa

$$\wp(mu) = R(\wp u), \tag{21}$$

dove m è un numero qualunque intero complesso di Gauss, cioè della forma $a + bi$ (a, b interi reali) ed R è il simbolo di una funzione razionale con coefficienti razionali in g_2. Siccome la (21) è vera per $m = 1$ e per $m = i$, basterà provare che se sussiste per m, sussiste anche per

$$m + i^\varepsilon \qquad (\varepsilon = 0, 1, 2, 3).$$

Ora per la formola d'addizione (IV), pag. 39, essendo $g_3 = 0$, si ha

$$\wp((m+i^\varepsilon)u) = \frac{2\{\wp(mu)\wp(i^\varepsilon u) - \frac{1}{4}g_2\}\cdot\{\wp(mu) + \wp(i^\varepsilon u)\} - \wp'(mu)\wp'(i^\varepsilon u)}{2\{\wp(mu) - \wp(i^\varepsilon u)\}^2}$$

Ma per la (20) si ha

$$\wp(i^\varepsilon u) = (-1)^\varepsilon \wp u, \qquad \wp'(i^\varepsilon u) = i^\varepsilon \wp' u$$

e dalla (21) derivando si ottiene

$$\wp'(mu) = \frac{1}{m} R'(\wp u)\cdot\wp' u,$$

onde

$$\wp'(mu)\,\wp'(i^\varepsilon u) = R_1(\wp u)$$

e ne risulta la proprietà asserita.

Ciò premesso, se ritorniamo per la $\wp u$ lemniscatica alla equazione (18) per la divisione dei periodi, vediamo che qualunque sua radice

$$\wp\left(\frac{2r\omega + s\omega'}{n}\right) = \wp\left((r + is)\frac{2\omega}{n}\right)$$

è una funzione razionale della prima $\wp\left(\frac{2\omega}{n}\right)$ e poichè ponendo

$$\wp\left((r+is)\frac{2\omega}{n}\right)=\psi\left(\wp\left(\frac{2\omega}{n}\right)\right)$$

$$\wp\left(r_1+is_1)\frac{2\omega}{n}\right)=\psi_1\left(\wp\left(\frac{2\omega}{n}\right)\right),$$

si vede subito che si ha

$$\wp\left((r+is)\ (r_1+is_1)\frac{2\omega}{n}\right)=\psi\left(\psi_1\left(\wp\frac{2\omega}{n}\right)\right)=\psi_1\left(\psi\left(\wp\frac{2\omega}{n}\right)\right),$$

ne concludiamo che l'equazione per la divisione dei periodi è nel caso attuale un'equazione Abeliana, ed è quindi risolubile per radicali.

Le funzioni lemniscatiche non sono del resto che un caso particolare di una intera classe di funzioni ellittiche, considerate da Abel, che ammettono formole di moltiplicazione complessa, e per le quali l'equazione per la divisione dei periodi è risolubile per radicali, come si vedrà nei due ultimi capitoli.

CAPITOLO XI.

Proprietà fondamentali della prima funzione modulare $J(\tau)$ (invariante assoluto). — La funzione $\wp(u; g_2, g_3)$, con assegnati invarianti. — Integrali ellittici di prima specie e loro inversione. — Integrali ellittici generali.

§ 117. — L'invariante assoluto $J=\frac{g_2^3}{g_2^3-27\,g_3^2}$, considerato come funzione del rapporto $\tau=\frac{\omega'}{\omega}$ dei periodi.

Nel presente capitolo cominciamo dal trattare la quistione, già posta al § 194: *Possono gli invarianti g_2, g_3 di una funzione ellittica $\wp u$ assumere valori arbitrari?* La risolveremo affermativamente, per una via invero alquanto indiretta, ma che ha il

vantaggio di procurarci la conoscenza della funzione fondamentale di una nuova ed importante classe di funzioni, *la classe delle funzioni modulari ellittiche.*

Cominciamo dal ricordare che, secondo le formole (XIII), pag. 32, gli invarianti g_2, g_3 si esprimono per i periodi $2\,\omega$, $2\,\omega'$ colle formole

$$g_2=\frac{15}{4}\sum{}'\frac{1}{(m\omega+n\omega')^4},\quad g_3=\frac{35}{16}\sum{}'\frac{1}{(m\omega+n\omega')^6}$$

e sono per ciò funzioni omogenee dei gradi -4, -6 rispettivamente di ω, ω'. È facile quindi formare delle espressioni razionali in g_2, g_3, che dipendano soltanto dal rapporto $\tau=\frac{\omega'}{\omega}$ dei periodi. Ricordiamo che

$$e_1=\wp\,\omega,\quad e_2=\wp\,(\omega+\omega'),\quad e_3=\wp\,\omega'$$

sono le radici della equazione di terzo grado

$$4\,e^3-g_2\,e-g_3=0.$$

Indicando con $\frac{\varDelta}{16}$ il discriminante

$$(e_1-e_2)^2\ (e_2-e_3)^2\ (e_3-e_1)^2$$

di questa equazione, avremo

$$\varDelta=g_2^3-27\,g_2^3.$$

Ora poniamo

$$J=\frac{g_2^3}{\varDelta}=\frac{g_2^3}{g_2^3-27\,g_3^2},$$

e J sarà funzione omogenea di grado zero in ω, ω', cioè dipenderà soltanto dal rapporto $\tau=\frac{\omega'}{\omega}$ dei periodi. Questa espressione J dicesi l'*invariante assoluto*, e primo oggetto della nostra ricerca sarà di provare che *J è funzione uniforme della variabile complessa τ, nel semipiano positivo τ.*

Consideriamo nel piano complesso τ un campo finito qualunque C che rimanga, anche col suo contorno, tutto nell' interno del semipiano positivo. Le due serie

$$(1)\qquad \begin{cases} G_2 = g_2\,\omega^4 = \dfrac{15}{4} \sum' \dfrac{1}{(m+n\tau)^4} \\[2ex] G_3 = g_3\,\omega^6 = \dfrac{35}{16} \sum' \dfrac{1}{(m+n\tau)^6} \end{cases}$$

convergono in egual grado, come ora dimostreremo, in tutto il campo C e rappresentano per ciò, in tutto C, delle funzioni finite, continue e monodrome di τ. Osserviamo intanto che, restando $\tau = a + i\beta$ in C, l'ordinata β si mantiene superiore ad una quantità fissa positiva β_0 e perciò

$$|\, m + n\tau \,| = \sqrt{(m+n\,a)^2 + n^2\beta^2}$$

si mantiene superiore o eguale alla più piccola d delle due quantità

$$\beta_0\,, \quad 1\,.$$

Per la medesima ragione la distanza β fra due punti $m + n\tau$, $m' + n'\tau$:

$$\delta = \sqrt{\{(m-m') + (n-n')\,a\}^2 + (n-n')^2\beta^2}$$

non scende, essa stessa, al disotto di d.

Fissato quindi un numero positivo $k < d$, se, procedendo come al § 69 (Cap. VI), dividiamo il piano in una rete di quadrati con lato $= \frac{k}{\sqrt{2}}$, potremo paragonare i moduli dei termini delle nostre serie con quelli delle due serie seguenti, indipendenti da τ, ed assolutamente convergenti

$$\sum_{r,s} \frac{1}{(r^2+s^2)^2\, \dfrac{k^4}{2^2}}\,, \qquad \sum_{r,s} \frac{1}{(r^2+s^2)^3\, \dfrac{k^6}{2^3}}\,;$$

onde risulta subito la convergenza in egual grado in tutto C delle serie (1).

Ne segue che la formola

$$(\mathrm{I})\qquad J(\tau) = \frac{g_2^3}{g_2^3 - 27\, g_3^2}$$

ci definisce una funzione della variabile complessa τ, continua e monodroma in tutto il semipiano positivo, l'asse reale escluso. Facilmente vediamo inoltre che $J(\tau)$ è anche sempre *finita* a qualunque distanza finita, escluso sempre l'asse reale. E infatti, se $\tau = a + i\beta$ è finito e $\beta > 0$, non può essere nullo il denominatore

$$g_2^3 - 27\, g_3^2 = 16\,(\wp\omega - \wp\omega')^2\; (\wp\omega - \wp(\omega+\omega'))^2\; (\wp\omega' - \wp(\omega+\omega'))^2,$$

giacchè le funzioni ellittiche di secondo ordine

$$\wp u - \wp\omega\,, \quad \wp u - \wp\omega'\,, \quad \wp u - \wp(\omega + \omega')$$

hanno già infinitesimi di secondo ordine in

$$u = \omega\,, \quad u = \omega'\,, \quad u = \omega + \omega'$$

rispettivamente, e non possono quindi annullarsi in punti non equivalenti a questi.

Facciamo ancora l'osservazione, che ci tornerà utile fra breve: *L' invariante assoluto* $J(\tau)$ *in due punti*

$$\tau = a + i\beta\,, \qquad \tau = -a + i\beta\,,$$

simmetrici rispetto all' asse immaginario, assume valori coniugati. Ciò accade infatti, come subito si vede, delle due serie

$$\sum' \frac{1}{(m+n\tau)^4}\,, \quad \sum' \frac{1}{(m+n\tau)^6}\,.$$

§ 118. — L' invariante $J(\tau)$ come funzione automorfa rispetto al gruppo modulare.

La funzione $J(\tau)$ è regolare, come si è visto, in tutto il semipiano positivo, l'asse reale escluso. Stabiliamo ora la proprietà fondamentale di questa funzione, ricercando quando accadrà che in due punti τ, τ' del semipiano positivo $J(\tau)$ riprenda il medesimo valore, cioè si abbia

$$J(\tau) = J(\tau').$$

Consideriamo per ciò le due funzioni $\wp$:

$$\wp(u \mid 1, \tau), \quad \wp(u \mid 1, \tau'),$$

coi rispettivi rapporti dei periodi τ, τ'. e indichiamone gli invarianti rispettivamente con

$$g_2, \; g_3; \quad g'_2, \; g'_3.$$

Si ha per ipotesi

$$\frac{g_2^3}{g_2^3 - 27\, g_3^2} = \frac{g'^3_2}{g'^3_2 - 27\, g'^2_3},$$

ossia indicando con l un fattore di proporzionalità

$$g_2^3 = \lambda\, g'^3_2, \qquad g_3^2 = \lambda\, g'^2_3.$$

Se con μ indichiamo un conveniente valore di $\sqrt[6]{\lambda}$, potremo scrivere

$$g_2 = \mu^2 g'_2, \qquad g_3 = \mu^3 g'_3.$$

Costruiamo ora una terza funzione ellittica

$$\wp(u \mid \Omega, \Omega\tau')$$

per la quale il rapporto dei periodi sia ancora τ; i suoi invarianti γ_2, γ_3 saranno quindi (§ 117)

$$\gamma_2 = \Omega^{-4} g'_2, \qquad \gamma_3 = \Omega^{-6} g'_3,$$

onde, prendendo $\Omega^2 = \dfrac{1}{\mu}$, avremo

$$\gamma_2 = g, \qquad \gamma_3 = g_3,$$

e però

$$\wp(u \mid \Omega, \Omega\tau') = \wp(u \mid 1, \tau \mid).$$

Per quanto si è visto al § 104, avremo quindi

$$(2) \begin{cases} \Omega\tau' = \alpha\tau + \beta \\ \Omega = \gamma\tau + \delta, \end{cases}$$

cioè

$$(3) \qquad \tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta},$$

essendo α, β, γ, δ numeri interi e $\alpha\delta - \beta\gamma = 1$.

Viceversa se τ' è legata a τ dalla (3), cioè da una sostituzione del *gruppo modulare* (Cap. II), ne seguirà

$$J(\tau') = J(\tau).$$

E infatti, indicando con Ω un fattore di proporzionalità, potremo sostituire le (2) alla (3) e le due funzioni coincidenti

$$\wp(u \mid 1, \tau), \qquad \wp(u \mid \Omega, \Omega\tau')$$

avranno i medesimi invarianti g_2, g_3 e però anche il medesimo invariante assoluto.

Riepilogando, abbiamo dunque: *condizione necessaria e sufficiente affinchè sia $J(\tau') = J(\tau)$ è che gli argomenti τ, τ' siano legati da una sostituzione del gruppo modulare*

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}.$$

Nella funzione $J(\tau)$ abbiamo così un nuovo esempio di funzioni automorfe (vedi § 98), il gruppo corrispondente di sostituzioni lineari essendo nel caso attuale il gruppo modulare. Questa funzione $J(\tau)$ non è che la prima e più semplice fra le *funzioni modulari*, delle quali in seguito tratteremo più diffusamente.

Se invece di considerare soltanto le sostituzioni del gruppo modulare, consideriamo anche quelle di seconda specie

$$\tau' = \frac{\alpha\tau_0 - \beta}{\gamma\tau_0 - \delta}$$

appartenenti al gruppo modulare ampliato (cap. II, § 18), per l'osservazione alla fine del paragrafo precedente, vediamo che in due tali punti τ, τ' la funzione modulare $J(\tau)$ assumerà valori coniugati, sicchè: *In due punti τ, τ' del semipiano positivo, equivalenti rispetto al gruppo modulare ampliato, $J(\tau)$ assume valori eguali o valori coniugati, secondo che la sostituzione del gruppo che fa passare da τ a τ' è di prima o di seconda specie.*

§ 119. — Distribuzione dei valori di $J(\tau)$ nella rete modulare.

Se ricordiamo ora la rappresentazione geometrica del gruppo modulare, che abbiamo stabilito nel Cap. II, e in particolare la divisione del semipiano positivo nella *rete modulare* (§ 20), questa figura acquisterà un corrispondente significato per la distribuzione dei valori dell'invariante assoluto. Intanto in ogni triangolo T' della rete $J(\tau)$ ripeterà i valori che prende nel primo triangolo fondamentale T, o i coniugati di questi, secondo che T' deriva dal fondamentale per un numero pari o dispari di riflessioni e basterà quindi che esaminiamo la distribuzione dei valori di $J(\tau)$ nel triangolo fondamentale. In primo luogo osserviamo che *su tutto il contorno del triangolo fondamentale, come sopra ogni circolo di riflessione del gruppo, $J(\tau)$ è reale.* E invero se C è un tale circolo e A, B due punti corrispondenti per la riflessione su C, i valori di J in a e b

$$J(a), \quad J(b)$$

sono coniugati; ma quando a cade sulla circonferenza C allora b coincide con a e però $J(a)$ è coniugato di sè stesso, cioè reale. Invece nell'interno del triangolo fondamentale $J(\tau)$ non è mai reale; poichè, altrimenti, nel punto simmetrico rispetto all'asse immaginario, $J(\tau)$ dovrebbe riprendere il medesimo valore e i due punti sarebbero equivalenti rispetto al gruppo modulare (non ampliato) Γ, ciò che non è. Segue di qui che in tutti i punti *interni* di T il coefficiente dell'immaginario in $J(\tau)$ serba sempre lo stesso segno. Vediamo ora quali valori $J(\tau)$ assume nei vertici

$$\tau = i, \qquad \tau = \varepsilon = e^{\frac{2\pi i}{3}}$$

di T; dico che si ha

$$J(i) = 1, \quad J(\varepsilon) = 0.$$

La prima cosa risulta da ciò che per la funzione lemniscatica $\wp(u \mid \omega, i\omega)$ si ha $g_3 = 0$ come si è visto al § 116. E similmente per la funzione $\wp$ (equianarmonica)

$$\wp(u \mid \omega, \varepsilon\omega)$$

avendo luogo, come risulta dalla formola di omogeneità, la formola di moltiplicazione complessa

$$\wp(\varepsilon u) = \varepsilon \wp u,$$

il confronto dei primi termini degli sviluppi di $\wp(\varepsilon u)$, $\varepsilon \wp u$ nell'intorno di $u = 0$ dà subito $g_2 = 0$ [1]). Siccome $J(\tau)$ sul contorno di T è sempre reale e non può mai riprendere due volte lo stesso valore, vediamo che nel tratto circolare da $\tau = \varepsilon$ a $\tau = i$ $J(\tau)$ andrà costantemente crescendo da 0 a 1, nel tratto rettilineo dell'asse immaginario da $\tau = i$ a $\tau = i\infty$ è sempre positivo e crescente a partire da $J = 1$, e nel tratto rettilineo $R(\tau) = -\frac{1}{2}$, da $\tau = \varepsilon$ a $\tau = -\frac{1}{2} + i\infty$, è sempre negativo e decrescente a partire da $J = 0$.

Volendo in fine esaminare come si comporta $J(\tau)$ in prossimità del vertice $\tau = \infty$, facciamo uso delle considerazioni seguenti.

Poichè $J(\tau)$ è funzione periodica di τ col periodo 1, $J(\tau + 1) = J(\tau)$, se poniamo

$$z = e^{2\pi i \tau}, \qquad \tau = \frac{1}{2\pi i} \log z,$$

sarà

$$J(\tau) = w(z)$$

una funzione di z esistente per tutti i valori di z di modulo $|z| < 1$ e sarà inoltre monodroma e regolare in tutti i punti della corri-

1) La medesima cosa, senza ricorrere alle proprietà delle $\wp$ lemniscatica ed equianarmonica, risulta direttamente dalla considerazione delle serie

$$\sum{}' \frac{1}{(m + n\tau)^6}, \qquad \sum{}' \frac{1}{(m + n\tau)^4}$$

la prima delle quali si annulla per $\tau = i$ e la seconda per $\tau = \varepsilon$, come si vede associando nel primo caso i numeri di Gauss quattro a quattro nel gruppo di numeri (associati)

$$m + ni, \quad i(m + ni), \quad i^2(m + ni), \quad i^3(m + ni)$$

e nel secondo i numeri $m + n\varepsilon$ tre a tre nel gruppo di numeri associati

$$m + n\varepsilon, \quad \varepsilon(m + n\varepsilon), \quad \varepsilon^2(m + n\varepsilon).$$

spondente area circolare, salvo che in $z = 0$. Quale specie di singolarità avrà $w(z)$ in $z = 0$? Non può essere una singolarità essenziale perchè nell'intorno di $z = 0$ $w(z)$ prenderebbe allora valori prossimi per es. ad 1 tanto quanto si vuole e $J(\tau)$, allontanandosi τ all'infinito entro la striscia

$$a = -\frac{1}{2}, \qquad a = +\frac{1}{2},$$

prenderebbe valori che $J(\tau)$ avrebbe già preso in prossimità di $\tau = i$, ciò che è assurdo.

Non può nemmeno $z = 0$ essere per $w(z)$ un polo d'ordine superiore al primo, giacchè allora, in prossimità di $z = 0$, $w(z)$ riprenderebbe due o più volte il medesimo valore e lo stesso accadrebbe per $J(\tau)$ entro la detta striscia a distanza grandissima. In fine non può darsi che $z = 0$ sia un punto regolare di $w(z)$, perchè allora $J(\tau)$, al crescere all'infinito dell'ordinata di τ, dovrebbe convergere verso un unico valore finito, ciò che è impossibile essendo $J(\tau)$, come si è visto, positivo e crescente sull'un lato rettilineo del triangolo fondamentale e negativo decrescente sull'altro. Se ne conclude che $w(z)$ si svilupperà per tutti i valori di z di modulo $|z| < 1$ così:

$$w(z) = \frac{A}{z} + a_0 + a_1 z + a_2 z^2 + \dots (A \neq 0),$$

e corrispondentemente avremo per $J(\tau)$ un'espressione analitica della forma

$$J(\tau) = A e^{-2\pi i\tau} + a_0 + a_1 e^{2\pi i\tau} + a_2 e^{4\pi i\tau} + \dots,$$

valevole per tutti i valori di τ d'ordinata positiva, cioè in tutto il campo di esistenza della funzione [1]). Nell'intorno di $\tau = \infty$, $J(\tau)$ si comporta dunque come $e^{-2\pi i\tau}$, e per ciò diciamo che $J(\tau)$ ha in $\tau = \infty$ una *singolarità logaritmica*. Una singolarità della medesima natura ha $J(\tau)$ in tutti i punti equivalenti, cioè nei punti razionali dell'asse reale, il che fa vedere appunto come il campo di esistenza di questa funzione analitica sia il semipiano positivo, l'asse reale essendo il limite del campo.

[1]) Ritorneremo più tardi su questo sviluppo di $J(\tau)$ per precisare la natura dei suoi coefficienti (vedi § 182).

§ 120. — Rappresentazione conforme del triangolo fondamentale sul semipiano.

Abbiamo già visto che, mentre τ percorre l'area del triangolo fondamentale T, il coefficiente dell'immaginario in $J(\tau)$ conserva sempre lo stesso segno, cioè, interpretando i valori di J nel suo piano complesso, $J(\tau)$ si muove in un semipiano. Per distinguere in quale, basta osservare che, percorrendo il contorno di T in verso positivo a partire per es. da $\tau = \varepsilon$, s'incontrano successivamente i vertici $\tau = \varepsilon$, $\tau = i$, $\tau = \infty$ e corrispondentemente $J(\tau)$ si muove sul suo asse reale in senso positivo. Dunque: *in tutto il triangolo fondamentale $J(\tau)$ ha sempre il coefficiente dell'immaginario positivo.*

Ora facilmente vediamo, per ragioni di continuità, che inversamente, fissato per J un valore qualunque J_0 di ordinata positiva (o nulla), vi è sempre uno (ed un solo) punto τ_0 di T ove $J(\tau)$ assume il valore prefissato J_0. Per dimostrare la cosa in tutto rigore possiamo usare le considerazioni seguenti. Per abbreviare diciamo valori α i valori J_0 che J prende effettivamente e valori β quei valori J_0 (se ne esistono) che J non può prendere. Vediamo subito che se J_0 è un valore α, un intorno sufficientemente piccolo di J_0 contiene tutti valori α (§ 57). Medesimamente dico che, se J_0 è un valore β, un intorno sufficientemente piccolo di J_0 conterrà tutti valori β. E infatti se, comunque piccolo si prendesse questo intorno, vi si trovassero sempre dei valori α, a ciascuno di questi punti corrisponderebbe un punto τ in T, e questi infiniti punti τ addensantisi in T, con ordinate minori di una quantità fissa [1]), avrebbero almeno un punto limite τ_0, ove $J(\tau)$ assumerebbe, a causa della continuità, precisamente il valore J_0, che sarebbe dunque un valore α. Ora sia J_0, se è possibile, un valore β_1 e J_1 un valore α, per es. lo zero; segniamo nel semipiano J il tratto rettilineo [2]) che unisce J_1 con J_0 e dividiamo i punti di questo tratto in due classi A, B attribuendo alla prima classe A quei punti J tali che il tratto da J_1 a J contenga tutti punti α, alla seconda B

[1]) Si ricordi che per τ crescente all'infinito, entro il triangolo fondamentale $J(\tau)$ cresce all'infinito come $e^{-2\pi i\tau}$.

[2]) Prendiamo per semplicità un tratto rettilineo che unisca J_0 con J_1 ma si potrebbe adoperare egualmente qualunque altra linea continua.

quelli tali che nel tratto $J_1\, J$ vi siano anche punti β. Questa divisione in due classi soddisfa alle condizioni fondamentali [1]) che assicurano l'esistenza di un punto limite $\bar{J}$ di separazione fra le due classi. Questo punto $\bar{J}$ sarebbe manifestamente un punto a; e allora, prolungando il tratto $J_1\, \bar{J}$ per un nuovo piccolo tratto, questo conterrebbe ancora tutti punti a, ciò che è assurdo.

Ne concludiamo: *Nell'interno del triangolo fondamentale T l'invariante assoluto $J(\tau)$ assume una ed una sola volta tutti i valori J_0 di ordinata positiva, e sul contorno tutti i valori reali da* $-\infty$ *a* $+\infty$.

Osserviamo inoltre che nell'interno del triangolo fondamentale ed anche sul contorno, i vertici esclusi, la derivata $\dfrac{dJ}{d\tau}$ non può mai annullarsi (nè diventare infinita); poichè nell'intorno di ogni punto, che non sia un vertice della rete modulare, $J(\tau)$ non prende che una sola volta i propri valori. Invece nell'intorno di $\tau = i$ e di tutti i punti equivalenti, $J(\tau)$ riprende *due* volte i valori prossimi ad 1, e perciò $J - 1$ diventa in $\tau = i$ infinitesimo del secondo ordine e $\dfrac{dJ}{d\tau}$ del primo. Similmente nell'intorno di $\tau = \varepsilon$ e dei vertici equivalenti, $J(\tau)$ riprende *tre* volte i valori prossimi a zero e perciò $J(\tau)$ diventa in $\tau = \varepsilon$ infinitesima del terzo ordine e $\dfrac{dJ}{d\tau}$ del secondo.

Dunque: *La funzione $J(\tau)$ dà la rappresentazione biunivoca conforme del triangolo fondamentale sul semipiano. Punti eccezionali della rappresentazione sono soltanto i vertici, ove gli angoli di* $\dfrac{\pi}{3}$, $\dfrac{\pi}{2}$, 0 *vengono cangiati in angoli piatti*.

Associando al triangolo fondamentale T il suo simmetrico rispetto all'asse immaginario, abbiamo il triangolo T fondamentale pel gruppo modulare Γ (§ 21); in esso $J(\tau)$ prende *una ed una sola volta* tutti i valori possibili, e soltanto in punti simmetrici del contorno riprende lo stesso valore. Questo modo di comportarsi della funzione automorfa $J(\tau)$ nel suo campo fondamentale è quindi, in un certo senso, più semplice di quello che offrono le funzioni ellittiche, le quali debbono nel parallelogrammo fondamentale riprendere due volte *almeno* il medesimo valore [2]).

[1]) DINI, *Fondamenti*, pag. 11.

[2]) L'intima ragione di questa differenza sta in ciò che il campo fondamentale di $J(\tau)$, quando s'immaginano saldati fra loro i lati corrispondenti in guisa da far coincidere i punti equivalenti, diventa una superficie chiusa di genere *zero*, mentre il parallelogrammo delle funzioni ellittiche dà una superficie chiusa di genere *uno* (toro).

§ 121. — La funzione inversa $\tau(J)$ e il teorema di Picard sulle trascendenti intere.

Consideriamo ora la funzione inversa dell'invariante assoluto $J(\tau)$, che si ottiene considerando τ come funzione di J. Nell'intorno di ogni valore J, differente da 0, 1, e ∞, si può, per quanto si è detto sopra, eseguire *univocamente* l'inversione, una volta scelto il valore τ_1 di τ, poichè lo sviluppo di $J - J_1$ per potenze di $\tau - \tau_1$ contiene effettivamente il termine colla prima potenza di $\tau - \tau_1$. Se $J_1 = 0$, allora τ_1 deve essere un vertice della rete equivalente a $\tau = \varepsilon$, e $\tau - \tau_1$, si sviluppa in serie di potenze di $J^{\frac{1}{3}}$ e così per $J_1 = 1$ in serie di potenze di $(J - 1)^{\frac{1}{2}}$ (cfr. § 58).

La rete modulare ci rappresenta chiaramente le proprietà fondamentali di questa funzione inversa $\tau(J)$, permettendoci di seguire, senza ambiguità, ogni suo prolungamento analitico. Fissiamo invero un valore iniziale J_1 di J, per es. nel semipiano positivo, al quale corrisponderà, in ogni triangolo non tratteggiato della rete modulare (Cap. II, § 20), un punto. Scegliamo per es. quello τ_1 appartenente al triangolo fondamentale 1 e prendiamo

$$\text{per } J = J_1, \qquad \tau = \tau_1.$$

Partendo da J_1, descriviamo con J un cammino chiuso qualunque, che, senza passare pei punti singolari $J = 0$, $J = 1$, $J = \infty$, ritorni in J_1. Lungo di esso potremo prolungare analiticamente la funzione senza alcuna ambiguità. Finchè il cammino considerato, partendo da J_1, rimane nel semipiano positivo, τ rimarrà sempre nel primo triangolo; ma appena J traversa l'asse reale τ entrerà in uno determinato dei tre triangoli tratteggiati aderenti al fondamentale e precisamente nel triangolo A, B o C (fig. 2, pag. 66, vol. I), secondo che J traversa l'asse reale nel tratto $1\,\infty$ o nel tratto $0\,\infty$, o in fine nel tratto $0\,1$. Fino ad un nuovo traversamento dell'asse reale, che riconduca J nel semipiano positivo, τ rimarrà nell'interno del nuovo triangolo; entrerà poi in un nuovo triangolo della rete perfettamente determinato al nuovo traversamento. Così seguitando si vede che, lungo tutto il cammino chiuso, τ avrà sempre un unico valore e, ritornato J in J_1, τ ritornerà o in τ_1 stesso, o in uno degli infiniti punti equivalenti $\frac{\alpha\tau_1+\beta}{\gamma\tau_1+\delta}$ rispetto al gruppo modulare. È chiaro poi che, inversamente, prendendo un conveniente cammino chiuso per J, possiamo far sì che τ, al ritorno, assuma uno qualunque degli infiniti valori equivalenti a τ_1.

Così adunque: *La funzione $\tau(J)$ è una funzione analitica infinitiforme, esistente in tutto il piano complesso J, i cui rami si ottengono tutti da uno di essi τ eseguendovi le sostituzioni del gruppo modulare. Ogni ramo è una funzione regolare di J in ogni punto distinto dai tre singolari $J=0$, $J=1$, $J=\infty$.*

Questi punti sono punti di diramazione, cioè girando attorno ad essi si permutano i rami della funzione. Precisamente un giro attorno a $J=0$ cangia τ in $-\frac{\tau+1}{\tau}$, per un giro attorno a $J=1$ τ si muta in $-\frac{1}{\tau}$ e infine un giro attorno a $J=\infty$ cangia τ in $\tau+1$ [1]).

Delle proprietà di questa funzione $\tau(J)$ Picard si è servito per dimostrare un teorema importante, che concerne il modo di comportarsi di una funzione nell'intorno di una singolarità essenziale [2]). Qui ci limitiamo al caso particolare di una trascendente intera $G(z)$ e dimostriamo: *Ogni trascendente intera prende a distanza finita tutti i valori finiti, eccettuato uno al più.*

Supponiamo che la trascendente intera $G(z)$ non prenda nè il valore finito A, nè il valore finito B; allora la trascendente intera

$$G_1(z)=\frac{G(z)-A}{B-A}$$

non prenderà nè il valore *zero*, nè il valore *uno*. Essendo $\tau(J)$ la funzione inversa dell'invariante assoluto sopra considerata, poniamo l'argomento $J=G_1(z)$ e studiamo la funzione di z

$$\varphi(z)=\tau(G_1(z)).$$

[1]) La rete modulare si può riguardare come una superficie Riemaniana ad infiniti fogli sulla quale vengono a trovarsi distese, in modo monodromo, le coppie di valori per J, τ legati dall'equazione trascendente $J=J(\tau)$; ciascun triangolo della rete del gruppo modulare rappresenta un foglio.

[2]) PICARD, *Traité d'Analyse* (3me edition), tome II, pag. 264.

Per fissare completamente questa funzione, basterà fissare che per un certo valore z_1 di z, fra gli infiniti valori corrispondenti di τ, se ne scelga uno determinato τ_1. Si otterrà così una funzione analitica $\varphi(z)$, regolare per ogni valore finito a di z, poichè per ipotesi

$$G_1(a)\neq 0,\ 1,\ \infty\ ;$$

la $\varphi(z)$ esiste dunque in tutto il piano complesso ed è regolare in ogni punto e perciò *monodroma*, come risulta da considerazioni del tutto simili a quelle che abbiamo sviluppato al § 77 per dimostrare il teorema fondamentale relativo ai rami di una funzione algebrica. Ne risulta che la $\varphi(z)=\tau[G_1(z)]$ sarebbe una trascendente intera col coefficiente dell'immaginario sempre positivo. Ma allora la trascendente intera $e^{i\varphi(z)}$ sarebbe di modulo sempre <1, ciò che è assurdo.

§ 122. — Esistenza della funzione $\wp(u;g_2,g_3)$ con invarianti assegnati.

Colle cognizioni delle proprietà fondamentali della funzione modulare $J(\tau)$, acquistate nei paragrafi precedenti, siamo ora in grado di stabilire l'importante teorema:

Nella funzione ellittica $\wp(u\mid\omega,\omega')$ si possono sempre assegnare ai periodi 2ω, $2\omega'$ tali valori che gli invarianti g_2, g_3 acquistino valori prefissati arbitrari γ_2, γ_3, purchè non sia nullo il discriminante

$$\Delta=\gamma_2^3-27\gamma_3^2.$$

Dai valori dati per g_2, g_3 calcoliamo infatti il corrispondente valore J_1 che dovrà avere l'invariante assoluto, e cioè

$$J_1=\frac{\gamma_2^3}{\gamma_2^3-27\gamma_3^2},$$

valore finito per ipotesi. Esisterà certamente nel triangolo fondamentale, o nel suo simmetrico rispetto all'asse immaginario, un valore τ_1 di τ, per il quale risulterà effettivamente

$$J(\tau_1)=J_1=\frac{\gamma_2^3}{\gamma_2^3-27\gamma_3^2}.$$

Essendo Ω una quantità per ora indeterminata, costruiamo la funzione ellittica $\wp(u \mid \Omega, \Omega\,\tau_1)$, il cui invariante assoluto sarà precisamente $= J_1$. Col processo stesso del § 118 si vede che si può sempre prendere Ω in guisa che gli invarianti g_2, g_3 della nostra $\wp\, u$ abbiano precisamente i valori assegnati γ_2, γ_3.

Nelle effettive applicazioni i valori dati degli invarianti sono sempre reali e reale è quindi pure il valore di J. Per i calcoli numerici, che si presentano nella pratica, basta quindi avere una tavola che permetta di seguire l'andamento numerico dell' invariante assoluto J lungo il contorno del triangolo fondamentale. Le tavole costruite da Legendre per il calcolo degli integrali ellittici nel suo *Traité des fonctions elliptiques* si prestano facilmente alla trasformazione richiesta.

Il risultato che abbiamo così conseguito può anche enunciarsi sotto altra forma, ricordando l'equazione differenziale cui soddisfa $\wp\, u$, e cioè:

$$\wp'^2 u = 4\,\wp^3 u - g_2\,\wp\, u - g_3 .$$

Possiamo dire infatti: *L'equazione differenziale del primo ordine*

$$\left(\frac{ds}{du}\right)^2 = 4\,s^3 - g_2\, s - g_3 \tag{4}$$

s'integra per mezzo della funzione ellittica $\wp\, u$, *qualunque siano i valori delle costanti* g_2, g_3, *purchè il polinomio di terzo grado in* s *del secondo membro non abbia fattori multipli.*

E infatti prendendo

$$s = \wp(u + C;\ \ g_2, g_3)$$

si ha l' integrale *generale* della (4).

Se si presenta il caso qui escluso

$$g_2^3 - 27\, g_3^2 = 0 ,$$

la quadratura

$$\int \frac{ds}{\sqrt{4\, s^3 - g_2\, s - g_3}}$$

che dobbiamo eseguire per integrare la (4), porta evidentemente ad un integrale della forma

$$\int \frac{ds}{(s-a)\,\sqrt{s-b}}$$

ovvero, ponendo $s - b = t^2$, all' integrale

$$\int \frac{2\,dt}{t^2 + k}$$

cioè ad un arco tangente (o ad un logaritmo), ed s, considerata come funzione del valore dell' integrale, è ancora una funzione monodroma, circolare (od iperbolica).

Propriamente dunque il caso

$$g_2^3 - 27\, g_3^2 = 0$$

non è un caso d'eccezione, ma soltanto un caso limite, ove la funzione $\wp\, u$ degenera in una funzione circolare (od iperbolica).

§ 123. — Equazione differenziale per le funzioni ellittiche del secondo ordine e problema d'inversione.

La funzione ellittica del secondo ordine $\wp(u\,;\, g_2\,,\, g_3)$ soddisfa all'equazione differenziale (4). Ora possiamo generalizzare questo risultato considerando una qualunque funzione ellittica *del secondo ordine* $w(u)$ e dimostrare che essa soddisfa ad un'equazione differenziale del primo ordine della forma

$$\left(\frac{dw}{du}\right)^2 = P(w) ,$$

dove $P(w)$ è un polinomio di terzo o quarto grado in w, secondo che $w(u)$ ha un solo infinito del secondo ordine nel parallelogrammo dei periodi, ovvero due infiniti staccati del primo ordine.

E infatti nel primo caso $\dfrac{dw}{du}$ sarà una funzione ellittica del terzo ordine, che avrà dunque tre infinitesimi del primo ordine, e, se indichiamo con w_1, w_2, w_3 i valori che assume w in questi tre infinitesimi di w', si vede subito che le due funzioni

$$\left(\frac{dw}{du}\right)^2, \quad (w - w_1)\ (w - w_2)\ (w - w_3)$$

hanno a comune periodi, infiniti ed infinitesimi, onde risulta appunto che si ha

$$\left(\frac{dw}{du}\right)^2 = A w^3 + B w^2 + C w + D, \tag{5}$$

essendo A, B, C, D costanti.

Se la $w(u)$ ha due infiniti del primo ordine, la sua derivata $\frac{dw}{du}$ è del quarto ordine, e un ragionamento analogo al precedente dimostra che si avrà allora

$$\left(\frac{dw}{du}\right)^2 = A w^4 + B w^3 + C w^2 + D w + E. \tag{6}$$

Le equazioni differenziali (5), (6) s' integrano evidentemente per funzioni ellittiche. Riesce ora ben naturale la domanda : *Dati arbitrariamente i polinomi di terzo o quarto grado nei secondi membri delle* (5), (6), *possono queste equazioni differenziali integrarsi per funzioni ellittiche ?*

In altre parole si chiede se è possibile determinare gli invarianti g_2, g_3 di una funzione $s = \wp u$ in guisa che l' integrale della (5) o della (6) possa porsi sotto la forma

$$w = F(\wp u, \wp' u) = F(s, \sqrt{4 s^3 - g_2 s - g_3}),$$

essendo F il simbolo di una funzione razionale nei due argomenti.

La questione così posta, alla quale è da rispondersi affermativamente, come ora dimostreremo, può anche formularsi nel modo seguente. Dalla (5) o (6) si trae

$$du = \frac{dw}{\sqrt{P(w)}},$$

essendo $P(w)$ un polinomio di terzo o quarto grado in w, e poichè, nell' ipotesi che la proprietà da dimostrarsi sussista, dobbiamo avere altresì con $s = \wp u$

$$du = \frac{ds}{\sqrt{4 s^3 - g_2 s - g_3}},$$

possiamo dare al nostro problema la seguente forma algebrica : *Ponendo w eguale ad una conveniente funzione razionale di s e di $\sqrt{4 s^3 - g_2 s - g_3}$, è possibile trasformare il differenziale* (*ellittico*)

$$\frac{dw}{\sqrt{P(w)}}$$

nella forma normale di Weierstrass

$$\frac{ds}{\sqrt{4 s^3 - g_2 s - g_3}}\ ?$$

Ciò è possibile, come si vedrà, in infiniti modi, fra i quali ne sceglieremo due più semplici e adatti agli scopi pratici.

Il problema qui enunciato porta il nome di *problema d' inversione*. Colla sua risoluzione noi veniamo invero a dimostrare che nell' integrale ellittico (di prima specie)

$$u = \int_a^w \frac{dw}{\sqrt{P(w)}},$$

considerando il limite superiore w come funzione del valore u dell' integrale, si ha una funzione uniforme di u doppiamente periodica, cioè una funzione ellittica.

§ 124. — Primo metodo d'inversione per mezzo di una sostituzione lineare.

Cominciamo dal caso in cui il polinomio $P(w)$ è di terzo grado e scriviamo, con coefficienti binomiali :

$$P(w) = a_0 w^3 + 3 a_1 w^2 + 3 a_2 w + a_3 .$$

In tal caso la trasformazione del differenziale ellittico $\frac{dw}{\sqrt{P(w)}}$, nella forma normale di Weierstrass

$$\frac{ds}{\sqrt{4 s^3 - g_2 s - g_3}}$$

si può fare nel modo più semplice con una sostituzione lineare intera

$$w = a + b s, \tag{7}$$

ciò che equivale a prendere per w (§ 123) una funzione ellittica di secondo ordine cogli infiniti stessi di $\wp u$. Colla sostituzione (7) si ha:

$$\frac{dw}{\sqrt{P(w)}} = \frac{b\,ds}{\sqrt{P(a+bs)}} =$$

$$= \frac{ds}{\sqrt{\frac{1}{b^2}\left\{P(a) + bs\,P'(a) + \frac{b^2 s^2}{2} P''(a) + \frac{b^3 s^3}{6} P'''(a)\right\}}} .$$

Basterà dunque disporre di a, b in guisa che sia

$$P'(a) = 0\,, \qquad b = \frac{24}{P'''(a)} .$$

Si ha dunque il risultato: *Il differenziale ellittico*

$$\frac{dw}{\sqrt{a_0 w^3 + 3a_1 w^2 + 3a_2 w + a_3}} ,$$

per mezzo della sostituzione lineare

$$w = -\frac{a_1}{a_0} + \frac{4}{a_0} s ,$$

si riduce alla forma normale di Weierstrass

$$\frac{ds}{\sqrt{4s^3 - g_2 s - g_3}} .$$

Passiamo ora al caso in cui $P(w)$ sia del quarto grado:

$$P(w) = a_0 w^4 + 4a_1 w^3 + 6a_2 w^2 + 4a_3 w + a_4 ;$$

in questo caso potremo raggiungere lo scopo ancora con una sostituzione lineare, ma frazionaria in luogo che intera, cioè della forma

(8) $$w = a + \frac{b}{s - c}\ [1]).$$

[1]) Ciò equivale a prendere per w (§ 123) una funzione ellittica del secondo ordine, i cui infiniti siano in due punti a, $2\omega + 2\omega' - a$ del parallelogrammo dei periodi.

Per meglio intendere il significato dei calcoli seguenti conviene ricorrere a variabili omogenee, scindendo w nel quoziente di due nuove variabili w_1, w_2:

$$w = \frac{w_1}{w_2}$$

e scrivendo quindi il differenziale ellittico sotto la forma omogenea

$$\frac{dw}{\sqrt{P(w)}} = \frac{w_2\,dw_1 - w_1\,dw_2}{\sqrt{a_0 w_1^4 + 4a_1 w_1^3 w_2 + 6a_2 w_1^2 w_2^2 + 4a_3 w_1 w_2^3 + a_4 w_2^4}} ,$$

dove attualmente sotto il segno radicale figura una *forma biquadratica*.

È ben noto che una tale forma possiede due *invarianti* S, T l'uno di secondo, l'altro di terzo grado nei coefficienti; le loro espressioni effettive sono:

(9) $$\left\{\begin{aligned} S &= a_0 a_4 + 3a_2^2 - 4a_1 a_3 \\ T &= \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix} = a_0 a_2 a_4 - a_0 a_3^2 + 2a_1 a_2 a_3 - a_1^2 a_4 - a_2^3 . \end{aligned}\right.$$

Eseguendo ora sulle variabili w_1, w_2 una sostituzione lineare

(10) $$\left\{\begin{aligned} w_1 &= b_1 s_1 + b_2 s_2 \\ w_2 &= c_1 s_1 + c_2 s_2 \end{aligned}\right.$$

e indicando con

$$a'_0 s_1^4 + 4a'_1 s_1^3 s_2 + \dots + a'_4 s_2^4$$

la forma trasformata, sarà evidentemente

$$\frac{w_2\,dw_1 - w_1\,dw_2}{\sqrt{a_0 w_1^4 + \dots + a_4 w_2^4}} = \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix} \frac{s_2\,ds_1 - s_1\,ds_2}{\sqrt{a'_0 s_1^4 + \dots + a'_4 s_2^4}}$$

Se ora disponiamo dei quattro coefficienti nella (10) in guisa che risulti

$$b_1 c_2 - b_2 c_1 = 1\,, \quad a'_0 = 0\,, \quad a'_1 = 1\,, \quad a'_2 = 0\,,$$

indi poniamo

$$g_2 = -4\,a'_3\,, \quad g_3 = -a'_4\,,$$

vediamo dalle (9) che g_2, g_3 saranno precisamente gli invarianti S', T' della trasformata e sarà per ciò

$$g_2 = S\,, \quad g_3 = T\,.$$

Restituendo le variabili non omogenee, otterremo

$$\frac{d\,w}{\sqrt{P\,(w)}} = \frac{d\,s}{\sqrt{4\,s^3 - g_2\,s - g_3}}\,,$$

mediante la sostituzione lineare

$$w = \frac{b_1\,s + b_2}{c_1\,s + c_2}\,.$$

Resta dunque soltanto che vediamo come si possono determinare i coefficienti a, b, c nella (8) in guisa da raggiungere lo scopo prefisso. Per ciò osserviamo che si ha colla sostituzione (8)

$$\frac{d\,w}{\sqrt{P\,(w)}} = -\frac{d\,s}{\sqrt{\dfrac{(s-c)^4}{b^2}\,P\left(a + \dfrac{b}{s-c}\right)}} = -\frac{d\,s}{\sqrt{P_1\,(s)}}\,,$$

ove si ponga

$$P_1\,(s) = \frac{(s-c)^4}{b^2}\,P\,(a) + \frac{(s-c)^3}{b}\,P'(a) + \frac{(s-c)^2}{2}\,P''\,(a) +$$

$$+ \frac{b\,(s-c)}{6}\,P'''(a) + \frac{b^2}{24}\,P^{\mathrm{IV}}\,(a)\,.$$

Basterà determinare a, b, c per modo che si abbia

$$P\,(a) = 0\,, \quad \frac{P'(a)}{b} = 4, \quad \frac{-3\,c}{b}\,P'(a) + \frac{P''(a)}{2} = 0,$$

ossia

$$P\,(a) = 0\,, \quad b = \frac{1}{4}\,P'\,(a), \quad c = \frac{1}{24}\,P''\,(a)\,.$$

Abbiamo dunque il risultato: *Per ridurre il differenziale ellittico*

$$\frac{d\,w}{\sqrt{P\,(w)}} = \frac{d\,w}{\sqrt{a_0\,w^4 + 4\,a_1\,w^3 + 6\,a_2\,w^2 + 4\,a_3\,w + a_4}}$$

alla forma normale di Weierstrass

$$\frac{d\,s}{\sqrt{4\,s^3 - g_2\,s - g_3}}$$

basta porre

$$w = a + \frac{\dfrac{1}{4}\,P'(a)}{s - \dfrac{1}{24}\,P''\,(a)} \tag{11}$$

essendo a una radice qualunque del polinomio di quarto grado $P\,(w)$. Gli invarianti g_2, g_3 risulteranno eguali ai due invarianti S, T di $P\,(w)$ e cioè:

$$\left\{\begin{aligned} g_2 &= a_0\,a_4 + 3\,a_2^2 - 4\,a_1\,a_3 \\ g_3 &= \begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix}\,. \end{aligned}\right. \tag{12}$$

Così resta giustificata, anche dal punto di vista algebrico, la denominazione di *invarianti* data a g_2, g_3.

È da osservarsi che, mentre nel caso in cui $P\,(w)$ è di terzo grado, i coefficienti della sostituzione da eseguirsi dipendono *razionalmente* dai coefficienti di $P\,(w)$, attualmente ne dipendono irrazionalmente, esprimendosi per una radice di $P\,(w) = 0$, che bisogna supporre nota. Però, ed è questo un punto essenziale, ove la funzione $\wp\,u$ di Weierstrass ha già un rilevante vantaggio su quelle di Jacobi, *gli invarianti g_2, g_3 della $\wp\,u$ si calcolano sempre razionalmente, come invarianti della forma biquadratica.*

§ 125. — Secondo metodo d' inversione.

Nei casi pratici il polinomio $P(w)$ è a coefficienti reali e però anche gli invarianti g_2, g_3 sono reali. Se non si conosce alcuna radice di $P(w) = 0$, ovvero, essendo queste tutte immaginarie, si vuole evitare nelle formole d' inversione d' introdurle esplicitamente, converrà meglio ricorrere al *secondo metodo d' inversione*, che ora passiamo ad esporre.

Essendo v un valore fisso dell'argomento, prendiamo per ciò a considerare la funzione ellittica del secondo ordine

$$y = \frac{1}{2} \frac{\wp' u - \wp' v}{\wp u - \wp v},$$

che abbiamo visto figurare nelle formole d'addizione (§ 106) e proponiamoci di costruire effettivamente il polinomio di quarto grado in y che eguaglia $\left(\frac{dy}{du}\right)^2$ [1]). Per ciò osserviamo che dalla formola (V) d'addizione (pag. 39) si ha

$$\wp(u+v) + \wp u + \wp v = y^2,$$

ossia

$$y^2 - 3\wp v = [\wp(u+v) - \wp v] + [\wp u - \wp v]. \tag{13}$$

La formola (III) (pag. 38) ci dà

$$\wp(u+v) - \wp v = -\frac{1}{2} \frac{\partial}{\partial v} \frac{\wp' u - \wp' v}{\wp u - \wp v} =$$

$$= \frac{1}{2} \frac{\wp'' v}{\wp u - \wp v} - \frac{1}{2} \frac{\wp' u - \wp' v}{(\wp u - \wp v)^2} \wp' v$$

e moltiplicando per $2(\wp u - \wp v)$ risulta

$$\wp'' v - 2y\wp' v = 2[\wp(u+v) - \wp v][\wp u - \wp v].$$

1) Che debba essere un polinomio di quarto (e non di terzo) grado in u risulta da ciò che la y ha due infiniti del primo ordine staccati, l' uno in $u = 0$, l'altro in $u = -v$.

Quadrando la (13) e sottraendovi il doppio di quest' ultima, si ottiene

$$(y^2 - 3\wp v)^2 + 2(2y\wp' v - \wp'' v) = [\wp(u+v) - \wp u]^2.$$

D'altronde, per la citata formola d'addizione (III), si ha

$$\wp(u+v) - \wp u = -\frac{dy}{du},$$

onde troviamo per la formola cercata

$$\left(\frac{dy}{du}\right)^2 = (y^2 - 3\wp v)^2 + 2(2y\wp' v - \wp'' v),$$

che, sostituendo per $\wp'' v$ la sua espressione $6\wp^2 v - \frac{1}{2} g^2$, diventa:

$$\left(\frac{dy}{du}\right)^2 = y^4 - 6\wp v\, y^2 + 4\wp' v\, y + g_2 - 3\wp^2 v. \tag{14}$$

Dopo ciò è molto facile ridurre una qualunque equazione differenziale (6)

$$\left(\frac{dw}{du}\right)^2 = a_0 w^4 + 4a_1 w^3 + 6a_2 w^2 + 4a_3 w + a_3 \tag{15}$$

a questa particolare forma (14) mediante una sostituzione lineare intera

$$w = A + By.$$

Si cominci infatti, colla nota sostituzione

$$w = -\frac{a_1}{a_0} + w_1,$$

a far sparire dal secondo membro di (15) il termine in w_1^3, dopo di che potremo scrivere

$$\left(\frac{dw_1}{du}\right)^2 = a_0 w_1^4 + 6a'_2 w_1^2 + 4a'_3 w_1 + a'_4. \tag{15*}$$

Gli invarianti S', T' di questo polinomio saranno gli stessi che in (15) e sarà perciò

$$a_0 a'_4 + 3a'^2_2 = S, \quad a_0 a'_2 a'_4 - a_0 a'^2_3 - a'^3_2 = T.$$

Ora, posto

$$w_1 = B\,y\,,$$

dobbiamo ridurre la (15*) alla (14), determinando convenientemente

$$B\,,\ g_2\,,\ g_3\,,\ v.$$

Dal confronto dei coefficienti nella supposta identità

$$B^2\left\{y^4 - 6\,\wp v\,.\,y^2 + 4\,\wp' v\,.\,y + g_2 - 3\,\wp^2 v\right\} =$$
$$= a_0 B^4 y^4 + 6\,a'_2 B^2 y^2 + 4\,a'_3 B\,y + a'_4$$

deduciamo

$$(16)\qquad B = \frac{1}{\sqrt{a_0}},\ \wp v = -a'_2\,,\ \wp' v = a'_3\sqrt{a_0},\ g_2 - 3\,\wp^2 v = a'_4\,a_0$$

e, poichè deve essere

$$\wp'^2 v = 4\,\wp^3 v - g_2\,\wp v - g_3\,,$$

otteniamo per gli invarianti i valori

$$g_2 = S,\quad g_3 = T\,,$$

dopo di che le (16) si riducono alle relazioni concordanti

$$\wp v = -a'_2\,,\quad \wp' v = a'_3\sqrt{a_0}$$

cioè

$$\wp v = \frac{a_1^2 - a_0 a_2}{a_0}\,,\quad \wp' v = \frac{2\,a_1^3 - 3\,a_0 a_1 a_2 + a_0^2 a_3}{a_0\sqrt{a_0}}\,.$$

Possiamo dunque formulare il risultato dei nostri calcoli col seguente teorema: *Per integrare l'equazione differenziale*

$$\left(\frac{dw}{du}\right)^2 = a_0 w^4 + 4\,a_1 w^3 + 6\,a_2 w^2 + 4\,a_3 w + a_4$$

per funzioni ellittiche, costruiscasi la funzione $\wp$ di Weierstrass cogli invarianti

$$\begin{cases} g_2 = S = a_0 a_4 + 3\,a_2^2 - 4\,a_1 a_3 \\ g_3 = T = a_0 a_2 a_4 - a_0 a_3^2 + 2\,a_1 a_2 a_3 - a_1^2 a_4 - a_2^3 \end{cases}$$

e determinando l'argomento costante v dalle relazioni concordanti

$$\wp v = \frac{a_1^2 - a_0 a_2}{a_0}\,,\qquad \wp' v = \frac{2\,a_1^3 - 3\,a_0 a_1 a_2 + a_0^2 a_3}{a_0\sqrt{a_0}}\,,$$

si avrà

$$\begin{cases} w = -\dfrac{a_1}{a_0} + \dfrac{1}{2\sqrt{a_0}}\,\dfrac{\wp' u - \wp' v}{\wp u - \wp v} \\[2ex] \dfrac{dw}{du} = \dfrac{1}{\sqrt{a_0}}\,(\wp u - \wp(u+v)). \end{cases}$$

In questo secondo modo d'inversione non si richiede la previa risoluzione dell'equazione di quarto grado $P(w) = 0$, anzi è chiaro come ne risulti *la risoluzione dell'equazione di quarto grado stessa per funzioni ellittiche.* E infatti il binomio

$$\wp u - \wp(u + v)$$

si annulla evidentemente per tutti e soli i valori u della forma

$$u = -\frac{v}{2} + m\,\omega + n\,\omega' \quad (m, n \text{ interi})$$

e però le radici dell'equazione di quarto grado saranno date dalla formola

$$w = -\frac{a_1}{a_0} - \frac{1}{2\sqrt{a_0}}\,\frac{\wp'\left(\dfrac{v}{2} + m\,\omega + n\,\omega'\right) + \wp' v}{\wp\left(\dfrac{v}{2} + m\,\omega + n\,\omega'\right) - \wp v}$$

dove basterà dare ad (m, n) i quattro valori di un sistema completo di coppie (mod 2), per es. (0, 0), (0, 1), (1, 0), (1, 1).

§ 126. — Integrazione delle funzioni razionali di una variabile w e di $\sqrt{P(w)}$

Coll'uno o coll'altro metodo d'inversione sopra discussi siamo in grado di risolvere il problema:

Dato un polinomio di terzo o quarto grado $P(w)$, esprimere contemporaneamente la variabile w e il radicale $\sqrt{P(w)}$ per funzioni ellittiche di un parametro ausiliario u.

A questo punto possiamo risolvere completamente il problema, che ha dato storicamente origine alla teoria delle funzioni ellittiche (§ 93) e cioè:

Essendo $F(w, \sqrt{P(w)})$ una funzione razionale di w e della radice quadrata di un polinomio $P(w)$ di terzo o quarto grado in w, eseguire la quadratura

$$J = \int F(w, \sqrt{P(w)})\, dw. \tag{17}$$

Introducendo il parametro ausiliario u, l'integrale precedente diventa evidentemente

$$J = \int F_1(\wp u, \wp' u)\, du,$$

dove F_1 è una funzione razionale di $\wp u$, $\wp' u$, cioè una funzione ellittica. La questione proposta si riduce dunque all'altra di trovare l'integrale di una funzione generale ellittica $f(u)$. Si vede subito che un tale integrale dà luogo ad una funzione ellittica aumentata di termini della forma

$$\log \sigma(u - v), \qquad \zeta(u - v).$$

E infatti, se decomponiamo la nostra funzione ellittica $f(u)$ in elementi semplici secondo la formola (I) (pag. 37)

$$f(u) = C + \sum \Big\{ A_0 \zeta(u - \beta) + A_1 \wp(u - \beta) + \frac{A_2}{2} \wp'(u - \beta) + \frac{A_3}{6} \wp''(u - \beta) + \dots \Big\},$$

otteniamo immediatamente

$$J = \int f(u)\, du = Cu + \sum A_0 \log \sigma(u - \beta) - \sum A_1 \zeta(u - \beta) + \psi(\wp u, \wp' u), \tag{18}$$

essendo ψ razionale in $\wp u$, $\wp' u$, cioè una funzione ellittica.

L'introduzione nell'analisi delle funzioni

$$\sigma u, \quad \zeta u, \quad \wp u,$$

o insomma dell'unica funzione σu, permette di eseguire tutte le quadrature (17).

Si osserverà che l'integrale ellittico (18), oltre l'argomento esplicito u e la parte periodica $\psi(\wp u, \wp' u)$, contiene anche le due parti non periodiche

$$\sum A_0 \log \sigma(u - \beta), \qquad \sum A_1 \zeta(u - \beta).$$

In casi particolari possono però queste parti sparire. Ciò accade per la prima quando tutti i residui di $f(u)$ sono nulli, quando cioè l'integrale Abeliano (17) è di prima categoria (cfr. § 90), e perchè sparisca anche la seconda basterà che sia $\Sigma A_1 = 0$, come risulta dalle formole

$$\zeta(u + 2\omega) = \zeta u + 2\eta, \qquad \zeta(u + 2\omega') = \zeta u + 2\eta'$$

ovvero anche dalla formola d'addizione per la ζu.

Un altro caso interessante si presenta quando, essendo sempre $\Sigma A_1 = 0$, i residui A_0 sono tali che il prodotto

$$\Pi [\sigma(u - \beta)]^{A_0}$$

sia una funzione ellittica, cioè razionale in $\wp u$, $\wp' u$. Allora il secondo membro della (18), prescindendo dal termine lineare in u, consta di una funzione razionale di $\wp u$, $\wp' u$ e del logaritmo di una tale funzione razionale.

§ 127. — Integrali normali ellittici delle tre specie secondo Weierstrass.

Ogni integrale J della forma (17) dicesi un *integrale ellittico*. Diciamo qui di passaggio che sotto questa denominazione si comprendono, più in generale, tutti gli integrali della forma

$$J = \int F(x, y)\, dx,$$

dove le variabili x, y siano legate da un'equazione algebrica

$$f(x, y) = 0$$

di genere uno. Si perverrebbe, nel modo del § 123, a queste più generali relazioni ellittiche, considerando una generale funzione ellittica w, che è appunto legata alla sua derivata w' da un'equazione algebrica di genere uno (o zero). Ma nel modo da noi scelto per lo sviluppo della teoria volgiamo specialmente l'attenzione ai particolari integrali ellittici (17). Se osserviamo che nella formola (18) si ha $\Sigma A_0 = 0$, vediamo che si può scrivere

$$\sum A_0 \log \sigma(u - \beta) = \sum A_0 \log \frac{\sigma(\beta - u)}{\sigma\beta\,\sigma u} + B,$$

essendo B una costante. D'altronde per la formola d'addizione della ζ

$$\zeta(u - \beta) = \zeta u - \zeta\beta + \frac{\wp' u + \wp'\beta}{\wp u - \wp\beta},$$

e possiamo quindi scrivere la (18) così:

$$J = \int f(u)\,du = Cu - \left(\sum A_1\right)\zeta u + \tag{18*}$$

$$+ \sum A_0 \log \frac{\sigma(\beta - u)}{\sigma\beta\,\sigma u} + \psi(u),$$

dove $\psi(u)$ è una nuova funzione ellittica. Ora, se poniamo

$$s = \wp u, \qquad \text{indi} \qquad \sqrt{4s^3 - g_2 s - g_3} = \wp' u,$$

vediamo che l'integrale generale ellittico

$$J = \int F(s, \sqrt{4s^3 - g_2 s - g_3})\,ds$$

si compone con termini delle seguenti quattro specie:

1° di una parte razionale in s e $\sqrt{4s^3 - g_2 s - g_3}$;

2° dell'integrale ellittico

$$u = \int \frac{ds}{\sqrt{4s^3 - g_2 s - g_3}}; \tag{A}$$

3° dell'integrale

$$\zeta u = \frac{\sigma' u}{\sigma u} = \int \frac{s\,ds}{\sqrt{4s^3 - g_2 s - g_3}}, \tag{B}$$

4° di un certo numero di termini della forma

$$\log \frac{\sigma(\beta - u)}{\sigma\beta\,\sigma u} = \int \frac{1}{2}\,\frac{\wp' u + \wp'\beta}{\wp u - \wp\beta}\,du - \frac{\sigma'\beta}{\sigma\beta}\,u + C;$$

ossia, prescindendo dal secondo termine, che è della forma (A), di integrali ellittici della forma

$$\int \frac{1}{2}\,\frac{\wp' u + \wp'\beta}{\wp u - \wp\beta}\,du. \tag{C}$$

Gli integrali ellittici (A), (B), (C) sono quelli che Weierstrass indica come integrali (elementari) di *prima*, *seconda* e *terza* specie rispettivamente [1]).

Come si vede: *Un integrale ellittico si compone di una parte razionale e di integrali elementari di prima, seconda e terza specie.*

[1]) Queste denominazioni corrispondono appunto a quelle in uso nella teoria generale degli integrali Abeliani (cfr. § 90). *Sulla superficie Riemanniana a due fogli per l'equazione algebrica*

$$y^2 = 4s^3 - g_2 s - g_3$$

l'integrale (A) è sempre finito, i suoi periodi fondamentali sono 2ω, $2\omega'$; l'integrale (B) ha un solo polo del primo ordine in $s = \infty$ (che è altresì punto di diramazione); l'integrale (C) ha due infiniti logaritmici in $s = \infty$ e $s = \wp\beta$, $y = \wp'\beta$ coi residui $-1 + 1$.

CAPITOLO XII.

Le tre funzioni σ pari di Weierstrass e le funzioni ellittiche di Jacobi sn v, cn v, dn v. — **Il quadrato k^2 del modulo come funzione modulare. — Formole d'addizione per** sn v, cn v, dn v.

§ 128. — Funzioni periodiche appartenenti a sottogruppi del gruppo modulare.

Una delle proprietà fondamentali delle funzioni di Weierstrass σu, $\wp u$, considerate come dipendenti dai periodi, è espressa dalle formole

$$\sigma(u \mid \alpha\omega+\beta\omega', \quad \gamma\omega+\delta\omega') = \sigma(u \mid \omega, \omega')$$
$$\wp(u \mid \alpha\omega+\beta\omega', \quad \gamma\omega+\delta\omega') = \wp(u \mid \omega, \omega'),$$

essendo

$$\begin{pmatrix} \alpha\omega+\beta\omega' & \gamma\omega+\delta\omega' \\ \omega & \omega' \end{pmatrix}$$

una qualunque sostituzione del gruppo modulare omogeneo. Il seguito della teoria ci conduce a considerare delle funzioni periodiche di prima o terza categoria (§ 101), che ammettono i periodi 2ω, $2\omega'$ o loro multipli [1]) e, senza rimanere invariate per tutte le sostituzioni $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare, tali rimangono per quelle di un sottogruppo *d' indice finito*.

Fra i sottogruppi del gruppo modulare si considerano specialmente i *sottogruppi congruenziali* (*Congruenzuntergruppen*), che sono cioè definiti da congruenze cui debbono soddisfare i coefficienti α, β, γ, δ rispetto ad un dato modulo n. I sottogruppi di

[1]) Naturalmente, se si tratta di funzioni periodiche di terza (o seconda) categoria, la periodicità s' intende soltanto relativa ai loro infiniti ed infinitesimi.

questa specie sono sempre contenuti nel sottogruppo *principale* Γ_n definito dalle congruenze

$$\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0 \\ 0, & 1\end{pmatrix} \pmod{n} \text{ [1])},$$

che contiene tutte le sostituzioni congrue coll' identità (mod n) ed hanno tutti indice finito. I sottogruppi principali Γ_n sono inoltre *invarianti* nel gruppo modulare.

Le funzioni periodiche appartenenti al sottogruppo Γ_n si diranno della n^{ma} specie (Stufe secondo Klein). In questo senso le σu, $\wp u$ appartengono alla prima specie. Nel caso seguente $n = 2$ rientrano le funzioni classiche di Jacobi

$$\text{sn}\, v, \quad \text{cn}\, v, \quad \text{dn}\, v.$$

Storicamente adunque lo studio delle funzioni ellittiche di seconda specie ha preceduto quello delle più semplici di prima specie (della $\wp u$). Arriveremo alle funzioni di Jacobi costruendo prima tre funzioni periodiche di terza categoria e di seconda specie introdotte da Weierstrass, le così dette *funzioni sigma pari*. Per ciò conviene innanzi tutto partire dalle considerazioni seguenti. Rispetto al modulo 2 le sostituzioni $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare Γ si ripartiscono nelle 6 classi seguenti:

$$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1,0 \\ 0,1\end{pmatrix}, \begin{pmatrix}0,1 \\ 1,0\end{pmatrix}, \begin{pmatrix}1,1 \\ 0,1\end{pmatrix}, \begin{pmatrix}1,1 \\ 1,0\end{pmatrix}, \begin{pmatrix}0,1 \\ 1,1\end{pmatrix}, \begin{pmatrix}1,0 \\ 1,1\end{pmatrix} \pmod{2}.$$

Quelle della prima classe formano appunto il sottogruppo Γ_2 e la ripartizione superiore in 6 classi corrisponde precisamente alla ripartizione delle sostituzioni di Γ rispetto a quelle del sottogruppo Γ_2, il quale adunque è in Γ un *sottogruppo* (*invariante*) *d' indice* 6.

Per ogni sostituzione di Γ

$$(1) \qquad \begin{cases} \Omega' = \alpha\omega'+\beta\omega \\ \Omega = \gamma\omega'+\delta\omega \end{cases}$$

[1]) Che le sostituzioni di questa specie formino gruppo risulta subito dalla legge di composizione delle loro sostituzioni.

si ha

$$\wp(u \mid \omega, \omega') = \wp(u, \Omega, \Omega')$$

e perciò le radici e_1, e_2, e_3 dell'equazione cubica

$$4e^3 - g_2 e - g_3 = 0,$$

che abbiamo definite colle formole

$$e_1 = \wp\,\omega, \quad e_2 = \wp(\omega + \omega'), \quad e_3 = \wp\,\omega',$$

per qualsiasi sostituzione (1) $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ di Γ non potranno che per mutarsi fra loro. Per vedere come si permutano, poniamo

$$e'_1 = \wp\,\Omega, \quad e'_2 = \wp(\Omega + \Omega'), \quad e_3 = \wp\,\Omega'$$

e distinguendo, come sopra, le sostituzioni $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ in 6 classi rispetto al sottogruppo Γ_2, potremo subito costruire la tabella seguente:

(A)

	Sostituzioni sopra $e_1\, e_2\, e_3$
$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0 \\ 0, 1\end{pmatrix} \pmod 2;\ e'_1 = e_1,\ e'_2 = e_2,\ e'_3 = e_3$	1
$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}0, 1 \\ 1, 0\end{pmatrix} \pmod 2;\ e'_1 = e_3,\ e'_2 = e_2,\ e'_3 = e_1$	$(e_1\, e_3)$
$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 1 \\ 0, 1\end{pmatrix} \pmod 2;\ e'_1 = e_1,\ e'_2 = e_3,\ e'_3 = e_2$	$(e_2\, e_3)$
$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 1 \\ 1, 0\end{pmatrix} \pmod 2,\ e'_1 = e_3,\ e'_2 = e_1,\ e'_3 = e_2$	$(e_1\, e_3\, e_2)$
$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}0, 1 \\ 1, 1\end{pmatrix} \pmod 2;\ e'_1 = e_2,\ e'_2 = e_3,\ e'_3 = e_1$	$(e_1\, e_2\, e_3)$
$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0 \\ 1, 1\end{pmatrix} \pmod 2;\ e'_1 = e_2,\ e'_2 = e_1,\ e'_3 = e_3$	$(e_1\, e_2)$

Come si vede, le sostituzioni $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ di Γ inducono sopra e_1, e_2, e_3 le 6 sostituzioni del gruppo totale su 3 elementi.

§ 129. — Le tre funzioni $\sigma_r\, u$.

Le tre funzioni $\sigma_r\, u$ pari si deducono dalla σu in modo semplice, aumentando l'argomento u della σ di uno dei semiperiodi

$$\omega, \quad \omega + \omega', \quad \omega'.$$

Per maggior simmetria poniamo

$$\omega_1 = \omega, \quad \omega_2 = \omega + \omega', \quad \omega_3 = \omega'$$

e analogamente

$$\eta_1 = \eta, \quad \eta_2 = \eta + \eta', \quad \eta_3 = \eta',$$

sicchè in generale

$$\eta_r = \zeta\,\omega_r \quad (r = 1, 2, 3).$$

Dalla formola fondamentale (VI) (pag. 17) per la σu si deduce che per un valore qualunque dell' indice r è

$$\sigma(u + 2\omega_r) = -e^{2\eta_r(u + \omega_r)}\,\sigma u,$$

nella qual formola, cangiando u in $u - \omega_r$, otteniamo

$$e^{-\eta_r u}\,\sigma(u + \omega_r) = e^{\eta_r u}\,\sigma(\omega_r - u).$$

La funzione

$$C e^{-\eta_r u}\,\sigma(u + \omega_r)$$

è adunque una funzione pari; se diamo alla costante C un tale valore che per $u = 0$ la funzione assuma il valore 1, avremo precisamente la funzione che Weierstrass indica col simbolo $\sigma_r\, u$. Avremo dunque per definizione

$$\text{(I)} \qquad \sigma_r\, u = e^{-\eta_r u}\,\frac{\sigma(u + \omega_r)}{\sigma\,\omega_r} = e^{\eta_r u}\,\frac{\sigma(\omega_r - u)}{\sigma\,\omega_r}$$

e dando ad r i suoi tre valori sarà

$$(\mathrm{I}^*) \qquad \sigma_1 u = e^{-\eta u}\,\frac{\sigma(u+\omega)}{\sigma\omega}\,, \quad \sigma_2 u = e^{-(\eta+\eta')u}\,\frac{\sigma(u+\omega+\omega')}{\sigma(\omega+\omega')}\,,$$

$$\sigma_3 u = e^{-\eta' u}\,\frac{\sigma(u+\omega')}{\sigma\omega'}\,.$$

Possiamo dimostrare subito che le σ pari, che sono evidentemente funzioni di terza categoria, appartengono precisamente al sottogruppo Γ_2 nel senso del paragrafo precedente. E invero dalla formola

$$\wp u - \wp \omega_r = \frac{\sigma(\omega_r - u)\,\sigma(\omega_r + u)}{\sigma^2\omega_r\,\sigma^2 u}\,,$$

che per la (I) può scriversi

$$(2) \qquad \wp u - \wp \omega_r = \frac{\sigma_r^2 u}{\sigma^2 u}\,,$$

risulta intanto evidente che, per qualunque sostituzione $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ di Γ sui periodi, i quadrati delle σ_r

$$\sigma_1^2 u\,, \quad \sigma_2^2 u\,, \quad \sigma_3^2 u$$

si permutano fra loro al modo stesso di

$$e_1\,, \quad e_2\,, \quad e_3$$

nella tabella (A). Ma poichè per $u = 0$ tutte e tre le funzioni σ_r riduconsi $= 1$, è chiaro che anche

$$\sigma_1 u\,, \quad \sigma_2 u\,, \quad \sigma_3 u$$

si permuteranno nel medesimo modo. Ne concludiamo: *Le tre σ pari*

$$\sigma_r(u \mid \omega, \omega')$$

rimangono assolutamente invariate, eseguendo sui periodi una sostituzione

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix} \pmod 2$$

del sottogruppo Γ_2; per ogni altra sostituzione di Γ si permutano semplicemente fra loro nel modo stesso di e_1, e_2, e_3 nella tabella (A).

Osserviamo ancora che gli infinitesimi delle quattro trascendenti intere

$$\sigma u\,, \quad \sigma_1 u\,, \quad \sigma_2 u\,, \quad \sigma_3 u$$

sono nei punti

$$\begin{array}{lll}
u_0 = 2m\omega + 2n\omega' & \text{per la} & \sigma u \\
u_0 = (2m+1)\omega + 2n\omega' & \text{»} \ \text{»} & \sigma_1 u \\
u_0 = (2m+1)\omega + (2n+1)\omega' & \text{»} \ \text{»} & \sigma_2 u \\
u_0 = 2m\omega + (2n+1)\omega' & \text{»} \ \text{»} & \sigma_3 u\,,
\end{array}$$

dove m, n indicano interi qualunque.

Infine dalla formola (VI) (pag. 17) per la σu, tenendo conto della identità

$$\eta\omega' - \eta'\omega = \frac{\pi i}{2}\,,$$

deduciamo le corrispondenti per $\sigma_1 u$, $\sigma_2 u$, $\sigma_3 u$, che riassumiamo nel prospetto seguente:

$$(\mathrm{B}) \quad \left\{\begin{aligned}
&\sigma(u + 2m\omega + 2n\omega') = \\
&\qquad = (-1)^{mn+m+n} \,.\, e^{(2m\eta+2n\eta')(u+m\omega+n\omega')} \,.\, \sigma u \\
&\sigma_1(u + 2m\omega + 2n\omega') = \\
&\qquad = (-1)^{mn+m} \,.\, e^{(2m\eta+2n\eta')(u+m\omega+n\omega')} \,.\, \sigma_1 u \\
&\sigma_2(u + 2m\omega + 2n\omega') = \\
&\qquad = (-1)^{mn} \,.\, e^{(2m\eta+2n\eta')(u+m\omega+n\omega')} \,.\, \sigma_2 u \\
&\sigma_3(u + 2m\omega + 2n\omega') = \\
&\qquad = (-1)^{mn+n} \,.\, e^{(2m\eta+2n\eta')(u+m\omega+n\omega')} \,.\, \sigma_3 u.
\end{aligned}\right.$$

§ 130. — Le funzioni ellittiche $\sqrt{\wp u - e_r}$ e i valori di $\sqrt{e_\alpha - e_\beta}$.

La formola (2) ci dimostra che la funzione

$$\sqrt{\wp u - e_r} = \pm\,\frac{\sigma_r u}{\sigma u}$$

si scinde colle sue due determinazioni in due funzioni monodrome distinte, ciò che risulta del resto anche dall'osservare che gli infinitesimi e gli infiniti delle funzioni

$$\wp u - e_r = \wp u - \wp \omega_r$$

sono tutti di ordine pari. Colla segnatura

$$\sqrt{\wp u - e_r}$$

intenderemo sempre la funzione $+\dfrac{\sigma_r u}{\sigma u}$, sicchè avremo

$$\text{(II)} \quad \sqrt{\wp u - e_1} = \frac{\sigma_1 u}{\sigma u}, \quad \sqrt{\wp u - e_2} = \frac{\sigma_2 u}{\sigma u}, \quad \sqrt{\wp u - e_3} = \frac{\sigma_3 u}{\sigma u}.$$

Mediante le formole (B) si constata subito che queste tre funzioni sono doppiamente periodiche del secondo ordine coi rispettivi periodi fondamentali

$$(2\omega,\ 4\omega'), \quad (2\omega + 2\omega',\ 4\omega), \quad (4\omega,\ 2\omega').$$

Alle (II) si coordina una formola notevole, che esprime $\wp' u$ per le σ; si ha infatti:

$$\wp' u = \pm 2\sqrt{(\wp u - e_1)(\wp u - e_2)(\wp u - e_3)} = \pm 2\,\frac{\sigma_1 u\, \sigma_2 u\, \sigma_3 u}{\sigma^3 u}$$

e il segno si determina subito dal modo di comportarsi di $\wp' u$ nell'intorno di $u = 0$, onde risulta

$$\text{(III)} \qquad \wp' u = -2\,\frac{\sigma_1 u\, \sigma_2 u\, \sigma_3 u}{\sigma^3 u}.$$

Fissato in modo preciso colle (II) il senso dei radicali $\sqrt{\wp u - e_r}$, intenderemo per $\sqrt{e_s - e_r}$ il valore $\dfrac{\sigma_r \omega_s}{\sigma \omega_s}$; sicchè sarà in generale

$$\sqrt{e_s - e_r} = \frac{e^{-\eta_r \omega_s}\, \sigma(\omega_r + \omega_s)}{\sigma\omega_r\, \sigma\omega_s} = \frac{e^{\eta_r \omega_s}\, \sigma(\omega_r - \omega_s)}{\sigma\omega_r\, \sigma\omega_s},$$

e potremo servirci, secondo torna più opportuno, dell'una o dell'altra formola. Avremo quindi senza alcuna ambiguità:

$$(a) \quad \begin{cases} \sqrt{e_2 - e_1} = \dfrac{\sigma_1 \omega_2}{\sigma \omega_2} = -e^{\eta_1 \omega_2}\, \dfrac{\sigma\omega_3}{\sigma\omega_1\, \sigma\omega_2} \\[2ex] \sqrt{e_3 - e_1} = \dfrac{\sigma_1 \omega_3}{\sigma \omega_3} = e^{-\eta_1 \omega_3}\, \dfrac{\sigma\omega_2}{\sigma\omega_1\, \sigma\omega_3} \end{cases}$$

$$(b) \quad \begin{cases} \sqrt{e_3 - e_2} = \dfrac{\sigma_2 \omega_3}{\sigma \omega_3} = e^{\eta_2 \omega_3}\, \dfrac{\sigma\omega_1}{\sigma\omega_2\, \sigma\omega_3} \\[2ex] \sqrt{e_1 - e_2} = \dfrac{\sigma_2 \omega_1}{\sigma \omega_1} = e^{\eta_2 \omega_1}\, \dfrac{\sigma\omega_3}{\sigma\omega_2\, \sigma\omega_1} \end{cases}$$

$$(c) \quad \begin{cases} \sqrt{e_1 - e_3} = \dfrac{\sigma_3 \omega_1}{\sigma \omega_1} = e^{-\eta_3 \omega_1}\, \dfrac{\sigma\omega_2}{\sigma\omega_3\, \sigma\omega_1} \\[2ex] \sqrt{e_2 - e_3} = \dfrac{\sigma_3 \omega_2}{\sigma \omega_2} = -e^{\eta_3 \omega_2}\, \dfrac{\sigma\omega_1}{\sigma\omega_3\, \sigma\omega_2}. \end{cases}$$

Dietro queste convenzioni risulta

$$(d) \quad \sqrt{e_1 - e_2} = i\sqrt{e_2 - e_1}, \quad \sqrt{e_2 - e_3} = i\sqrt{e_3 - e_2}, \quad \sqrt{e_1 - e_3} = i\sqrt{e_3 - e_1}.$$

Moltiplicando la seconda delle (b) per la prima delle (c), risulta

$$\sqrt{e_1 - e_2} \cdot \sqrt{e_1 - e_3} = \frac{e^{\eta_1 \omega_1}}{\sigma^2 \omega_1}$$

ed estraendo nuovamente la radice quadrata, coll'adottare nel secondo membro la determinazione $\dfrac{e^{\frac{1}{2}\eta_1 \omega_1}}{\sigma\omega_1}$, e analogamente procedendo per gli altri prodotti

$$\sqrt{e_2 - e_3}\ \sqrt{e_2 - e_1}, \qquad \sqrt{e_3 - e_1}\ \sqrt{e_3 - e_2},$$

avremo le formole

$$\text{(IV)} \quad \begin{cases} \sqrt[4]{e_1 - e_2}\ \sqrt[4]{e_1 - e_3} = \dfrac{e^{\frac{1}{2}\eta_1 \omega_1}}{\sigma\omega_1} \\[2ex] \sqrt[4]{e_2 - e_3}\ \sqrt[4]{e_2 - e_1} = \dfrac{e^{\frac{1}{2}\eta_2 \omega_2}}{\sigma\omega_2} \\[2ex] \sqrt[4]{e_3 - e_1}\ \sqrt[4]{e_3 - e_2} = \dfrac{e^{\frac{1}{2}\eta_3 \omega_3}}{\sigma\omega_3}, \end{cases}$$

dalle quali segue una notevole identità. Dalla formola

$$\frac{1}{(e_1 - e_2)(e_1 - e_3)} = \frac{e_3 - e_2}{(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)},$$

permutando circolarmente gli indici e sommando, si ottiene la identità

$$\frac{1}{(e_1 - e_2)\,(e_1 - e_3)} + \frac{1}{(e_2 - e_3)\,(e_2 - e_1)} + \frac{1}{(e_3 - e_1)\,(e_3 - e_2)} = 0,$$

ovvero per le (IV)

$$\text{(V)} \quad \left(e^{-\frac{\eta_1 \omega_1}{2}}\, \sigma\, \omega_1\right)^4 + \left(e^{-\frac{\eta_2 \omega_2}{2}}\, \sigma\, \omega_2\right)^4 + \left(e^{-\frac{\eta_3 \omega_3}{2}}\, \sigma\, \omega_3\right)^4 = 0,$$

che è la formola richiesta.

§ 131. — Aggiunta di semiperiodi all'argomento della $\sigma_r\, u$.

Cerchiamo ora l'effetto prodotto sopra una qualunque delle funzioni σ per l'aggiunta all'argomento u di un *semiperiodo* arbitrario

$$\Omega = m\, \omega + n\, \omega'$$

essendo m, n due numeri interi, di cui uno almeno impari. Se poniamo

$$H = m\, \eta + n\, \eta',$$

avremo, per la proprietà fondamentale della $\sigma\, u$:

$$\sigma\,(u + 2\,\Omega) = -\, e^{2\mathrm{H}(u+\Omega)}\, \sigma\, u\,,$$

da cui cangiando u in $u - \Omega$

$$e^{-\mathrm{H}u}\, \sigma\,(u + \Omega) = e^{\mathrm{H}u}\, \sigma\,(\Omega - u).$$

Ponendo

$$\text{(3)} \qquad \sigma_{m\,n}\; u = e^{-\mathrm{H}u}\, \frac{\sigma\,(u + \Omega)}{\sigma\,\Omega}\,,$$

si avrà evidentemente

$$\sigma_{10}\, u = \sigma_1\, u\,, \qquad \sigma_{01}\, u = \sigma_3\, u\,, \qquad \sigma_{11}\, u = \sigma_2\, u\,.$$

Ma si trova subito che, aumentando sia m, sia n di 2, la $\sigma_{mn}\, u$ non cangia:

$$\sigma_{m+2,\,n}\; u = \sigma_{m,\,n+2}\; u = \sigma_{mn}\; u\,,$$

e però la funzione $\sigma_{mn}\, u$ non dipende dai valori assoluti degli indici m, n, ma solo dalla loro parità o disparità, talchè si ha

$$\begin{cases} \sigma_{mn}\; u = \sigma_1\, u & \text{per} \quad (m, n) \equiv (1, 0) \pmod 2 \\ \sigma_{mn}\; u = \sigma_2\, u & \;\;\text{»} \qquad (m, n) \equiv (1, 1) \\ \sigma_{mn}\; u = \sigma_3\, u & \;\;\text{»} \qquad (m, n) \equiv (0, 1)\,. \end{cases}$$

La formola (3) può dunque riguardarsi come esprimente $\sigma\,(u + \Omega)$ per una delle altre funzioni σ. Ora nella (3) aumentiamo u di $r\,\omega + s\,\omega'$ con r, s interi qualunque, non ambedue pari, e distinguiamo due casi secondo che i numeri $m + r$, $n + s$ sono ambedue pari, ovvero no. Nel primo caso si ha

$$\sigma_{mn}\,(u + r\,\omega + s\,\omega') = C\, e^{(r\eta + s\eta')u}\, \sigma\, u$$

e determinando il fattore costante C col fare $u = -\,(r\,\omega + s\,\omega')$ otteniamo

$$\text{(4)} \quad \sigma_{mn}\,(u + r\,\omega + s\,\omega') = -\, e^{(r\eta + s\eta')\,(u + r\omega + s\omega')}\, \frac{\sigma\, u}{\sigma\,(r\,\omega + s\,\omega')}\,,$$

formola che vale per

$$(m + r,\; n + s) \equiv (0, 0) \pmod 2.$$

Nel secondo caso risulta invece

$$\sigma_{mn}\,(u + r\,\omega + s\,\omega') = C'\, e^{(r\eta + s\eta')u}\, \sigma_{m+r,\; n+s}\; u$$

e determinando C' col fare, per es., $u = 0$ si ha la seconda formola domandata

$$\text{(4*)} \quad \sigma_{mn}\,(u + r\,\omega + s\,\omega') = e^{(r\eta + s\eta')u}\, \sigma_{mn}\,(r\,\omega + s\,\omega')\; \sigma_{m+n,\; r+s}\; u$$

per $(m + n,\; r + s) \not\equiv (0, 0)$ mod 2.

§ 132. — Sviluppo della trascendente intera $\sigma_r u$ in serie di potenze di u.

Le trascendenti intere $\sigma_r u$ $(r = 1, 2, 3)$ sono sviluppabili in serie di potenze di u, convergenti in tutto il piano, ed importa ora che precisiamo la natura dei coefficienti di queste serie. Dimostreremo: *I coefficienti a_n dello sviluppo in serie di*

$$\sigma_r u = \sum_0^\infty a_n u^{2n}$$

sono formati razionalmente cogli invarianti g_2, g_3 e colla radice e_r corrispondente dell'equazione cubica

$$4 e^3 - g_2 e - g_3 = 0 .$$

Risulta di qui nuovamente che, per ogni sostituzione $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare sui periodi, le tre funzioni

$$\sigma_1 u, \quad \sigma_2 u, \quad \sigma_3 u$$

si permutano fra loro al modo stesso di

$$e_1, \quad e_2, \quad e_3 .$$

Per stabilire la proprietà enunciata, consideriamo la funzione più generale periodica di terza categoria

$$\varphi(u) = e^{-u\zeta v} \frac{\sigma(u+v)}{\sigma v}, \tag{5}$$

dove v è un parametro; per $v = \omega_r$, otterremo precisamente la $\sigma_r u$. La $\varphi(u)$ è funzione anche del parametro v e derivando rispetto ad u e v otteniamo

$$\frac{\partial \log \varphi}{\partial u} = \zeta(u+v) - \zeta v$$

$$\frac{\partial \log \varphi}{\partial v} = \zeta(u+v) - \zeta v + u \wp v ,$$

onde risulta che φ soddisfa l'equazione a derivate parziali del primo ordine

$$\frac{\partial \varphi}{\partial u} - \frac{\partial \varphi}{\partial v} + u \varphi \wp v = 0 . \tag{6}$$

Ora supponiamo che sia

$$\varphi(u) = 1 + A_1 u + A_2 \frac{u^2}{1 \cdot 2} +$$
$$+ A_3 \frac{u^3}{1 \cdot 2 \cdot 3} + \dots + A_n \frac{u^n}{1 \cdot 2 \cdot 3 \dots n} + \dots$$

lo sviluppo di $\varphi(u)$ in serie delle potenze ascendenti di u; i coefficienti A_n saranno funzioni analitiche uniformi di v e potremo applicare la derivazione per serie sia rispetto ad u, sia rispetto a v. Dalla (6) risulta quindi pei coefficienti A_n la formola ricorrente

$$A_n = \frac{d A_{n-1}}{d v} - (n-1) A_{n-2} \wp v .$$

Partendo dai primi valori

$$A_1 = 0, \quad A_2 = -\wp v, \quad A_3 = -\wp' v,$$
$$A_4 = -\wp'' v + 3 \wp^2 v = -3 \wp^2 v + \frac{1}{2} g_2 ,$$

vediamo adunque che i coefficienti A_n sono funzioni razionali intere di $\wp v$ per n pari, con coefficienti razionali interi in g_2, g_3, mentre per n dispari sono eguali al prodotto di $\wp' v$ per una tale funzione. Se facciamo $v = \omega_r$, la $\varphi(u)$ si muta in $\sigma_r u$; e poichè

$$\wp \omega_r = e_r , \quad \wp' \omega_r = 0 ,$$

ne risulta la verità del teorema enunciato. È chiaro poi che nei coefficienti dello sviluppo di $\sigma_r u$ si potrà far figurare e_r a potenze non superiori alla seconda. Così si ha:

$$\sigma_r u = 1 - e_r \frac{u^2}{1 \cdot 2} + \left(\frac{1}{2} g_2 - e_r^2\right) \frac{u^4}{1 \cdot 2 \cdot 3 \cdot 4} + \dots$$

§ 133. — Le funzioni ellittiche di Jacobi sn v, cn v, dn v.

I risultati dei paragrafi precedenti conducono direttamente alle tre funzioni ellittiche di Jacobi di cui ora tratteremo; esse sono funzioni doppiamente periodiche appartenenti, secondo i concetti generali del § 128, al sottogruppo $\Gamma_2 : \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0 \\ 0, 1\end{pmatrix}$ (mod 2).

Consideriamo perciò le tre funzioni

$$(7) \qquad \varphi(u) = \sqrt{e_1 - e_3}\,\frac{\sigma u}{\sigma_3 u}, \quad \varphi_1(u) = \frac{\sigma_1 u}{\sigma_3 u}, \quad \varphi_2(u) = \frac{\sigma_2 u}{\sigma_3 u},$$

le quali, secondo le formole (B) (pag. 104) hanno i rispettivi periodi elementari

$$(4\omega,\ 2\omega'), \quad (4\omega,\ 2\omega + 2\omega'), \quad (2\omega,\ 4\omega'),$$

ed hanno infiniti di primo ordine nei punti

$$u_\infty = 2m\omega + (2n+1)\omega'$$

ed infinitesimi di primo ordine rispettivamente nei punti

$$u_0 = 2m\omega + 2n\omega', \quad u_0 = (2m+1)\omega + 2n\omega',$$
$$u_0 = (2m+1)\omega + (2n+1)\omega',$$

percorrendo m, n tutti i valori interi. Inoltre queste funzioni sodisfano alle condizioni iniziali

$$(8) \quad \lim_{u=0} \frac{\varphi(u)}{u} = \sqrt{e_1 - e_3}, \quad \varphi(\omega) = 1, \quad \varphi_1(0) = 1, \quad \varphi_2(0) = 1.$$

Calcoliamo poi i residui di queste tre funzioni per $u = \omega'$, osservando che si ha

$$\lim_{z=\omega'} \frac{u - \omega'}{\sigma_3 u} = -e^{-\eta_3\omega_3}\,\sigma\omega_3 \text{ [1]}$$

[1]) Ciò risulta subito dalla formola

$$\sigma_3(u + \omega_3) = -e^{\eta_3(u+\omega_3)}\frac{\sigma u}{\sigma\omega_3}$$

indi

$$\lim_{u=\omega_3}\left(\frac{u - \omega_3}{\sigma_3 u}\right) = \lim_{u=0}\frac{u}{\sigma_3(u+\omega_3)} = -e^{-\eta_3\omega_3}\,\sigma\omega_3.$$

Tenendo conto delle formole (a), (b), (c) (pagg. 105 e 106) troviamo:

$$(9) \qquad \lim_{u=\omega'}[(u-\omega')\,\varphi(u)] = \frac{1}{\sqrt{e_2 - e_3}},$$

$$\lim_{u=\omega'}[(u-\omega')\,\varphi_1(u)] = -\frac{i}{\sqrt{e_2 - e_3}},$$

$$\lim_{u=\omega'}[(u-\omega')\,\varphi_2(u)] = -\frac{i}{\sqrt{e_1 - e_2}}.$$

Osserviamo ancora che, per le proprietà di omogeneità della σu, della ζu e della $\wp u$ (§§ 95, 104), se si moltiplicano argomento e periodi per un medesimo fattore λ, le

$$\sigma u, \quad \zeta u, \quad \wp u$$

acquistano rispettivamente i fattori

$$\lambda, \quad \frac{1}{\lambda}, \quad \frac{1}{\lambda^2}$$

e per ciò le costanti

$$\eta_r, \quad \sqrt{e_r - e_s}$$

il fattore $\frac{1}{\lambda}$, onde segue che $\sigma_1 u$, $\sigma_2 u$, $\sigma_3 u$ restano invariate. Le nostre tre funzioni (7) godono dunque della comune proprietà espressa dalla formola

$$\Phi(\lambda u \mid \lambda\omega, \lambda\omega') = \Phi(u \mid \omega, \omega').$$

Con una semplice mutazione dell'argomento è facile quindi cangiare le $\varphi(u)$ in tre funzioni dipendenti solo dall'argomento e dal rapporto $\tau = \frac{\omega'}{\omega}$ dei periodi. Pongasi perciò

$$u\sqrt{e_1 - e_3} = v$$

e si riguardino

$$\varphi(u) = \sqrt{e_1 - e_3}\,\frac{\sigma u}{\sigma_3 u}\,, \quad \varphi_1(u) = \frac{\sigma_1 u}{\sigma_3 u}\,, \quad \varphi_2(u) = \frac{\sigma_2 u}{\sigma_3 u}$$

come funzioni del nuovo argomento v. Esse dipenderanno, oltre che dall'argomento, soltanto dal rapporto τ dei periodi; sono queste precisamente le tre funzioni ellittiche di Jacobi

$$\text{sen am } v \text{ o sn } v, \quad \cos \text{am } v \text{ o cn } v, \ \Delta \text{ am } v \text{ o dn } v.$$

Abbiamo dunque per definizione

$$\text{(C)} \qquad \left\{ \begin{aligned} \operatorname{sn} v &= \sqrt{e_1 - e_3}\,\frac{\sigma u}{\sigma_3 u} \\ \operatorname{cn} v &= \frac{\sigma_1 u}{\sigma_3 u} \\ \operatorname{dn} v &= \frac{\sigma_2 u}{\sigma_3 u} \end{aligned} \right\} \quad v = u\sqrt{e_1 - e_3}\,.$$

Se poniamo inoltre, per usare delle notazioni di Jacobi:

$$K = \omega\sqrt{e_1 - e_3}\,, \qquad i K' = \omega'\sqrt{e_1 - e_3}\,,$$

vediamo che sussistono le proprietà fondamentali seguenti:

Le tre funzioni ellittiche di Jacobi hanno rispettivamente i periodi elementari

$$\begin{array}{lll} 4K, & 2iK' & \text{per sn } v, \\ 4K, & 2K + 2iK' & \text{per cn } v, \\ 2K, & 4iK' & \text{per dn } v; \end{array}$$

i loro infiniti di primo ordine sono nei punti

$$v_\infty = 2mK + (2n+1)iK'$$

e gli infinitesimi rispettivamente in

$$\left\{ \begin{array}{ll} v_0 = 2mK + 2niK' & \text{per sn } v \\ v_0 = (2m+1)K + 2niK' & \text{per cn } v \\ v_0 = (2m+1)K + (2n+1)iK' & \text{per dn } v\,. \end{array} \right.$$

Tutte tre e sono funzioni ellittiche di secondo ordine, nel loro rispettivo parallelogrammo dei periodi.

Le formole (8), (9) si cangiano poi nelle seguenti, che importa notare:

$$\text{(8*)} \qquad \lim_{v=0}\left(\frac{\operatorname{sn} v}{v}\right) = 1\,, \quad \operatorname{cn} 0 = 1\,, \quad \operatorname{dn} 0 = 1\,, \quad \operatorname{sn} K = 1\,,$$

$$\text{(9*)} \qquad \lim_{v=iK'}[(v - iK')\operatorname{sn} v] = \frac{1}{k}\,, \quad \lim_{v=iK'}[(v - iK')\operatorname{cn} v] = -\frac{i}{k}\,,$$

$$\lim_{v=iK'}[(v - iK')\operatorname{dn} v] = -i\,,$$

avendo posto

$$\text{(VI)} \qquad k = \sqrt{\frac{e_2 - e_3}{e_1 - e_3}}\,.$$

Questa costante k, che dipende soltanto dal rapporto $\tau = \dfrac{\omega'}{\omega} = \dfrac{iK'}{K}$ dei periodi, dicesi il *modulo* delle funzioni ellittiche sn v, cn v, dn v e, considerata come funzione di τ, è storicamente la prima funzione studiata della classe delle *funzioni modulari*, alla quale ha dato appunto il nome.

Insieme al modulo k, conviene considerare anche il così detto *modulo complementare* k' definito dalla formola

$$\text{(VI*)} \qquad k' = \sqrt{\frac{e_1 - e_2}{e_1 - e_3}}\,,$$

i radicali avendo i sensi precisi loro attribuiti nelle formole (a), (b), (c), pagg. 105 e 106. Fra il modulo k ed il complementare k' ha luogo evidentemente la relazione

$$\text{(10)} \qquad k^2 + k'^2 = 1\,.$$

È inoltre da notarsi che si ha

$$\text{(11)} \qquad \operatorname{dn} K = \frac{\sigma_2 \omega_1}{\sigma_3 \omega_1} = k'\,.$$

Osserviamo poi che delle tre funzioni ellittiche di Jacobi la prima sn v è impari, le altre due cn v, dn v sono pari; inoltre aumentando v di $2K$ o $2iK'$ si comportano nel modo seguente:

$$\begin{cases} \operatorname{sn}(2K+v) = -\operatorname{sn} v, & \operatorname{sn}(2iK'+v) = \operatorname{sn} v \\ \operatorname{cn}(2K+v) = -\operatorname{cn} v, & \operatorname{cn}(2iK'+v) = -\operatorname{cn} v \\ \operatorname{dn}(2K+v) = \operatorname{dn} v, & \operatorname{dn}(2iK'+v) = -\operatorname{dn} v. \end{cases}$$

Notiamo in fine la formola

$$\operatorname{sn}(2K-v) = \operatorname{sn} v.$$

§ 134. — Relazioni fra sn v, cn v, dn v e loro derivate.

Fra i quadrati di sn v, cn v, dn v, hanno luogo due semplici relazioni, che si deducono immediatamente dalle loro espressioni per la $\wp$ di Weierstrass:

$$\text{(VII)} \qquad \operatorname{sn} v = \frac{\sqrt{e_1-e_3}}{\sqrt{\wp u - e_3}}, \qquad \operatorname{cn} v = \frac{\sqrt{\wp u - e_1}}{\sqrt{\wp u - e_3}},$$

$$\operatorname{dn} v = \frac{\sqrt{\wp u - e_2}}{\sqrt{\wp u - e_3}} \quad (v = u\sqrt{e_1 - e_3});$$

si hanno quindi le relazioni cercate

$$\text{(12)} \qquad \operatorname{sn}^2 v + \operatorname{cn}^2 v = 1, \qquad k^2 \operatorname{sn}^2 v + \operatorname{dn}^2 v = 1.$$

Stabiliamo ora le formole che esprimono le derivate di sn v, cn v, dn v per le funzioni stesse di Jacobi. Derivando per ciò le (VII), col ricordare che

$$\wp' u = -2\sqrt{(\wp u - e_1)(\wp u - e_2)(\wp u - e_3)},$$

si otterranno subito le formole importanti

$$\text{(VIII)} \qquad \begin{cases} \dfrac{d \operatorname{sn} v}{dv} = \operatorname{cn} v \operatorname{dn} v \\ \dfrac{d \operatorname{cn} v}{dv} = -\operatorname{sn} v \operatorname{dn} v \\ \dfrac{d \operatorname{dn} v}{dv} = -k^2 \operatorname{sn} v \operatorname{cn} v, \end{cases}$$

che potrebbero facilmente stabilirsi per via diretta dalle proprietà caratteristiche di sn v, cn v, dn v [1]).

Da queste formole si trae subito una conseguenza importante nel teorema: *Le funzioni ellittiche di Jacobi* sn v, cn v, dn v, *dipendono razionalmente dal quadrato k^2 del modulo, come la funzione di Weierstrass $\wp(u; g_2, g_3)$ dagli invarianti g_2, g_3*. Queste tre funzioni sono infatti sviluppabili in serie di potenze di v, convergenti entro il cerchio che ha per raggio la minima distanza dell'origine dai vertici della rete parallelogrammica $2mK + 2niK'$; ora le formole (VIII), e quelle che se ne ottengono per successiva derivazione, dimostrano che i coefficienti di queste serie sono polinomî razionali interi in k^2. Pei primi termini di questi sviluppi abbiamo:

$$\begin{cases} \operatorname{sn} v = v - (k^2+1)\dfrac{v^3}{1.2.3} + (k^4 + 14k^2 + 1)\dfrac{v^5}{\pi(5)} + \dots \\ \operatorname{cn} v = 1 - \dfrac{v^2}{1.2} + (4k^2+1)\dfrac{v^4}{1.2.3.4} + \dots \\ \operatorname{dn} v = 1 - \dfrac{k^2 v^2}{1.2} + k^2(k^2+4)\dfrac{v^4}{1.2.3.4} + \dots \end{cases}$$

Quando si vuol porre in evidenza, per le funzioni ellittiche di Jacobi, il valore del rapporto τ dei periodi, ovvero quello del modulo k, si scrive rispettivamente

$$\operatorname{sn}(v, \tau), \quad \operatorname{cn}(v, \tau), \quad \operatorname{dn}(v, \tau),$$

ovvero

$$\operatorname{sn}(v, k), \quad \operatorname{cn}(v, k), \quad \operatorname{dn}(v, k).$$

Ambedue i sistemi di segnatura sono a determinazione univoca.

§ 135. — Il quadrato k^2 del modulo come funzione modulare.

Studiamo ora quale specie di funzione è il quadrato k^2 del modulo, considerato come funzione del rapporto τ dei periodi.

[1]) Del resto basta stabilire la prima delle (VIII), e le altre ne seguono derivando le (12).

Dimostriamo in primo luogo che $J(\tau)$ è una funzione razionale del sesto grado di k^2. E infatti si ha

$$k^2 = \frac{e_2 - e_3}{e_1 - e_3}, \qquad k'^2 = 1 - k^2 = \frac{e_1 - e_2}{e_1 - e_3},$$

onde

$$1 - k^2 k'^2 = \frac{(e_1 - e_3)^2 - (e_2 - e_3)\,(e_1 - e_2)}{(e_1 - e_3)^2} =$$

$$= \frac{e_1^2 + e_2^2 + e_3^2 - e_1 e_2 - e_2 e_3 - e_3 e_1}{(e_1 - e_3)^2},$$

cioè

$$1 - k^2 k'^2 = \frac{3}{4} \; \frac{g_2}{(e_1 - e_3)^2}.$$

Ne segue

$$J(\tau) = \frac{g_2^3}{16\,(e_1 - e_2)^2\,(e_2 - e_3)^2\,(e_3 - e_1)^2} = \frac{\dfrac{g_2^3}{(e_1 - e_3)^6}}{16\left(\dfrac{e_2 - e_3}{e_1 - e_3}\right)^2 \left(\dfrac{e_1 - e_2}{e_1 - e_3}\right)^2}$$

e infine

$$\text{(IX)} \qquad J(\tau) = \frac{4}{27} \; \frac{(1 - k^2 k'^2)^3}{k^4 k'^4} = \frac{4}{27} \; \frac{(1 - k^2 + k^4)^3}{k^4\,(1 - k^2)^2},$$

formola che dimostra la proprietà enunciata.

Si vede dunque che k^2 è una funzione della variabile complessa τ; di più essa è monodroma, come lo dimostra la sua espressione analitica

$$k^2 = \frac{e_2 - e_3}{e_1 - e_3},$$

ed inoltre in tutto il semipiano positivo τ, l'asse reale escluso, è finita e diversa da 0 e da 1, come segue dalla (IX) ovvero dalla precedente.

Ricerchiamo ora per quali valori τ' dell'argomento la funzione $k^2(\tau)$ riprenderà il medesimo valore. Intanto se

$$k^2(\tau') = k^2(\tau),$$

sarà a più forte ragione

$$J(\tau') = J(\tau)$$

e quindi

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta},$$

essendo $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ una sostituzione del gruppo modulare. D'altra parte la tabella (A) del § 128 (pag. 101) ci mostra immediatamente che l'effetto prodotto sopra $k^2(\tau)$ dalla sostituzione $\dfrac{\alpha\tau + \beta}{\gamma\tau + \delta}$ è diverso a seconda del carattere di $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ (mod 2); e precisamente si ha

$$\left.\begin{array}{lll}
k^2\left(\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = k^2(\tau) & \text{per} & \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0 \\ 0, & 1\end{pmatrix} \\
k^2\left(\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = 1 - k^2(\tau) & \text{»} & \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1 \\ 1, & 0\end{pmatrix} \\
k^2\left(\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \dfrac{k^2(\tau)}{k^2(\tau) - 1} & \text{»} & \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 1 \\ 0, & 1\end{pmatrix} \\
k^2\left(\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \dfrac{k^2(\tau) - 1}{k^2(\tau)} & \text{»} & \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 1 \\ 1, & 0\end{pmatrix} \\
k^2\left(\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \dfrac{1}{1 - k^2(\tau)} & \text{»} & \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1 \\ 1, & 1\end{pmatrix} \\
k^2\left(\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \dfrac{1}{k^2(\tau)} & \text{»} & \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0 \\ 1, & 1\end{pmatrix}
\end{array}\right\} \text{(mod 2)}.$$

Come si vede: *La funzione $k^2(\tau)$ rimane invariata per tutte e sole quelle sostituzioni del gruppo modulare, che appartengono al sottogruppo $\Gamma_2 \equiv \begin{pmatrix}1, & 0 \\ 0, & 1\end{pmatrix}$ (mod 2): per le altre essa subisce le sostituzioni lineari del gruppo anarmonico* [1].

$$\left(k^2,\; 1 - k^2,\; \frac{k^2}{k^2 - 1},\; \frac{k^2 - 1}{k^2},\; \frac{k^2}{1 - k^2},\; \frac{1}{k^2}\right).$$

[1]) Si osservi che k^2 è il birapporto dei quattro valori (e_1, e_2, ∞, e_3) ed una permutazione di e_1, e_2, e_3 induce quindi sopra k^2 le sostituzioni lineari del detto gruppo.

Di qui, per quanto si è visto alla fine del § 134, risulta altresì il teorema:

Le funzioni ellittiche di Jacobi

$$\operatorname{sn}(v,\tau), \quad \operatorname{cn}(v,\tau), \quad \operatorname{dn}(v,\tau),$$

considerate come funzioni del rapporto τ dei periodi, restano invariate per tutte le sostituzioni del sottogruppo $\Gamma_2 \equiv \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ (mod 2).

Come si trasformino per le altre sostituzioni del gruppo modulare sarà esaminato fra breve (vedi § 137).

§ 136. — Formole d'addizione per sn v, cn v, dn v.

Diamo ora le formole d'addizione degli argomenti per le funzioni ellittiche di Jacobi sn v, cn v, dn v, mediante le quali si esprimono

$$\operatorname{sn}(v_1+v_2), \quad \operatorname{cn}(v_1+v_2), \quad \operatorname{dn}(v_1+v_2)$$

razionalmente per

$$\operatorname{sn} v_1, \quad \operatorname{cn} v_1, \quad \operatorname{dn} v_1; \qquad \operatorname{sn} v_2, \quad \operatorname{cn} v_2, \quad \operatorname{dn} v_2.$$

Cominciamo dal caso particolare in cui uno degli argomenti è un semiperiodo

$$K, \quad iK', \quad K+iK'.$$

Ricordando le (VII), pag. 115, che esprimono sn v, cn v, dn v per la $\wp u$ e le formole d'addizione dei semiperiodi nella $\wp u$ (pag 40), troviamo subito

$$\begin{cases} \operatorname{sn}(v+K)=a\dfrac{\operatorname{cn} v}{\operatorname{dn} v}, & \operatorname{cn}(v+K)=b\dfrac{\operatorname{sn} v}{\operatorname{dn} v}, \quad \operatorname{dn}(v+K)=\dfrac{c}{\operatorname{dn} v}, \\ \operatorname{sn}(v+iK')=\dfrac{a'}{\operatorname{sn} v}, & \operatorname{cn}(v+iK')=b'\dfrac{\operatorname{dn} v}{\operatorname{sn} v}, \quad \operatorname{dn}(v+iK')=c'\dfrac{\operatorname{cn} v}{\operatorname{sn} v}, \end{cases}$$

dove a, b, c, a', b', c' sono fattori costanti [1]).

[1]) Queste formole si possono anche stabilire subito direttamente, considerando che in ciascuna di esse le funzioni a destra e sinistra hanno a comune periodi, infiniti ed infinitesimi.

Per determinare questi fattori si faccia nella prima e nella terza $v=0$, nella seconda invece $v=-K$, e nelle ultime tre si moltiplichi per v e si passi al limite per $v=0$. Avendo riguardo alle formole (8*) (9*) (pag. 114), si trova così per le formole domandate:

$$(13)\quad \begin{cases} \operatorname{sn}(v+K)=\dfrac{\operatorname{cn} v}{\operatorname{dn} v}, \quad \operatorname{cn}(v+K)=-k'\dfrac{\operatorname{sn} v}{\operatorname{dn} v}, \\ \qquad \operatorname{dn}(v+K)=\dfrac{k'}{\operatorname{dn} v}. \\ \operatorname{sn}(v+iK')=\dfrac{1}{k\operatorname{sn} v}, \quad \operatorname{cn}(v+iK')=-\dfrac{i}{k}\dfrac{\operatorname{dn} v}{\operatorname{sn} v}, \\ \qquad \operatorname{dn}(v+iK')=-i\dfrac{\operatorname{cn} v}{\operatorname{sn} v}. \end{cases}$$

Ne seguono altresì le formole

$$(14)\quad \operatorname{sn}(v+K+iK')=\frac{\operatorname{dn} v}{k\operatorname{cn} v}, \qquad \operatorname{cn}(v+K+iK')=-\frac{ik'}{k\operatorname{cn} v},$$

$$\operatorname{dn}(v+K+iK')=ik'\frac{\operatorname{sn} v}{\operatorname{cn} v};$$

e facendo $v=0$, si hanno le altre pure notevoli:

$$\operatorname{sn}(K+iK')=\frac{1}{k}, \qquad \operatorname{cn}(K+iK')=-\frac{ik'}{k}.$$

Per stabilire ora le formole generali d'addizione, consideriamo le tre funzioni ellittiche

$$\operatorname{sn} v \operatorname{sn}(v+a), \qquad \operatorname{cn} v \operatorname{cn}(v+a), \qquad \operatorname{dn} v \operatorname{dn}(v+a)$$

(dove a e una costante qualunque), che hanno evidentemente i periodi $2K$, $2iK'$ e nel parallelogrammo fondamentale $(2K, 2iK')$ hanno due infiniti del primo ordine nei punti

$$v_\infty \equiv iK', \qquad -a+iK',$$

con residui naturalmente eguali e di segno contrario. Ora i residui in $v=iK'$ delle tre funzioni sono rispettivamente

$$\frac{1}{k}\operatorname{sn}(a+iK'), \quad -\frac{i}{k}\operatorname{cn}(a+iK'), \quad -i\operatorname{dn}(a+iK'),$$

ossia per le (13):

$$\frac{1}{k^2 \operatorname{sn} a}, \quad -\frac{1}{k^2}\frac{\operatorname{dn} a}{\operatorname{sn} a}, \quad -\frac{\operatorname{cn} a}{\operatorname{sn} a}.$$

Per conseguenza le due funzioni

$$\operatorname{dn} v \operatorname{dn}(v+a) + k^2 \operatorname{cn} a \operatorname{sn} v \operatorname{sn}(v+a)$$

$$\operatorname{cn} v \operatorname{cn}(v+a) + \operatorname{dn} a \operatorname{sn} v \operatorname{sn}(v+a)$$

sono doppiamente periodiche e prive di poli, e quindi costanti, e siccome per $v = 0$ si riducono rispettivamente a dn a, cn a avremo

$$(a) \quad \begin{cases} \operatorname{cn} v \operatorname{cn}(v+a) + \operatorname{dn} a \operatorname{sn} v \operatorname{sn}(v+a) = \operatorname{cn} a \\ \operatorname{dn} v \operatorname{dn}(v+a) + k^2 \operatorname{cn} a \operatorname{sn} v \operatorname{sn}(v+a) = \operatorname{dn} a. \end{cases}$$

Permutiamo nella prima a con v e risolviamo le due equazioni così ottenute

$$\begin{cases} \operatorname{cn} v \operatorname{cn}(v+a) + \operatorname{dn} a \operatorname{sn} v \operatorname{sn}(v+a) = \operatorname{cn} a \\ \operatorname{cn} a \operatorname{cn}(v+a) + \operatorname{dn} v \operatorname{sn} a \operatorname{sn}(v+a) = \operatorname{cn} v \end{cases}$$

rispetto a sn $(v+a)$. Otteniamo la prima formola d'addizione

$$\operatorname{sn}(v+a) = \frac{\operatorname{sn}^2 v - \operatorname{sn}^2 a}{\operatorname{sn} v \operatorname{cn} a \operatorname{dn} a - \operatorname{sn} a \operatorname{cn} v \operatorname{dn} v},$$

alla quale si suol dare comunemente un'altra forma moltiplicando nel secondo membro numeratore e denominatore per

$$\operatorname{sn} v \operatorname{cn} a \operatorname{dn} a + \operatorname{sn} a \operatorname{cn} v \operatorname{dn} v.$$

Così il denominatore diventa

$$\operatorname{sn}^2 v \operatorname{cn}^2 a \operatorname{dn}^2 a - \operatorname{sn}^2 a \operatorname{cn}^2 v \operatorname{dn}^2 v = (\operatorname{sn}^2 v - \operatorname{sn}^2 a)(1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v)$$

e perciò

$$\operatorname{sn}(v+a) = \frac{\operatorname{sn} v \operatorname{cn} a \operatorname{dn} a + \operatorname{sn} a \operatorname{cn} v \operatorname{dn} v}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v}.$$

Sostituendo nelle (a), si trovano le formole per cn $(v+a)$, dn $(v+a)$, che riepiloghiamo nel quadro:

$$(15) \quad \begin{cases} \operatorname{sn}(v+a) = \dfrac{\operatorname{sn} v \operatorname{cn} a \operatorname{dn} a + \operatorname{sn} a \operatorname{cn} v \operatorname{dn} v}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v} \\[2ex] \operatorname{cn}(v+a) = \dfrac{\operatorname{cn} v \operatorname{cn} a - \operatorname{sn} v \operatorname{dn} v \operatorname{sn} a \operatorname{dn} a}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v} \\[2ex] \operatorname{dn}(v+a) = \dfrac{\operatorname{dn} v \operatorname{dn} a - k^2 \operatorname{sn} v \operatorname{cn} v \operatorname{sn} a \operatorname{cn} a}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v}. \end{cases}$$

Si osserverà che ciascuna di queste formole si può scrivere in guisa da far figurare soltanto la funzione ellittica a cui è relativa e la sua derivata. Così per es.:

$$\operatorname{sn}(v+a) = \frac{\operatorname{sn} v \dfrac{d \operatorname{sn} a}{d a} + \operatorname{sn} a \dfrac{d \operatorname{sn} v}{d v}}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v} \quad \text{ecc.}$$

Dalle (15), cangiando a in $-a$ e sommando, risultano le altre

$$(15^*) \quad \begin{cases} \operatorname{sn}(v+a) + \operatorname{sn}(v-a) = \dfrac{2 \operatorname{sn} v \operatorname{cn} a \operatorname{dn} a}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v} \\[2ex] \operatorname{cn}(v+a) + \operatorname{cn}(v-a) = \dfrac{2 \operatorname{cn} v \operatorname{cn} a}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v} \\[2ex] \operatorname{dn}(v+a) + \operatorname{dn}(v-a) = \dfrac{2 \operatorname{dn} v \operatorname{dn} a}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v}. \end{cases}$$

A queste formole fondamentali d'addizione per le funzioni di Jacobi se ne collegano svariatissime altre, delle quali citeremo qui soltanto quelle che dànno i prodotti

$$\operatorname{sn}(v+a)\operatorname{sn}(v-a), \quad \operatorname{cn}(v+a)\operatorname{cn}(v-a), \quad \operatorname{dn}(v+a)\operatorname{dn}(v-a).$$

Queste si deducono nel modo più semplice dalle (15*) cangiando rispettivamente nella prima, seconda e terza di esse v in

$$v + iK', \quad v + K + iK', \quad v + K$$

ed applicando le formole (13), (14) d'addizione dei semiperiodi. Si ottengono in tal guisa le formole domandate:

$$
(16)\quad \left\{
\begin{aligned}
&\operatorname{sn}(v+\alpha)\operatorname{sn}(v-\alpha) = \frac{\operatorname{sn}^2 v - \operatorname{sn}^2 \alpha}{1-k^2 \operatorname{sn}^2 \alpha \operatorname{sn}^2 v} \\
&\operatorname{cn}(v+\alpha)\operatorname{cn}(v-\alpha) = \frac{\operatorname{cn}^2 v \operatorname{cn}^2 \alpha - k'^2 \operatorname{sn}^2 v \operatorname{sn}^2 \alpha}{1-k^2 \operatorname{sn}^2 \alpha \operatorname{sn}^2 v} = \\
&\qquad = \frac{\operatorname{cn}^2 v - \operatorname{sn}^2 \alpha \operatorname{dn}^2 v}{1-k^2 \operatorname{sn}^2 \alpha \operatorname{sn}^2 v} \\
&\operatorname{dn}(v+\alpha)\operatorname{dn}(v-\alpha) = \frac{\operatorname{dn}^2 v \operatorname{dn}^2 \alpha + k^2 k'^2 \operatorname{sn}^2 v \operatorname{sn}^2 \alpha}{1-k^2 \operatorname{sn}^2 \alpha \operatorname{sn}^2 v} = \\
&\qquad = \frac{\operatorname{dn}^2 v - k^2 \operatorname{sn}^2 \alpha \operatorname{cn}^2 v}{1-k^2 \operatorname{sn}^2 \alpha \operatorname{sn}^2 v}\,.
\end{aligned}
\right.
$$

§ 137. — Trasformazione di primo ordine per sn v, cn v, dn v.

Abbiamo veduto che le funzioni ellittiche di Jacobi

$$\operatorname{sn}(v,\tau),\quad \operatorname{cn}(v,\tau),\quad \operatorname{dn}(v,\tau)$$

restano invariate quando sul rapporto τ dei periodi si eseguisce una sostituzione

$$\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$$

del sottogruppo $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix}$ (mod 2). Ci proponiamo ora di esaminare come cangiano per le altre sostituzioni del gruppo modulare. Manifestamente avremo qui sei casi diversi, a seconda del carattere della sostituzione $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ (mod 2); ma basterà che ricerchiamo l'effetto prodotto dall'una e dall'altra delle due sostituzioni elementari del gruppo modulare

$$\begin{pmatrix}0, 1\\ -1, 0\end{pmatrix} \qquad \begin{pmatrix}1, 1\\ 0, 1\end{pmatrix}.$$

A tale oggetto esprimeremo sn v, cn v, dn v per le σ colle formole (C), pag. 113, ed esamineremo il corrispondente effetto pro-

dotto sulle σ. Indicando con $2\overline{\omega}$, $2\overline{\omega}'$ i nuovi periodi, porremo per ciò una prima volta

$$(\alpha)\qquad \overline{\omega}' = \omega \qquad \overline{\omega} = -\omega'$$

ed una seconda volta

$$(\beta)\qquad \overline{\omega}' = \omega' + \omega \qquad \overline{\omega} = \omega.$$

Poniamo

$$\overline{\sigma}_r u = \sigma_r(u \mid \overline{\omega}, \overline{\omega}')$$

e dalla tabella (A), pag. 101, dedurremo immediatamente:

$$\left.\begin{aligned}
&\overline{\sigma} u = \sigma u \quad \overline{\sigma}_1 u = \sigma_3 u \quad \overline{\sigma}_2 u = \sigma_2 u \quad \overline{\sigma}_3 u = \sigma_1 u \\
&\qquad e'_1 = e_3 \quad e'_2 = e_2 \quad e'_3 = e_1
\end{aligned}\right\}\ \text{nel caso } (\alpha)$$

invece

$$\left.\begin{aligned}
&\overline{\sigma} u = \sigma u \quad \overline{\sigma}_1 u = \sigma_1 u \quad \overline{\sigma}_2 u = \sigma_3 u \quad \overline{\sigma}_3 u = \sigma_2 u \\
&\qquad e'_1 = e_1 \quad e'_2 = e_3 \quad e'_3 = e_2
\end{aligned}\right\}\ \text{nel caso } (\beta)$$

Ora si hanno le formole

$$\left.\begin{aligned}
&\operatorname{sn}(v,\tau) = \\
&= \sqrt{e_1-e_3}\,\frac{\sigma u}{\sigma_3 u} \\
&\operatorname{cn}(v,\tau) = \frac{\sigma_1 u}{\sigma_3 u} \\
&\operatorname{dn}(v,\tau) = \frac{\sigma_2 u}{\sigma_3 u}
\end{aligned}\right\}
\begin{aligned}
&\tau = \frac{\omega'}{\omega} \\
&v = \sqrt{e_1-e_3}\, u
\end{aligned}
\qquad
\left.\begin{aligned}
&\operatorname{sn}(\overline{v},\overline{\tau}) = \\
&= \sqrt{e'_1-e'_3}\,\frac{\overline{\sigma} u}{\overline{\sigma}_3 u} \\
&\operatorname{cn}(\overline{v},\overline{\tau}) = \frac{\overline{\sigma}_1 u}{\overline{\sigma}_3 u} \\
&\operatorname{dn}(\overline{v},\overline{\tau}) = \frac{\overline{\sigma}_2 u}{\overline{\sigma}_3 u}
\end{aligned}\right\}
\begin{aligned}
&\overline{\tau} = \frac{\overline{\omega}'}{\overline{\omega}} \\
&\overline{v} = \sqrt{e'_1-e'_3}\, u\,,
\end{aligned}$$

onde risulta

$$\overline{v} = \frac{\sqrt{e_3-e_1}}{\sqrt{e_1-e_3}}\, v = -i\, v \quad \text{nel caso } (\alpha)$$

$$\overline{v} = \frac{\sqrt{e_1-e_2}}{\sqrt{e_1-e_3}}\, v = k'\, v \quad \text{nel caso } (\beta)$$

Le formole cercate sono dunque le seguenti

$$\text{(X)} \qquad \operatorname{sn}\left(i\,v\,,\,-\frac{1}{\tau}\right) = i\,\frac{\operatorname{sn}(v,\tau)}{\operatorname{cn}(v,\tau)}\,,$$

$$\operatorname{cn}\left(i\,v\,,\,-\frac{1}{\tau}\right) = \frac{1}{\operatorname{cn}(v,\tau)}\,, \qquad \operatorname{dn}\left(i\,v\,,\,-\frac{1}{\tau}\right) = \frac{\operatorname{dn}(v,\tau)}{\operatorname{cn}(v,\tau)}$$

$$\text{(XI)} \qquad \operatorname{sn}(k'v,\tau+1) = k'\,\frac{\operatorname{sn}(v,\tau)}{\operatorname{dn}(v,\tau)}\,,$$

$$\operatorname{cn}(k'v,\tau+1 = \frac{\operatorname{cn}(v,\tau)}{\operatorname{dn}(v,\tau)}\,, \qquad \operatorname{dn}(k'v,\tau+1) = \frac{1}{\operatorname{dn}(v,\tau)}\,.$$

Se si osserva poi che nel primo caso il modulo trasformato è

$$k\left(-\frac{1}{\tau}\right) = \frac{\sqrt{e_2-e_1}}{\sqrt{e_3-e_1}} = k'$$

e nel secondo

$$k(\tau+1) = \frac{\sqrt{e_3-e_2}}{\sqrt{e_1-e_2}} = -\frac{i\,k}{k'}\,,$$

ponendo in evidenza i moduli anzichè il rapporto dei periodi, potremo scrivere:

$$\text{(X*)} \qquad \operatorname{sn}(i v, k') = i\,\frac{\operatorname{sn}(v,k)}{\operatorname{cn}(v,k)}\,,$$

$$\operatorname{cn}(i\,v,k') = \frac{1}{\operatorname{cn}(v,k)}\,, \qquad \operatorname{dn}(i\,v,k') = \frac{\operatorname{dn}(v,k)}{\operatorname{cn}(v,k)}$$

$$\text{(XI*)} \qquad \operatorname{sn}\left(k'v,\,\frac{i\,k}{k'}\right) = k'\,\frac{\operatorname{sn}(v,k)}{\operatorname{dn}(v,k)}\,,$$

$$\operatorname{cn}\left(k'v,\,\frac{i\,k}{k'}\right) = \frac{\operatorname{cn}(v,k)}{\operatorname{dn}(v,k)}\,, \qquad \operatorname{dn}\left(k'\,v,\,\frac{i\,k}{k'}\right) = \frac{1}{\operatorname{dn}(v,k)}\,.$$

Le (X*) diconsi le formole della *trasformazione complementare*, come quelle che dànno il passaggio dalle funzioni ellittiche di modulo k a quelle col modulo complementare k'.

CAPITOLO XIII.

Le funzioni $\wp\, u$, $\sigma\, u$ e $\sigma_r u$ per valori reali degli invarianti e le funzioni di Jacobi sn v, cn v, dn v, **per valori reali del modulo k fra 0 e 1. — Integrali ellittici di Legendre e Jacobi.**

§ 138. — Osservazioni fondamentali sulla funzione $\wp\,(u;\,g_2, g_3)$ con invarianti reali.

Fino ad ora ci siamo occupati della teoria generale delle funzioni ellittiche, e in particolare delle funzioni di Weierstrass e di Jacobi, senza distinzione fra i valori reali od immaginari degli argomenti o delle funzioni. Ma, nelle applicazioni pratiche, è il reale soltanto che entra in considerazione, ed è per ciò necessario che studiamo meglio l'andamento delle nostre funzioni, con speciale riguardo ai valori reali, per quei casi che si presentano nelle effettive applicazioni.

Le funzioni ellittiche si introducono sempre in pratica in problemi d'inversione, cioè nella integrazione di funzioni razionali

$$F\,(w,\ \sqrt{P\,(w)}\,)\,,$$

essendo $P\,(w)$ un polinomio di terzo o quarto grado (§ 126). E siccome i polinomî $P\,(w)$, che si presentano effettivamente, sono sempre a coefficienti reali e quindi anche ad invarianti reali g_2, g_3, così il problema fondamentale da proporsi è il seguente: *Studiare l'andamento della funzione*

$$\wp\,(u\,;\ g_2\,,\ g_3)$$

per valori reali degli invarianti g_2, g_3.

Cominciamo per questo dall'osservare che dallo sviluppo della trascendente intera (pag. 35)

$$\sigma\,(u\,;\ g_2\,,\ g_3) = u - \frac{g_2}{240}\,u^5 + \ldots,$$

i coefficienti essendo nel caso attuale reali (perchè funzioni razionali intere a coefficienti razionali di g_2, g_3), risulta: *La funzione σu con invarianti reali è reale per valori reali e puramente immaginaria per valori puramente immaginari dell'argomento u.*

Lo stesso vale evidentemente per la funzione ζu mentre invece: *La funzione $\wp(u\,;\,g_2,\,g_3)$ con invarianti reali è reale tanto sull'asse delle quantità reali, come su quello delle immaginarie.*

Ma in generale, quando una funzione analitica è reale lungo un tratto rettilineo del piano complesso, in punti simmetrici rispetto a questo tratto assume valori coniugati [1]), onde si vede che: *La $\wp(u\,;\,g_2,\,g_3)$ in punti simmetrici rispetto all'asse delle quantità reali, o delle immaginarie, assume valori coniugati.*

Dopo di ciò è facile vedere che nel caso attuale ad ogni periodo $2\,\Omega$ della $\wp\,u$ corrisponderà un periodo coniugato $2\,\Omega_0$.

Sia infatti $2\,\Omega$ un periodo qualunque di $\wp\,u$; se u è reale $= x$, pei valori coniugati

$$x + 2\,\Omega, \quad x + 2\,\Omega_0$$

dell'argomento la $\wp$ assumerà valori coniugati e, poichè

$$\wp\,(x + 2\,\Omega) = \wp\,(x)$$

è reale, sarà

$$\wp\,(x + 2\,\Omega_0) = \wp\,x.$$

[1]) Tutto si riduce a dimostrare questa proprietà pel caso di un tratto dell'asse reale, il caso generale riportandosi a questo con una sostituzione lineare intera sull'argomento. Ora se a è un punto dell'asse reale, nel cui intorno la funzione $f(z)$ sia regolare, si avrà

$$f(z) = \sum a_n\,(z - a)^n$$

e i coefficienti a_n saranno per ipotesi reali, onde a valori coniugati di z *entro il cerchio di convergenza di* (1) corrisponderanno certamente valori coniugati per tutte le derivate. Ma allora, se un prolungamento analitico di (1) è

$$f(z) = \sum b_n\,(z - \gamma)^n,$$

si vede subito che un secondo prolungamento analitico sarà

$$f(z) = \Sigma\,\bar{b}_n\,(z - \bar{\gamma})^n$$

essendo $\bar{\gamma}$, $\bar{b}_n$ le coniugate di γ, b_n. Così ad ogni ulteriore prolungamento analitico di $f(z)$ corrisponderà un prolungamento coniugato, ciò che dimostra il teorema.

Dunque la funzione

$$\wp\,(u + 2\,\Omega_0) - \wp\,u,$$

essendo nulla sull'asse reale, sarà costantemente nulla, cioè $2\,\Omega_0$ è anche un periodo di $\wp\,u$, c. d. d.

Ora osserviamo che, fissati i valori (reali) degli invarianti g_2, g_3, i periodi fondamentali $2\,\omega$, $2\,\omega'$ della $\wp\,u$ sono determinati soltanto a meno di una sostituzione lineare $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare. Poichè il valore

$$J = \frac{g_2^3}{g_2^3 - 27\,g_3^2}$$

dell'invariante assoluto è reale, un corrispondente valore di $\tau = \dfrac{\omega'}{\omega}$ sarà certamente sul contorno del triangolo fondamentale (cfr. § 119) e noi intenderemo colla notazione

$$2\,\omega, \quad 2\,\omega'$$

quei periodi fondamentali che rispondono ad un rapporto τ sul detto contorno. A questa coppia di periodi ne sostituiremo poi ogni volta una seconda *equivalente*, che indicheremo con

$$2\,\omega_1, \qquad 2\,\omega_3$$

più adatta nei singoli casi alla ricerca.

§ 139. — Caso del discriminante positivo $\Delta = g_2^3 - 27\,g_3^2 > 0$. Rappresentazione conforme di un rettangolo sul semipiano.

Dobbiamo distinguere nel nostro studio due casi, secondo che il valore del discriminante

$$\Delta = g_2^3 - 27\,g_3^2 = 16\,(e_1 - e_2)^2\,(e_2 - e_3)^2\,(e_3 - e_1)^2$$

è positivo o negativo. Consideriamo qui il primo caso; allora si ha evidentemente

$$g_2 > 0, \qquad J(\tau) > 1,$$

e però l'indice di τ nel triangolo fondamentale è sull'asse immaginario.

Inoltre le tre radici e_1, e_2, e_3 dell'equazione cubica

$$4e^3 - g_2 e - g_3 = 0$$

sono, nel caso attuale, tutte e tre reali.

Dalle formole

$$g_2 = \frac{60}{\omega^4} \sum{}' \frac{1}{(2m + 2n\tau)^4}, \qquad g_3 = \frac{140}{\omega^6} \sum{}' \frac{1}{(2m + 2n\tau)^6},$$

essendo reali le serie dei secondi membri, segue che ω^2 è reale e quindi ω reale, o puramente immaginario, e corrispondentemente ω' puramente immaginario o reale. Porremo nel primo caso

$$\omega_1 = \omega, \qquad \omega_3 = \omega',$$

e nel secondo

$$\omega_1 = -\omega', \qquad \omega_3 = \omega,$$

$\left(\text{ciò che equivale a cangiar } \tau \text{ in } -\frac{1}{\tau}\right)$ ed avremo quindi che: *i due periodi fondamentali $2\omega_1, 2\omega_3$ saranno reale il primo e puramente immaginario il secondo.*

Il parallelogrammo fondamentale dei periodi diventerà quindi nel caso attuale il rettangolo

$$(0, 2\omega_1, \quad 2\omega_1 + 2\omega_3, \quad 2\omega_3).$$

Dividiamolo per mezzo delle linee mediane

$$(\omega_1, \omega_1 + 2\omega_3), \quad (\omega_3, 2\omega_1 + \omega_3)$$

in quattro rettangoli parziali congruenti (come nella fig. 10 a pag. 130) ed osserviamo che, a causa della formola

$$\wp(2\omega_1 + 2\omega_3 - u) = \wp(u),$$

nel terzo di questi rettangoli

$$(\omega_1 + \omega_3, \ 2\omega_1 + \omega_3, \ 2\omega_1 + 2\omega_3, \ \omega_1 + 2\omega_3)$$

la $\wp u$ riprende i valori già presi nel primo rettangolo

$$(0, \omega_1, \omega_1 + \omega_3, \omega_3),$$

nel quale adunque assumerà ogni suo valore una sola volta. In punti simmetrici rispetto all'asse reale o immaginario la $\wp u$ assume valori coniugati e lo stesso accade quindi in punti simme-

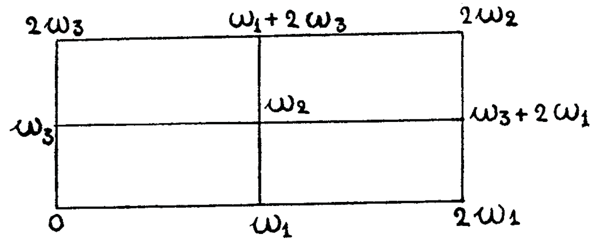

Fig. 10.

trici rispetto alle due linee mediane, sulle quali conseguentemente la $\wp u$ è reale [1]). Ne segue che nel secondo e quarto dei detti rettangoli minori $\wp u$ prende i valori coniugati a quelli del primo e terzo rettangolo.

Su tutto il contorno del primo rettangolo

$$(0, \omega_1, \omega_1 + \omega_3, \omega_3)$$

la funzione $\wp u$ è reale; e poichè in prossimità di $u = 0$ sull'asse reale è grandissima positiva, e invece sull'asse immaginario grandissima negativa, come risulta dallo sviluppo

$$\wp u = \frac{1}{u^2} + \frac{g_2}{28} u^2 + \ldots$$

nell' intorno di $u = 0$, vediamo che percorrendo il detto contorno nel senso positivo, a partire dall'origine, la $\wp u$ andrà *continuamente* decrescendo da $+\infty$ a $-\infty$. Ora nei vertici

$$\omega_1, \ \omega_1 + \omega_3 = \omega_2, \ \omega_3$$

[1]) Ciò risulta anche immediatamente dalle formole d'addizione dei semiperiodi (pag. 40), le radici e_1, e_2, e_3 essendo qui reali.

la $\wp u$ assume i valori

$$\wp \omega_1 = e_1 , \quad \wp \omega_2 = e_2 , \quad \wp \omega_3 = e_3 .$$

Si vede dunque che e_1, e_2, e_3 risultano così ordinate per grandezza decrescente, cioè :

$$e_1 > e_2 > e_3 ;$$

e poichè

$$e_1 + e_2 + e_3 = 0 ,$$

sarà e_1 positiva, e_3 negativa. Quanto al segno di e_2, a causa di

$$g_3 = 4 e_1 e_2 e_3 ,$$

sarà evidentemente opposto a quello di g_3.

Ogni valore reale è già preso dalla $\wp u$ due volte in punti non equivalenti dei lati e delle mediane del rettangolo dei periodi, onde segue che nell' interno di ciascuno dei quattro rettangoli minori la $\wp u$ è sempre complessa e perciò il coefficiente dell' immaginario in $\wp u$ serba ivi sempre lo stesso segno. Così per es. nell' interno del primo rettangolo $(0, \omega_1, \omega_1 + \omega_3, \omega_3)$, a causa dell'andamento da $+\infty$ a $-\infty$ sul contorno percorso in verso positivo, il coefficiente dell' immaginario in $\wp u$ è sempre negativo. È chiaro poi che ogni valore

$$s = \alpha + i \beta ,$$

con $\beta < 0$, sarà preso da $\wp u$ una ed una sola volta nell' interno del detto rettangolo. D'altronde $\dfrac{ds}{du} = \wp' u$ non vi s'annulla mai, nè diventa infinita, salvo ai quattro vertici $0, \omega_1, \omega_1 + \omega_3, \omega_3$; per ciò se poniamo

$$s = \wp u$$

ed interpretiamo s nel suo piano complesso, vediamo che : *La funzione $s = \wp u$ dà la rappresentazione conforme biunivoca del rettangolo $(0, \omega_1, \omega_2, \omega_3)$ sul semipiano negativo s; gli unici punti eccezionali della rappresentazione sono i vertici del rettangolo.*

Si osservi in fine che, dando a g_2, g_3 convenienti valori reali con $g_2^3 - 27 g_3^2 > 0$, si può far coincidere il nostro rettangolo con

un rettangolo qualunque dato a priori, onde risulta : *Il problema della rappresentazione conforme di un rettangolo sopra un semipiano conduce direttamente alla funzione di Weierstrass $\wp(u; g_2, g_3)$ con invarianti reali e discriminante positivo.*

§ 140. — Andamento della $\wp' u$. - La cubica $y^2 = 4x^3 - g_2 x - g_3$.

Osserviamo anche l'andamento di $\wp' u$ sul contorno del rettangolo $(0, \omega_1, \omega_2, \omega_3)$. Mentre l'argomento u e la $\wp u$ lungo i quattro tratti del contorno variano rispettivamente negli intervalli :

$$u \text{ da } 0 \ldots\ldots \omega_1 ; \quad \omega_1 \ldots\ldots \omega_2 ; \quad \omega_2 \ldots\ldots \omega_3 ; \quad \omega_3 \ldots\ldots 0$$

$$\wp u \text{ da } +\infty \ldots\ldots e_1 ; \quad e_1 \ldots\ldots e_2 ; \quad e_2 \ldots\ldots e_3 ; \quad e_3 \ldots\ldots -\infty ,$$

vediamo che l'andamento di

$$\wp' u = -2 \sqrt{(\wp u - e_1)(\wp u - e_2)(\wp u - e_3)}$$

è il seguente

$$\left.\begin{array}{c} u \text{ da } 0 \ldots\ldots \omega_1 \\ \wp' u \text{ reale negativa} \\ \text{da } \infty - \ldots\ldots 0 \end{array}\right\} \quad \left.\begin{array}{c} u \text{ da } \omega_1 \ldots\ldots \omega_2 \\ \wp' u \text{ immaginaria positiva} \end{array}\right\}$$

$$\left.\begin{array}{c} u \text{ da } \omega_2 \ldots\ldots \omega_3 \\ \text{da } 0 \text{ a } \infty \\ \wp' u \text{ reale positiva} \end{array}\right\} \quad \begin{array}{c} u \text{ da } \omega_3 \ldots\ldots 0 \\ \wp' u \text{ immaginaria negativa.} \end{array}$$

In particolare si osservi : *I valori dell' argomento u che rendono simultaneamente reali $\wp u$, $\wp' u$, sono della forma*

$$u = \xi , \quad u = \xi + \omega_3 \quad (\xi \text{ reale}).$$

Si ottiene una chiara interpretazione geometrica del corso reale delle funzioni $\wp u$, $\wp' u$ nel modo seguente. Essendo x, y coordinate cartesiane di un punto mobile in un piano, si consideri la curva definita dalle equazioni

$$x = \wp u\,, \qquad y = \wp' u\,,$$

che è evidentemente la cubica

(1) $$y^2 = 4\,x^3 - g_2\,x - g_3\,.$$

Ora importa osservare che: *questa equazione rappresenta la più generale curva del terzo ordine, a meno di trasformazioni proiettive.* Per vederlo nel modo più semplice passiamo alle coordinate omogenee, ponendo

$$x = \frac{x_1}{x_3}\,, \qquad y = \frac{x_2}{x_3}\,,$$

sicchè l'equazione diventa:

(2) $$x_2^2\,x_3 - 4\,x_1^3 + g_2\,x_1\,x_3^2 + g_3\,x_3^3 = 0.$$

Se esaminiamo quale particolare relazione ha l'attuale triangolo di riferimento colla curva, vediamo che hanno luogo le seguenti proprietà:

1° Il vertice (0, 1, 0) è un flesso della curva e il lato $x_3 = 0$ è la corrispondente tangente di flesso;

2° il lato $x_3 = 0$ è la *polare armonica* del flesso (cioè insieme colla tangente $x_3 = 0$ di flesso costituisce la conica polare del flesso);

3° il lato $x_1 = 0$ è la polare lineare del vertice (1, 0, 0), punto d'incontro delle due rette ora dette.

Viceversa si vedrà subito che, preso il triangolo di riferimento nel modo descritto, si può dare all'equazione della curva del terzo ordine la forma normale (2) di Weierstrass. Abbiamo dunque il risultato: *Le coordinate di un punto mobile sopra una curva generale del terzo ordine possono esprimersi per funzioni ellittiche di un parametro.*

Si osservi di più che, se l'equazione data della cubica è a coefficienti reali, la trasformazione indicata si può ottenere per via

reale e per ciò gli invarianti g_1, g_3 saranno reali [1]). Ritornando ora al caso particolare, che trattiamo attualmente, del discriminante $\Delta = g_2^3 - 27\,g_3^2 > 0$, esaminiamo il corso reale della nostra curva (1). Per quanto si è visto sopra, otterremo i punti reali della nostra curva o prendendo

$$u = \xi \qquad (\xi \text{ reale})\,,$$

ovvero

$$u = \xi + \omega_3\,.$$

Basterà naturalmente far variare ξ fra $-\omega_1$ e $+\omega_1$, perchè quando ξ aumenta di multipli di $2\omega_1$ il punto della curva riprende la medesima posizione. Anzi, a causa delle formole

$$\wp(-u) = \wp u$$

$$\wp'(-u) = -\wp' u\,,$$

basterà far crescere ξ da 0 a ω_1 e si otterrà una prima metà della curva, che ribaltata attorno all'asse delle x darà la seconda metà.

Ora, quando u cresce da 0 ad ω_1, la $x = \wp u$ decresce da $+\infty$ ad $e_1 > 0$, mentre $y = \wp' u$ cresce da $-\infty$ a 0, sicchè si ha una prima metà di un ramo infinito della curva al di sotto dell'asse delle x, che esce dal punto $(e_1, 0)$ dell'asse delle x, ortogonalmente a quest'asse.

Ribaltando questa prima metà del ramo attorno all'asse x, si ottiene il ramo completo infinito, che contiene tutti e soli i punti reali della curva, *corrispondenti a valori reali di u.*

Veniamo a considerare gli altri valori di u, che dànno ancora punti reali della curva, cioè i valori della forma $u = \xi + \omega_3$, dove facciamo crescere ξ da 0 a ω_1; allora $x = \wp u$ crescerà da e_3 a e_2 ed $y = \wp' u$ passerà per una serie di valori positivi, annullandosi agli estremi. Corrispondentemente avremo un tratto finito della nostra curva che parte dal punto $(e_3, 0)$ dell'asse delle x per arrivare al punto $(e_2, 0)$ e che sarà ortogonale negli estremi all'asse stesso.

[1]) Prescindendo da coefficienti numerici, g_2, g_3 coincidono precisamente cogli invarianti S, T di quarto e sesto grado rispettivamente della forma cubica ternaria (SALMON, *Algèbre supérieure*, Treizième Leçon).

Per ribaltamento attorno all'asse delle x otteniamo la seconda parte reale della cubica, costituita di una parte chiusa (ovale). Dunque: *La cubica*

$$y_2 = 4\,x^3 - g_2\,x - g_3\,,$$

nel caso di

$$\Delta = g_2^3 - 27\,g_3^2 > 0\,,$$

consta di due rami diversi, di cui l' uno è infinito, l'altro un ovale.

§ 141. — Alcune applicazioni geometriche.

La rappresentazione parametrica dei punti di una cubica generale per mezzo delle funzioni ellittiche dà luogo ad una serie di interessanti applicazioni geometriche, di cui qui accenneremo solo le fondamentali, avvertendo che nel presente paragrafo non facciamo più alcuna ipotesi speciale riguardo agli invarianti g_2, g_3, che possono essere reali o complessi.

Un punto mobile (x, y) della cubica è dato dalle formole

$$x = \wp\,u\,, \quad y = \wp'\,u\,;$$

ad ogni valore di u corrisponde un unico punto della curva ed il punto resta il medesimo per valori congrui dell'argomento.

Viceversa, se due punti u_1, u_2 della curva coincidono, si ha $u_1 \equiv u_2$, cioè

$$u_1 = u_2 + 2\,m\,\omega_1 + 2\,n\,\omega_3\,(m, n \text{ interi}).$$

Cerchiamo ora la condizione perchè tre punti u_1, u_2, u_3 della cubica siano in linea retta. Se $y = a\,x + b$ è l' equazione della retta che li contiene [1], la funzione ellittica del terzo ordine

$$\wp' u - a\,\wp\,u - b\,,$$

[1]) Il caso in cui l'equazione della retta sia $x = k$ rientra in questo, uno dei tre punti d' incontro essendo allora all' infinito in $u = 0$.

con un polo di terzo ordine nell' origine, ha gli infinitesimi incongrui u_1, u_2, u_3 e perciò si ha

$$u_1 + u_2 + u_3 \equiv 0.$$

È questa, come subito si vede, la condizione necessaria e sufficiente perchè i tre punti u_1, u_2, u_2 siano allineati (teorema d'Abel).

Di qui si può dedurre di nuovo il teorema d'addizione per la $\wp\,u$, sotto la forma del § 108 (pag. 44):

$$\begin{vmatrix} 1 & \wp\,(u_1 + u_2) & -\wp'\,(u_1 + u_2) \\ 1 & \wp\,u_1 & \wp' u_1 \\ 1 & \wp\,u_2 & \wp' u_2 \end{vmatrix} = 0.$$

Più in generale consideriamo una curva d'ordine n

$$f\,(x\,, y) = 0$$

e i suoi punti d' incontro colla cubica. La funzione $f\,(\wp\,u, \wp' u)$ è una funzione ellittica d'ordine $3\,n$, che ha dunque $3\,n$ punti d' infinitesimo $u_1, u_2, \ldots, u_{3n}$ [1]) ed un solo infinito d'ordine $3\,n$ in $u = 0$, sicchè pel teorema d'Abel si ha

$$u_1 + u_2 + \ldots + u_{3n} \equiv 0\,.$$

Questa esprime la condizione necessaria e sufficiente perchè $3\,n$ punti u_1, u_2, ..., u_{3n} della cubica costituiscano i punti d' intersezione della cubica con una curva d'ordine n.

Applichiamo questi teoremi generali alla risoluzione di due problemi:

1° *Tangenti che da un punto della cubica partono alla cubica stessa.* — Sia u il punto di partenza e v il punto di contatto di una delle anzidette tangenti: dovremo avere pel teorema d'Abel

$$u + 2\,v \equiv 0,$$

[1]) Può anche darsi che, mancando alcuni termini in $f\,(x, y)$, la funzione ellittica $f\,(\wp\,u, \wp u')$ sia d' ordine minore di $3n$, per es. $3n - r$; allora r delle intersezioni sono raccolte nel flesso all' infinito.

ciò che dà per v i quattro valori distinti

$$-\frac{u}{2}, \qquad -\frac{u}{2}+\omega_1, \qquad -\frac{u}{2}+\omega_2, \qquad -\frac{u}{2}+\omega_3,$$

onde si conclude che da ogni punto della cubica si possono condurre quattro tangenti alla cubica.

Se la cubica è reale e a discriminante positivo, vediamo che da ogni punto del ramo infinito partono quattro tangenti tutte reali alla curva, laddove da un punto dell'ovale partono tangenti tutte immaginarie.

2° *Punti d'inflessione.* — Un flesso della curva è un punto ove la tangente ha tre punti coincidenti a comune colla curva.

Il parametro u di un flesso deve soddisfare alla condizione (necessaria e sufficiente):

$$3u \equiv 0;$$

si hanno quindi *nove flessi* con argomento

$$u = \frac{2m\omega_1 + 2n\omega_3}{3}; \qquad \left.\begin{matrix} m \\ n \end{matrix}\right\} = 0,\ 1,\ 2.$$

Se u_1, u_2, sono due flessi, ed u_3 il punto ove la loro congiungente incontra la cubica, si ha

$$u_1 + u_2 + u_3 \equiv 0, \qquad 3u_1 \equiv 0, \qquad 3u_2 \equiv 0,$$

onde anche $3u_3 \equiv 0$; ne segue il noto teorema: *La congiungente due flessi di una cubica incontra la curva in un terzo flesso.*

Ritornando al caso di una cubica reale a discriminante

$$g_2^3 - 27g_3^2 > 0,$$

vediamo allora che dei nove flessi tre soltanto sono reali e cioè i flessi

$$0, \quad \frac{2\omega_1}{3}, \qquad \frac{4\omega_1}{3},$$

situati sul ramo infinito della curva.

§ 142. — La $\wp(u; g_2, g_3)$ con invarianti reali e discriminante negativo.

Veniamo al caso del discriminante negativo, riprendendo le considerazioni dei §§ 138, 139. Essendo

$$g_2^3 - 27g_3^2 < 0,$$

potrà essere $g_2 > 0$ o $g_2 < 0$; nel primo caso sarà

$$J = \frac{g_2^3}{g_2^3 - 27g_3^2} < 0$$

e nel secondo

$$0 < J < 1,$$

cioè $\tau = \frac{\omega'}{\omega}$ sarà nel primo caso sul lato rettilineo $R(\tau) = -\frac{1}{2}$ del triangolo fondamentale, nel secondo invece sull'arco circolare $|\tau| = 1$. Insieme ai periodi 2ω, $2\omega'$ la $\wp u$ ammetterà i periodi coniugati $2\omega_0$, $-2\omega'_0$ [1]) e sussisteranno quindi le formole:

$$\left\{\begin{aligned} -\omega'_0 &= \alpha\omega' + \beta\omega \\ \omega_0 &= \gamma\omega' + \delta\omega, \end{aligned}\right.$$

con $\alpha, \beta, \gamma, \delta$ interi e, poichè queste formule debbono anche valere cangiando i in $-i$, si vede che anche $2\omega_0$, $-2\omega'_0$ saranno periodi fondamentali, cioè sarà $\alpha\delta - \beta\gamma = 1$. Ora essendo

$$-\tau_0 = \frac{\alpha\tau + \beta}{\gamma\tau + \delta} \qquad (\alpha\delta - \beta\gamma = 1)$$

il punto τ è equivalente, rispetto al gruppo modulare, al simmetrico rispetto all'asse immaginario e avremo perciò

a) $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} = \begin{pmatrix} 0, & \mp 1 \\ \pm 1, & 0 \end{pmatrix}$, se τ è sull'arco circolare,

b) $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} = \begin{pmatrix} \pm 1, & \pm 1 \\ 0, & \pm 1 \end{pmatrix}$, se τ è sul lato rettilineo $R(\tau) = -\frac{1}{2}$.

[1]) Prendiamo $-2\omega'_0$ in luogo di $2\omega'_0$, perchè il rapporto $-\frac{\omega'_0}{\omega_0}$ si conservi col coefficiente dell' immaginario positivo

In ambedue i casi diciamo che: *Si possono sostituire a* 2ω, $2\omega'$ *due nuovi periodi fondamentali* $2\omega_1$, $2\omega_3$ *tali che l'uno sia coniugato dell'altro.*

Pongasi invero

$$\omega_1 = r\,\omega + s\,\omega',$$

indi ω_3 eguale alla quantità coniugata

$$\omega_3 = r\,\omega_0 + s\,\omega'_0 = (r\delta - s\beta)\,\omega + (r\gamma - s\alpha)\,\omega';$$

basterà che determiniamo gli interi r, s in guisa che sia

$$r(r\gamma - s\alpha) - s(r\delta - s\beta) = 1$$

cioè

$$\gamma r^2 - (\alpha + \delta)\,r s + \beta s^2 = 1,$$

il che è possibile tanto nel caso a) quanto nel caso b).

Scelti così i due periodi fondamentali $2\omega_1$, $2\omega_3$ in guisa che l'uno sia coniugato dell'altro, poniamo

$$\omega_3 = a + i\,b, \quad \omega_1 = a - i\,b,$$

e supposto, come è lecito, $a > 0$ sarà altresì $b > 0$. La funzione $\wp u$ ammetterà anche i due periodi

$$2\omega_2 = 2\omega_3 + 2\omega_1 = 4a$$

$$2\omega'_2 = 2\omega_3 - 2\omega_1 = 4\,i\,b,$$

reale il primo e puramente immaginario il secondo, come nel caso del discriminante positivo. Per altro è da osservarsi che nel caso attuale questi due periodi $2\omega_2$, $2\omega'_3$, non sono più *fondamentali* come prima, perchè il determinante $\begin{vmatrix} 1, & 1 \\ -1, & 1 \end{vmatrix}$ della sostituzione, che li lega ai fondamentali, non è eguale all' unità ma a 2.

Nel rettangolo $(0, \omega_2, 2\omega_3, \omega'_2)$ della figura 11 (a pag. 140) la funzione $\wp u$, a causa della formola

$$\wp(2\omega_3 - u) = \wp u,$$

riprende *due volte* ogni valore; sul suo contorno essa è reale coll'andamento seguente:

$$u \text{ da } 0 \ldots \omega_2; \quad \omega_2 \ldots \omega_2 + \omega'_2 = 2\omega_3; \quad 2\omega_3 \ldots \omega'_2; \quad \omega'_2 \ldots 0$$

$$\wp u \text{ da } +\infty \ldots e_2; \quad e_2 \ldots -\infty; \quad +\infty \ldots e_2; \quad e_2 \ldots -\infty$$

e corrispondentemente la $\wp' u$ offre l'andamento seguente

$(0, \omega_2)$;	$(\omega_2, 2\omega_3)$;
$\wp' u$ reale negativa	$\wp' u$ immaginaria positiva
$(2\omega_3, \omega'_2)$;	$(\omega'_2, 0)$
$\wp' u$ reale positiva	$\wp' u$ immaginaria negativa

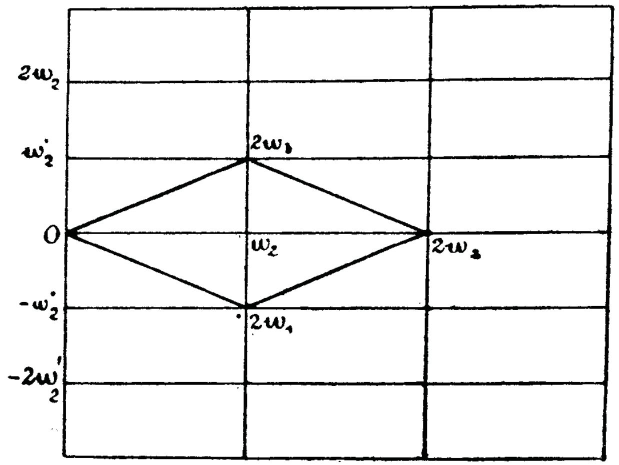

Fig. 11.

Nell' *interno* del detto rettangolo la $\wp u$ non è mai reale e per ciò il coefficiente dell' immaginario in $\wp u$ conserva sempre lo stesso segno, che si vede essere il negativo.

Vi ha un solo punto nell' interno ove $\wp' u$ si annulla, ed è il centro del rettangolo $u = \omega_3$, ove $\wp u = e_3$. L' immagine di questo rettangolo nel piano $s = \wp u$ ricopre due volte il semipiano negativo, avendo in $s = e_3$ un punto di diramazione del primo ordine.

Si osserverà che, per l'opportuna scelta dei periodi: *La radice media e_2 è reale, mentre e_1, e_3 sono immaginarie coniugate, la e_1 avendo positivo il coefficiente dell'immaginario; inoltre e_2 è positiva o negativa con g_3.*

Dallo studio precedente risulta che, se un argomento u rende simultaneamente

$$\wp u, \qquad \wp' u$$

reali, sarà u reale a meno di multipli del periodo immaginario $2\omega_3$. In questo caso adunque, per avere tutti i punti reali della cubica

$$x = \wp u, \qquad y = \wp u,$$

basterà far variare u per valori reali da $u = -\omega_2$ ad $u = \omega_2$ e quindi: *La cubica*

$$y^2 = 4x^3 - g_2 x - g_3$$

nel caso di

$$g_2^3 - 27 g_3^2 < 0$$

consta di un solo ramo infinito.

Anche in questo caso avremo tre soli flessi reali in linea retta, corrispondenti agli argomenti

$$u = 0, \quad \frac{2\omega_1 + 2\omega_3}{3}, \qquad \frac{4\omega_1 + 4\omega_3}{3}.$$

§ 143. — Degenerazione della funzione $\wp(u; g_2 g_3)$ nel caso $g_2^3 - 27 g_3^2 = 0$.

Esaminiamo ora quello che accade della funzione $\wp(u \mid \omega, \omega')$ quando il rapporto $\tau = \frac{\omega'}{\omega}$ dei periodi si fa tendere, per valori puramente immaginari, a ∞ ovvero a zero; allora $J(\tau)$ diventa infinito e il discriminante $g_2^3 - 27 g_3^2$, supposto che g_2 non vada a zero, tende a zero.

a) Se diamo ad ω un valore reale fisso e facciamo tendere $\omega' = i\beta\omega$ per valori puramente immaginari all'infinito, la serie

doppia che ci definisce la $\wp u$ (pag. 13) si cangia nella serie semplice:

$$\wp u = \frac{1}{u^2} + \sum_{m=1}^{m=\infty} \left\{ \frac{1}{(u - 2m\omega)^2} + \frac{1}{(u + 2m\omega)^2} \right\} - \frac{2}{(2\omega)^2} \sum \frac{1}{m^2}.$$

Ora a causa delle formole del § 64 (parte I, pag. 199) si ha

$$\frac{1}{u^2} + \sum_1^{\infty} \left\{ \frac{1}{(u - 2m\omega)^2} + \frac{1}{(u + 2m\omega)^2} \right\} = \left(\frac{\pi}{2\omega}\right)^2 \frac{1}{\operatorname{sen}^2\left(\frac{\pi u}{2\omega}\right)}$$

$$\sum_1^{\infty} \frac{1}{m^2} = \frac{\pi^2}{6}$$

e possiamo quindi enunciare il risultato:

Se, avendo ω un valore fisso reale, si fa crescere ω' all' infinito per valori puramente immaginari, la $\wp(u \mid \omega, \omega')$ degenera nella funzione circolare

$$\text{(A)} \qquad \wp u = -\frac{1}{3}\left(\frac{\pi}{2\omega}\right)^2 + \left(\frac{\pi}{2\omega}\right)^2 \frac{1}{\operatorname{sen}^2\left(\frac{\pi u}{2\omega}\right)}.$$

Conseguentemente la ζu e la σu degenerano anch'esse, secondo le formole

$$\zeta u = \frac{\pi}{2\omega} \cot\left(\frac{\pi u}{2\omega}\right) + \frac{1}{3}\left(\frac{\pi}{2\omega}\right)^2 u,$$

$$\sigma u = e^{\frac{1}{6}\left(\frac{\pi u}{2\omega}\right)^2} \frac{2\omega}{\pi} \operatorname{sen}\left(\frac{\pi u}{2\omega}\right).$$

b) Teniamo ora fisso $\omega' = i\beta$ puramente immaginario e facciamo crescere ω reale all' infinito, con che τ convergerà sull'asse immaginario a 0; si vedrà che la $\wp u$ degenera allora nella funzione iperbolica

$$\text{(B)} \qquad \wp u = \frac{1}{3}\left(\frac{\pi}{2\beta}\right)^2 + \left(\frac{\pi}{2\beta}\right)^2 \frac{1}{\operatorname{senh}^2\left(\frac{\pi u}{2\beta}\right)}.$$

Nei modi (A), (B) di degenerazione della $\wp u$ è chiaro che due delle radici e_1, e_2, e_3 vengono a coincidere e precisamente in (A) e_2 viene a coincidere con e_3, e nel caso (B) coincide e_2 con e_1.

e) Possiamo in fine considerare un terzo modo di degenerazione, corrispondente al caso che si abbia insieme $g_2 = g_3 = 0$. Basta per ciò far crescere ω, ω' simultaneamente all' infinito, conservando finito il loro rapporto; allora al limite si ha

$$\wp u = \frac{1}{u^2}, \qquad \zeta u = \frac{1}{u}, \qquad \sigma u = u$$

$$e_1 = e_2 = e_3 = 0.$$

§ 144. — Le funzioni sn v, cn v, dn v per valori reali positivi e < 1 di k^2.

Le funzioni ellittiche di Jacobi

$$\mathrm{sn}\, v, \quad \mathrm{cn}\, v, \quad \mathrm{dn}\, v$$

che si presentano nelle applicazioni (quando nella trattazione di un problema che porta alle funzioni ellittiche si vogliano introdurre quelle di Jacobi in luogo della $\wp u$ di Weierstrass) corrispondono sempre al caso in cui gli invarianti g_2, g_3 sono reali e il discriminante $g_2^3 - 27\, g_3^2 > 0$.

Allora e_1, e_2, e_3 sono reali e disposte per ordine decrescente e le formole *a*) *b*) *c*) § 130 (pagg. 105 e 106), dànno per

$$\sqrt{e_1 - e_2}, \qquad \sqrt{e_1 - e_3}, \qquad \sqrt{e_2 - e_3}$$

valori reali e positivi; quindi

$$k = \frac{\sqrt{e_2 - e_3}}{\sqrt{e_1 - e_3}}, \qquad k' = \frac{\sqrt{e_1 - e_2}}{\sqrt{e_1 - e_3}}$$

sono reali, positivi e < 1 e le quantità di Jacobi

$$K = \omega \sqrt{e_1 - e_3}, \qquad K' = \frac{\omega'}{i} \sqrt{e_1 - e_3}$$

sono pure reali e positive.

Le tre funzioni di Jacobi

$$\mathrm{sn}\, v, \quad \mathrm{cn}\, v, \quad \mathrm{dn}\, v$$

assumono valori reali sull'asse reale, mentre sull'asse immaginario la prima è puramente immaginaria e le due ultime sono ancora reali. Osserviamo ora specialmente l'andamento di sn v, cn v, dn v per valori reali dell'argomento. Le formole

$$\mathrm{sn}^2 v + \mathrm{cn}^2 v = 1$$

$$\mathrm{dn}^2 v + k^2\, \mathrm{sn}^2 v = 1$$

dimostrano che sn v, cn v sono sempre comprese fra -1 e $+1$ mentre dn v, che non s'annulla mai sull'asse reale, è sempre positiva e compresa fra 1 e k'.

Più in particolare, crescendo v da 0 a K, sn v cresce da 0 a 1, poi da K a $2K$ decresce da 1 a 0. Secondo la formola

$$\mathrm{sn}\,(2K + v) = -\,\mathrm{sn}\, v,$$

sn v cangia di segno fra $2K$ e $4K$, e al di là di $4K$ riprende periodicamente i medesimi valori. Analogamente succede per cn v e le curve

$$y = \mathrm{sn}\, x, \quad y = \mathrm{cn}\, x$$

hanno quindi una forma sinusoidale.

La curva

$$y = \mathrm{dn}\, x$$

ha il periodo $2K$ parallelo all'asse delle x e rimane tutta al di sopra di quest'asse, avendo per ordinata massima

$$y = 1 \ \text{ per } x = 0,\ \pm 2K,\ \pm 4K \ldots.$$

e per ordinata minima

$$y = k' \ \text{ per } x = \pm K,\ \pm 3K,\ \pm 5K \ldots.$$

Ogni tratto da $y = 1$ a $y = k'$ volge prima la concavità, indi la convessità all'asse delle x, flettendosi nel punto ove

$$\mathrm{sn}^2 x = \mathrm{cn}^2 x = \frac{1}{2}.$$

Mediante le formole di trasformazione complementare [(X*) § 137] si può ridurre il calcolo delle funzioni di Jacobi, nel caso che ci occupa, e per valori complessi qualunque dell'argomento, al caso di argomento reale, cioè possiamo separare in

$$\operatorname{sn}(\alpha+i\beta), \qquad \operatorname{cn}(\alpha+i\beta), \qquad \operatorname{dn}(\alpha+i\beta)$$

la parte reale dall'immaginaria. Si ha invero per le formole citate

$$\operatorname{sn}(i\beta,k)=i\,\frac{\operatorname{sn}(\beta,k')}{\operatorname{cn}(\beta,k')},$$

$$\operatorname{cn}(i\beta,k)=\frac{1}{\operatorname{cn}(\beta,k')}, \qquad \operatorname{dn}(i\beta,k)=\frac{\operatorname{dn}(\beta,k')}{\operatorname{cn}(\beta,k')}$$

e, servendosi delle formole d'addizione, si ottengono subito le formole richieste.

Così per es. si ha :

$$\operatorname{sn}(\alpha+i\beta,k)=$$

$$=\frac{\operatorname{sn}(\alpha,k)\operatorname{cn}(i\beta,k)\operatorname{dn}(i\beta,k)+\operatorname{sn}(i\beta,k)\operatorname{cn}(\alpha,k)\operatorname{dn}(\alpha,k)}{1-k^2\operatorname{sn}^2(\alpha,k)\operatorname{sn}^2(i\beta,k)}$$

e per ciò

$$\operatorname{sn}(\alpha+i\beta,k)=$$

$$=\frac{\operatorname{sn}(\alpha,k)\operatorname{dn}(\beta,k')+i\operatorname{sn}(\beta,k')\operatorname{cn}(\beta,k')\operatorname{cn}(\alpha,k)\operatorname{dn}(\alpha,k)}{\operatorname{cn}^2(\beta,k')+k'\operatorname{sn}^2(\alpha,k)\operatorname{sn}^2(\beta,k')}$$

e analogamente per

$$\operatorname{dn}(\alpha+i\beta), \qquad \operatorname{cn}(\alpha+i\beta).$$

§ 145. — Integrale ellittico di prima specie di Legendre. Integrali completi K, K'. - Degenerazione di $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$.

Dalla formola

$$\frac{d\operatorname{sn} v}{dv}=\operatorname{cn} v\operatorname{dn} v=\sqrt{(1-\operatorname{sn}^2 v)(1-k^2\operatorname{sn}^2 v)}$$

ponendo

$$\operatorname{sn} v = x$$

e osservando che per $v=0$ si ha $x=0$ risulta

$$v=\int_0^x\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}. \tag{3}$$

L'integrale del secondo membro è *l'integrale ellittico di prima specie* di Legendre. Limitandoci al caso delle applicazioni in cui k è reale, positivo <1, e la x varia da -1 a $+1$, si può porre

$$x=\operatorname{sen}\varphi,$$

ove φ è un angolo reale, e ne risulta

$$v=\int_0^\varphi\frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}}. \tag{4}$$

Legendre indicava col simbolo $F(\varphi,k)$ l'integrale del secondo membro, e dava il nome di *amplitudine* all'intervallo φ d'integrazione, onde appunto è derivato il nome di *seno amplitudine* alla funzione inversa

$$x=\operatorname{sn} v=\operatorname{sen}\varphi.$$

Osservando che si ha

$$\operatorname{sn} K = 1,$$

si ha subito per K l'espressione per integrale definito

$$K=\int_0^1\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}= \tag{5}$$

$$=\int_0^{\frac{\pi}{2}}\frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}}=F\left(\frac{\pi}{2},k\right).$$

Si può ottenere un'espressione analoga per K' osservando che, a causa delle formole

$$\operatorname{sn}(v+K)=\frac{\operatorname{cn} v}{\operatorname{dn} v}, \quad \operatorname{sn}(K+iK')=\frac{1}{k},$$

facendo crescere v pel cammino rettilineo da K a $K + i K'$, la $x = \operatorname{sn} v$ cresce, per valori reali, da 1 a $\frac{1}{k}$ e si ha per ciò:

$$K + i K' = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2 x^2)}} + \\ + \int_1^{\frac{1}{k}} \frac{dx}{\sqrt{(1-x^2)(1-k^2 x^2)}},$$

onde

$$K' = \int_1^{\frac{1}{k}} \frac{dx}{\sqrt{(x^2-1)(1-k^2 x^2)}}.$$

Cangiando in questo integrale la variabile x nella x', col porre

$$k^2 x^2 + k'^2 x'^2 = 1,$$

si ottiene subito

$$K' = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k'^2 x^2)}} = F\left(\frac{\pi}{2}, k'\right),$$

formola che, messa a confronto colla (5), dimostra che K' si esprime per k' come K per k, la qual cosa si poteva anche dedurre dalle formole di trasformazione complementare.

Per mezzo di queste formole vediamo subito come degenerano le funzioni ellittiche di Jacobi nei casi limiti:

$$k = 0, \quad k = 1.$$

Si ha infatti per $k = 0$

$$K = \frac{\pi}{2}, \qquad K' = \infty$$

$$\operatorname{sn} v = \operatorname{sen} v,$$

cioè

(7) $$\operatorname{sn}(v, 0) = \operatorname{sen} v, \quad \operatorname{cn}(v, 0) = \cos v, \quad \operatorname{dn}(v, 0) = 1.$$

Similmente dalle formole stesse, o da quelle della trasformazione complementare, deducesi

(8) $$\operatorname{sn}(v, 1) = \operatorname{tangh} v, \qquad \operatorname{cn}(v, 1) = \operatorname{dn}(v, 1) = \frac{1}{\cosh v}.$$

§ 146. — Gli integrali di seconda specie $E(v)$, $Z(v)$ di Legendre e Jacobi.

Nella teoria di Legendre, oltre all' integrale ellittico di prima specie

$$\int \frac{dx}{\sqrt{(1-x^2)(1-k^2 x^2)}},$$

si presentavano gli altri due integrali elementari

$$\int \frac{\sqrt{1-k^2 x^2}}{\sqrt{1-x^2}}\, dx, \qquad \int \frac{dx}{(1+n x^2)\sqrt{(1-x^2)(1-k^2 x^2)}},$$

che Legendre chiamava rispettivamente integrali di seconda e terza specie. L' integrazione di ogni funzione razionale

$$F(x, \sqrt{(1-x^2)(1-k^2 x^2)})$$

si riportava a funzioni ordinarie e ad un aggregato di integrali elementari delle tre specie (cfr. § 127). Per il confronto delle formole della teoria di Legendre, le quali si trovano adoperate in trattati e memorie classiche, con quelle di Weierstrass diamo le formole di passaggio alle funzioni σu e $\wp u$ di Weierstrass.

Ponendo $x = \operatorname{sn}(v, k)$, l' integrale di seconda specie di Legendre diventa

$$\int_0^x \frac{\sqrt{1-k^2 x^2}}{\sqrt{1-x^2}}\, dx = \int_0^v \operatorname{dn}^2 v\, dv.$$

Siccome la funzione $\mathrm{dn}^2 v$ ha residui tutti nulli (perchè nel parallelogrammo dei periodi $(2K, 2iK)$ $\mathrm{dn}^2 v$ ha un solo infinito), l' integrale stesso è una funzione monodroma di v che s' indica, secondo Legendre e Jacobi, con

$$E(v) = \int_0^v \mathrm{dn}^2 v \, dv .$$

Per esprimere $E(v)$ coi simboli di Weierstrass, osserviamo che si ha

$$\mathrm{dn}^2 v = \frac{\wp u - e_2}{\wp u - e_3} = 1 + \frac{e_3 - e_2}{\wp u - e_3} \quad (v = u\sqrt{e_1 - e_2}),$$

e per le formole d'addizione dei semi periodi:

$$\mathrm{dn}^2 v = \frac{e_1}{e_1 - e_3} - \frac{1}{e_1 - e_3} \wp(u + \omega') .$$

Risulta quindi

$$E(v) = \frac{1}{\sqrt{e_1 - e_3}} \left\{ \frac{\sigma'(u + \omega')}{\sigma(u + \omega)} + e_1 u - \eta' \right\},$$

ovvero

$$\text{(I)} \qquad E(v) = \frac{1}{\sqrt{e_1 - e_3}} \left\{ \frac{\sigma_3' u}{\sigma_3 u} + e_1 u \right\}, \quad v = u\sqrt{e_1 - e_3},$$

che è la formola richiesta.

Indicando poi, come faceva Legendre, con E *l' integrale completo*:

$$E = \int_0^1 \frac{\sqrt{1 - k^2 x^2}}{\sqrt{1 - x^2}} \, dx = \int_0^K \mathrm{dn}^2 v \, dv ,$$

avremo dalla (I)

$$\text{(I*)} \qquad E = \frac{1}{\sqrt{e_1 - e_3}} (e_1 \omega + \eta) .$$

Ponendo $x = \operatorname{sen} \varphi$, Legendre usava per l' integrale di seconda specie la notazione

$$\int_0^x \frac{\sqrt{1 - k^2 x^2}}{\sqrt{1 - x^2}} \, dx = \int_0^\varphi \sqrt{1 - k^2 \operatorname{sen}^2 \varphi} \, d\varphi = E(\varphi, k),$$

talchè l' integrale completo E è dato da $E\left(\frac{\pi}{2}, k\right)$.

L' integrale $E(\varphi, k)$ si presenta appunto nel calcolo dell'arco dell'ellisse. Se si esprimono le coordinate di un punto mobile sull'ellisse di semiassi a, b, per l'angolo eccentrico φ colle formole

$$x = a \operatorname{sen} \varphi, \qquad y = b \cos \varphi ,$$

e si pone

$$k = \frac{\sqrt{a^2 - b^2}}{a} \quad \text{(eccentricità)},$$

per l'arco s di ellisse, contato a partire dall'estremità dell' asse minore, si ha

$$s = a \int_0^\varphi \sqrt{1 - k^2 \operatorname{sen}^2 \varphi} \, d\varphi = a E(\varphi, k).$$

L' integrale completo $E\left(\frac{\pi}{2}, k\right) = E$ misura adunque la lunghezza di un quadrante dell' ellisse di semi-asse maggiore $= 1$ e di eccentricità k.

All' integrale di seconda specie di Legendre Jacobi sostituiva l'altro

$$\int_0^x \frac{x^2 \, dx}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} =$$

$$= \frac{1}{k^2} \left[\int_0^x \frac{dx}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} - \int_0^x \frac{\sqrt{1 - k^2 x^2}}{\sqrt{1 - x^2}} \, dx \right],$$

e indicava col simbolo $Z(v)$ la funzione

$$Z(v) = E(v) - \frac{E}{K} v.$$

La $Z(v)$ di Jacobi si esprime, per le (I) (I*), mediante le funzioni di Weierstrass colla formola:

$$\text{(II)} \qquad Z(v) = \frac{1}{\sqrt{e_1 - e_3}} \left[\frac{\sigma'_3 u}{\sigma_3 u} - \frac{\eta}{\omega} u \right], \quad v = u\sqrt{e_1 - e_3}.$$

§ 147. — L' integrale di terza specie $\Pi(v, a)$ di Jacobi.

Jacobi considerava come integrale di terza specie il seguente

$$\int \frac{x^2\, dx}{(1 + n x^2)\sqrt{(1 - x^2)\,(1 - k^2 x^2)}},$$

che si compone evidentemente con integrali di prima e terza specie di Legendre. Ponendo $x = \operatorname{sn} v$ e indicando con a una conveniente costante, Jacobi indicava col simbolo

$$\Pi(v, a)$$

l' integrale di terza specie

$$\Pi(v, a) = k^2 \operatorname{sn} a \operatorname{cn} a \operatorname{dn} a \int_0^v \frac{\operatorname{sn}^2 v\, dv}{1 - k^2 \operatorname{sn}^2 a \operatorname{sn}^2 v},$$

che vogliamo qui esprimere per funzioni di Weierstrass. A tale scopo rammentiamo le formole

$$\left.\begin{aligned} \operatorname{sn} v &= \sqrt{e_1 - e_3}\,\frac{\sigma u}{\sigma_3 u} = \frac{\sqrt{e_1 - e_3}}{\sqrt{\wp u - e_3}} \\ \operatorname{cn} v &= \frac{\sigma_1 u}{\sigma_3 u} = \frac{\sqrt{\wp u - e_1}}{\sqrt{\wp u - e_3}} \\ \operatorname{dn} v &= \frac{\sigma_2 u}{\sigma_3 u} = \frac{\sqrt{\wp u - e_2}}{\sqrt{\wp u - e_3}} \end{aligned}\right\} \begin{aligned} v &= u\sqrt{e_1 - e_3} \\ k^2 &= \frac{e_2 - e_3}{e_1 - e_3} \end{aligned}$$

e ponendo per brevità

$$b = \frac{a}{\sqrt{e_1 - e_3}},$$

troveremo:

$$\Pi(v, a) = (e_1 - e_3)(e_2 - e_3)\,\frac{\sigma b \cdot \sigma_1 b \cdot \sigma_2 b}{\sigma_3^3 b} \int_0^u \frac{du}{\wp u - \dfrac{(e_1 - e_3)(e_2 - e_3)}{\wp b - e_3}}.$$

Ora, ricordando le formole

$$\wp' u = -\frac{2\,\sigma_1 u\, \sigma_2 u\, \sigma_3 u}{\sigma^3 u}, \qquad \wp(u + \omega') - e_3 = \frac{(e_1 - e_3)(e_2 - e_3)}{\wp u - e_3},$$

$$\wp'(u + \omega') = -\frac{(e_1 - e_3)(e_2 - e_3)\,\wp' u}{(\wp u - e_3)^2}$$

avremo subito

$$\Pi(v, a) = \frac{1}{2} \int_0^u \frac{\wp'(b + \omega')}{\wp u - \wp(b + \omega')}\, du.$$

Ma, per le formole d'addizione della ζu, si ha

$$\frac{1}{2}\,\frac{\wp'(b + \omega')}{\wp u - \wp(b + \omega')} = \frac{1}{2}\,\zeta(u - b - \omega') -$$

$$- \frac{1}{2}\,\zeta(u + b + \omega') + \zeta(b + \omega'),$$

ed essendo

$$\zeta(u - b - \omega') = \frac{\sigma'_3(u - b)}{\sigma_3(u - b)} - \eta',$$

$$\zeta(u + b + \omega') = \frac{\sigma'_3(u + b)}{\sigma_3(u + b)} + \eta',$$

potremo scrivere

$$\frac{1}{2}\,\frac{\wp'(b + \omega')}{\wp u - \wp(b + \omega')} = \frac{1}{2}\,\frac{\sigma'_3(u - b)}{\sigma_3(u - b)} - \frac{1}{2}\,\frac{\sigma'_3(u + b)}{\sigma_3(u + b)} + \frac{\sigma'_3 b}{\sigma_3 b},$$

onde infine avremo per la formola cercata

$$\text{(III)} \qquad \Pi(v, a) = \frac{1}{2} \log \frac{\sigma_3(u - b)}{\sigma_3(u + b)} + \frac{\sigma'_3 b}{\sigma_3 b}\, u \quad \left\{ \begin{aligned} v &= u\sqrt{e_1 - e_3} \\ b &= a\sqrt{e_1 - e_3}. \end{aligned} \right.$$

§ 148. — Riduzione dell'integrale ellittico di prima specie alla forma normale di Legendre.

Per completare queste notizie sull'antica teoria degli integrali ellittici, daremo ancora il processo che serve a ridurre il differenziale ellittico di prima specie

$$\frac{dw}{\sqrt{P(w)}}, \tag{9}$$

ove $P(w)$ è un polinomio di terzo o quarto grado in w, alla forma normale di Legendre

$$\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} \tag{10}$$

e, avendo riguardo ai casi che effettivamente si presentano nelle applicazioni ove $P(w)$ è a coefficienti reali, dimostreremo come la riduzione possa sempre farsi in guisa che ne risulti k^2 reale, positivo e <1.

Basterà che riduciamo, con una sostituzione razionale, il differenziale (9) alla forma

$$\frac{dy}{\sqrt{y(1-y)(1-k^2y)}} \tag{11}$$

poichè la sostituzione quadratica

$$y = x^2$$

fa passare dalla forma (11) alla (10). Ora il passaggio dalla (9) alla (11) si può sempre conseguire con una sostituzione lineare

$$w = \frac{a+by}{c+dy}. \tag{12}$$

E invero, se $P(w)$ è del terzo grado, si prenda semplicemente

$$w = a + by$$

e si determinino a, b in guisa che una radice α di $P(w)=0$ venga portata in $y=0$ ed una seconda β in $y=1$; si ponga cioè

$$w = \alpha + (\beta - \alpha)\, y.$$

Allora, posto

$$P(w) = A(w-\alpha)(w-\beta)(w-\gamma),$$

risulterà

$$\frac{dw}{\sqrt{P(w)}} = C\,\frac{dy}{\sqrt{y(1-y)(1-k^2y)}},$$

ove si è posto

$$C = \frac{1}{\sqrt{A(\gamma-\alpha)}}, \qquad k^2 = \frac{\beta-\alpha}{\gamma-\alpha}\ [1].$$

Sia ora $P(w)$ del quarto grado e, omettendo un fattore costante, scriviamo

$$P(w) = (w-\alpha)(w-\beta)(w-\gamma)(w-\delta).$$

La sostituzione (12) dà:

$$\frac{dw}{\sqrt{P(w)}} =$$

$$= \frac{(bc-ad)\,dy}{(c+dy)^2\sqrt{\left(\frac{a+by}{c+dy}-\alpha\right)\left(\frac{a+by}{c+dy}-\beta\right)\left(\frac{a+by}{c+dy}-\gamma\right)\left(\frac{a+by}{c+dy}-\delta\right)}}.$$

Perchè questo differenziale abbia la forma voluta (11), basta che uno dei binomî sotto il segno, per es. $w-\beta$, si riduca a $\frac{c'}{c+dy}$, cioè che la radice β di $P(w)=0$ sia portata in $y=\infty$, e gli altri binomî si annullino rispettivamente per $y = 0, 1, \frac{1}{k^2}$. La (12) dovrà dunque portare rispettivamente α, β, γ in $0, \infty, 1$, e sarà per ciò

$$y = \frac{\gamma-\beta}{\gamma-\alpha}\,\frac{w-\alpha}{w-\beta}.$$

[1]) Si osservi che k^2 è il rapporto anarmonico dei quattro valori $\alpha, \infty, \beta, \gamma$.

La quarta radice δ viene portata in

$$\frac{\gamma-\beta}{\gamma-\alpha}\ \frac{\delta-\alpha}{\delta-\beta},$$

onde si ha

$$k^2 = (\alpha\,\beta\,\gamma\,\delta) = \frac{\alpha-\gamma}{\alpha-\delta}\cdot\frac{\beta-\delta}{\beta-\gamma}.$$

Dipendentemente dall'ordine delle quattro radici si potrà effettuare la riduzione richiesta in 24 modi diversi, ai quali corrispondono però soltanto sei valori del rapporto anarmonico:

$$k^2,\quad \frac{1}{k^2},\quad 1-k^2,\quad \frac{1}{1-k^2},\quad \frac{k^2}{k^2-1},\quad \frac{k^2-1}{k^2}.$$

Se $P(w)$ è a coefficienti reali e le sue radici sono tutte reali, o tutte complesse, i sei valori del rapporto anarmonico sono reali ed uno di essi è positivo e < 1.

Quando si avessero invece due radici reali α, β e due immaginarie (coniugate) γ, δ, colla trasformazione

$$t^2 = \frac{w-\alpha}{w-\beta}$$

risulterebbe

$$\frac{dw}{\sqrt{P(w)}} = \frac{2(\alpha-\beta)}{\sqrt{(\beta-\gamma)(\beta-\delta)}}\ \frac{dt}{\sqrt{\left(t^2-\frac{\alpha-\gamma}{\beta-\gamma}\right)\left(t^2-\frac{\alpha-\delta}{\beta-\delta}\right)}}$$

e il polinomio di quarto grado in t avrebbe radici tutte complesse, talchè si ricade nel caso precedente.

Nel caso di un polinomio $P(w)$ di terzo grado a radici reali si avrà ancora immediatamente il medesimo risultato. E se una delle radici è reale, le altre due immaginarie, con una sostituzione lineare ci ricondurremo al caso di un polinomio di quarto grado con due radici reali e due immaginarie.

Per ridurre il differenziale ellittico di prima specie alla forma normale di Legendre occorre, come si vede, conoscere le radici di $P(w) = 0$. Uno dei principali vantaggi del metodo di Weierstrass (cap. X, §§ 124–127) è appunto questo che la riduzione alla forma normale si effettua razionalmente per gli invarianti, ossia pei coefficienti del polinomio $P(w)$.

CAPITOLO XIV.

Sviluppi in prodotti infiniti ed in serie trigonometriche delle funzioni σ. — Le serie ϑ di Jacobi e le loro proprietà.

§ 149. — Sviluppo in prodotto infinito semplice per $\sigma_3 u$.

Ci proponiamo ora di far conoscere le principali espressioni analitiche per prodotti infiniti e per serie trigonometriche delle funzioni ellittiche e loro affini. Questi sviluppi presentano un grande interesse teorico e pratico insieme, per la loro legge di costruzione e per la loro rapida convergenza nei casi delle applicazioni, che li rende molto adatti al calcolo numerico.

Cominceremo dal dare gli sviluppi in prodotti infiniti semplici delle funzioni σ, σ_1, σ_2, σ_3 di Weierstrass. Potremmo per ciò ricorrere allo sviluppo della σu in prodotto infinito doppio (§ 94), convertirlo in prodotto infinito semplice e dedurne poi i prodotti infiniti per le altre σ_r. Qui preferiamo dedurre queste espressioni analitiche direttamente dalle proprietà caratteristiche della $\sigma_r u$.

Prendiamo per es. la $\sigma_3 u$; essa gode delle seguenti proprietà:

1ª è una trascendente intera cogli infinitesimi del primo ordine nei punti

$$u_0 = 2m\omega + (2n+1)\omega'$$

2ª aumentando l'argomento u di 2ω o $2\omega'$, essa si comporta nel modo seguente (§ 129)

$$(a)\qquad \begin{cases} \sigma_3(u+2\omega) = e^{2\eta(u+\omega)}\,\sigma_3 u \\ \sigma_3(u+2\omega') = -e^{2\eta'(u+\omega')}\,\sigma_3 u \end{cases}$$

3ª per $u=0$ è $\sigma_3 u = 1$.

Queste sono, come subito si vede, proprietà *caratteristiche* della $\sigma_3 u$, cioè, se una trascendente intera $G(u)$ vi soddisfa, essa coincide con $\sigma_3 u$.

Sostituiamo alla $\sigma_3 u$ un'altra trascendente intera periodica di terza categoria (§ 101) $\psi(u)$, che abbia il periodo assoluto 2ω. Pongasi per ciò

$$\psi(u) = e^{\frac{-\eta u^2}{2\omega}} \sigma_3 u$$

e la $\psi(u)$ avrà le proprietà 1ª e 3ª della $\sigma_3 u$, mentre la 2ª, a causa di $\eta\omega' - \eta'\omega = \frac{\pi i}{2}$, si tradurrà nelle altre

$$(a^*) \qquad \begin{cases} \psi(u + 2\omega) = \psi(u) \\ \psi(u + 2\omega') = -e^{-\frac{\pi i}{\omega}(u+\omega')} \psi(u). \end{cases}$$

Pongasi ora

$$e^{\frac{\pi i u}{\omega}} = z, \qquad e^{\frac{\pi i \omega'}{\omega}} = q,$$

onde sarà q una costante di modulo < 1, e si consideri $\psi(u)$ come funzione di z

$$\psi(u) = \varphi(z).$$

La $\varphi(z)$ sarà una funzione *monodroma* di z sempre finita e continua, tranne che nei due punti singolari (essenziali) $z = 0$, $z = \infty$, e godrà delle seguenti proprietà:

1ª $\varphi(z)$ ha infinitesimi del primo ordine nei punti

$$z_0 = \begin{cases} q, \quad q^3, \quad q^5 \; \ldots. \; q^{2n+1} \quad \ldots. \\ q^{-1}, \; q^{-3}, \; q^{-5} \ldots. \; q^{-(2n+1)} \ldots. \end{cases}$$

2ª $\varphi(z)$ soddisfa all'equazione funzionale

$$\varphi(q^2 z) = -\frac{1}{qz}\varphi(z).$$

3ª per $z = 1$ è $\varphi(z) = 1$.

Ora poichè la serie

$$q + q^3 + q^5 + \ldots.$$

converge assolutamente, a causa di $|q| < 1$, è facile (§ 66) costruire una prima funzione che abbia gli infinitesimi nei punti

$$z_0 = q^{-1}, \quad q^{-3}, \quad q^{-5} \ldots,$$

come pure una seconda che li abbia invece in

$$z_0 = q, \; q^3, \; q^5 \ldots.$$

Esse saranno date rispettivamente dai due prodotti infiniti

$$\prod_{n=1}^{n=\infty} (1 - q^{2n-1} z), \qquad \prod_{n=1}^{n=\infty} \left(1 - \frac{q^{2n-1}}{z}\right),$$

dei quali il primo converge assolutamente ed in egual grado in qualunque campo finito ed il secondo in tutto il piano, escluso $z = 0$. Riunendo i due prodotti, si ha la funzione

$$\prod_{n=1}^{n=\infty} (1 - q^{2n-1} z)\left(1 - \frac{q^{2n-1}}{z}\right),$$

che ha le proprietà prima e seconda della $\varphi(z)$, e non differisce quindi da $\varphi(z)$ che per un fattore costante; si trova subito

$$\varphi(z) = \prod_{n=1}^{n=\infty} \frac{(1 - q^{2n-1} z)\left(1 - \frac{q^{2n-1}}{z}\right)}{(1 - q^{2n-1})^2},$$

e ponendo per z il suo valore, abbiamo così la prima espressione analitica cercata per la $\sigma_3 u$ sotto la forma:

$$a) \qquad e^{\frac{-\eta u^2}{2\omega}} \cdot \sigma_3 u = \prod_{n=1}^{n=\infty} \frac{\left(1 - q^{2n-1} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n-1} e^{\frac{-\pi i u}{\omega}}\right)}{(1 - q^{2n-1})^2}.$$

§ 150. — Sviluppi in prodotti infiniti per le σ, σ_r e per le costanti $\sqrt{e_1-e_2}$, $\sqrt{e_1-e_3}$, $\sqrt{e_2-e_3}$, $\sqrt[24]{\Delta}$.

Dallo sviluppo ora trovato per $\sigma_3 u$, ricorrendo alle formole del § 131, facilmente ritroviamo gli sviluppi analoghi per le rimanenti σ. Si ha infatti

$$\sigma u = A\, e^{\eta' u}\, \sigma_3 (u - \omega'),$$

dove A è una costante, e per ciò

$$e^{\frac{-\eta u^2}{2\omega}} \sigma u = A' e^{\left(\eta' - \frac{\eta\omega'}{\omega}\right) u} \prod_{n=1}^{n=\infty} \left(1 - q^{2n-2} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n} e^{\frac{-\pi i u}{\omega}}\right),$$

ossia

$$e^{\frac{-\eta u^2}{2\omega}} \sigma u = A' e^{\frac{-\pi i u}{2\omega}} \left(1 - e^{\frac{\pi i u}{\omega}}\right) \prod_{n=1}^{n=\infty} \left(1 - q^{2n} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n} e^{\frac{-\pi i u}{\omega}}\right) =$$

$$= A'' \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) \prod_{n=1}^{n=\infty} \left(1 - q^{2n} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n} e^{\frac{-\pi i u}{\omega}}\right).$$

Per determinare A'' si divida dall' una e dall'altra parte per u e si passi al limite per $u = 0$, osservando che

$$\lim_{u=0} \left(\frac{\sigma u}{u}\right) = 1, \qquad \lim_{u=0} \frac{\operatorname{sen}\left(\frac{\pi u}{2\omega}\right)}{u} = \frac{\pi}{2\omega},$$

e si troverà quindi

$$(\beta) \qquad e^{\frac{-\eta u^2}{2\omega}} \sigma u = \frac{2\omega}{\pi} \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) \prod_{n=1}^{n=\infty} \frac{\left(1 - q^{2n} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n} e^{\frac{-\pi i u}{\omega}}\right)}{(1 - q^{2n})^2}.$$

Dalle α) β), mediante le formole

$$\left.\begin{aligned} \sigma_2 u &= B\, e^{-\eta u}\, \sigma_3 (u + \omega) \\ \sigma_1 u &= C\, e^{-\eta u}\, \sigma\, (u + \omega) \end{aligned}\right\} \quad B,\ C \text{ costanti},$$

si deducono subito gli sviluppi analoghi per $\sigma_1 u$, $\sigma_2 u$. Riuniamo le quattro formole nella tabella seguente:

$$(\mathrm{I}) \left\{ \begin{aligned}
e^{\frac{-\eta u^2}{2\omega}} \sigma u &= \frac{2\omega}{\pi} \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) \prod_{n=1}^{n=\infty} \frac{\left(1 - q^{2n} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n} e^{\frac{-\pi i u}{\omega}}\right)}{(1 - q^{2n})^2} = \\
&= \frac{2\omega}{\pi} \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) \prod_{n=1}^{n=\infty} \frac{1 - 2 q^{2n} \cos \frac{\pi u}{\omega} + q^{4n}}{(1 - q^{2n})^2} \\
e^{\frac{-\eta u^2}{2\omega}} \sigma_1 u &= \cos\left(\frac{\pi u}{2\omega}\right) \prod_{1}^{\infty} \frac{\left(1 + q^{2n} e^{\frac{\pi i u}{\omega}}\right)\left(1 + q^{2n} e^{\frac{-\pi i u}{\omega}}\right)}{(1 + q^{2n})^2} = \\
&= \cos\left(\frac{\pi u}{2\omega}\right) \prod_{1}^{\infty} \frac{1 + 2 q^{2n} \cos \frac{\pi u}{\omega} + q^{4n}}{(1 + q^{2n})^2} \\
e^{\frac{-\eta u^2}{2\omega}} \sigma_2 u &= \prod_{1}^{\infty} \frac{\left(1 + q^{2n-1} e^{\frac{\pi i u}{\omega}}\right)\left(1 + q^{2n-1} e^{\frac{-\pi i u}{\omega}}\right)}{(1 + q^{2n-1})^2} = \\
&= \prod_{1}^{\infty} \frac{1 + 2 q^{2n-1} \cos \frac{\pi u}{\omega} + q^{4n-2}}{(1 - q^{2n-1})^2}. \\
e^{\frac{-\eta u^2}{2\omega}} \sigma_3 u &= \prod_{1}^{\infty} \frac{\left(1 - q^{2n-1} e^{\frac{\pi i u}{\omega}}\right)\left(1 - q^{2n-1} e^{\frac{-\pi i u}{\omega}}\right)}{(1 - q^{2n-1})^2} = \\
&= \prod_{1}^{\infty} \frac{1 - 2 q^{2n-1} \cos \frac{\pi u}{\omega} + q^{4n-2}}{(1 - q^{2n-1})^2}.
\end{aligned}\right.$$

Dalle formole precedenti e dalle (a) (b) (c), (pagg. 105 e 106), che dànno la precisa definizione dei valori delle costanti

$$\sqrt{e_1 - e_2}, \qquad \sqrt{e_1 - e_3}, \qquad \sqrt{e_2 - e_3},$$

possiamo dedurre gli sviluppi in prodotti infiniti per queste ultime quantità.

Osserviamo a tale scopo che, ponendo

$$(1)\qquad U_1 = e^{\frac{-\eta_1\omega_1}{2}}\,\sigma\omega_1\,,\qquad U_2 = e^{\frac{-\eta_2\omega_2}{2}}\,\sigma\omega_2\,,\qquad U_3 = e^{\frac{-\eta_3\omega_3}{2}}\,\sigma\omega_3\,,$$

le citate formole ci dànno

$$(2)\qquad \begin{cases} \sqrt{e_1-e_2} = e^{\eta_2\omega_1}\dfrac{\sigma\omega_3}{\sigma\omega_1\,\sigma\omega_2} = e^{-\frac{\pi i}{4}}\dfrac{U_3}{U_1U_2} \\[2ex] \sqrt{e_2-e_3} = -\,e^{\eta_3\omega_2}\dfrac{\sigma\omega_1}{\sigma\omega_2\,\sigma\omega_3} = -\,e^{-\frac{\pi i}{4}}\dfrac{U_1}{U_2U_3} \\[2ex] \sqrt{e_1-e_3} = e^{-\eta_3\omega_1}\dfrac{\sigma\omega_2}{\sigma\omega_1\,\sigma\omega_3} = e^{-\frac{\pi i}{4}}\dfrac{U_2}{U_1U_3}\,, \end{cases}$$

e tutto si riduce quindi a calcolare U_1, U_2, U_3.

Nelle formole (I) figurano i seguenti quattro prodotti infiniti;

$$(3)\qquad Q_0 = \prod_1^\infty (1-q^{2n})\,,\qquad Q_1 = \prod_1^\infty (1+q^{2n})\,,$$

$$Q_2 = \prod_1^\infty (1+q^{2n-1})\,,\qquad Q_3 = \prod_1^\infty (1-q^{2n-1})\,,$$

che moltiplicati fra loro danno

$$Q_0\,Q_1\,Q_2\,Q_3 = \prod_1^\infty (1-q^{4n})\,(1-q^{4n-2}) = Q_0\,,$$

e fra gli ultimi tre sussiste per ciò l'identità

$$(4)\qquad Q_1\,Q_2\,Q_3 = 1.$$

Ora per calcolare U_1 facciamo nella prima delle (I) $u=\omega$ ed avremo subito

$$(a)\qquad U_1 = \frac{2\omega}{\pi}\,\frac{Q_1^2}{Q_0^2}\,.$$

Se nella medesima formola (I) facciamo poi $u=\omega'$ risulterà

$$e^{\frac{-\eta\omega'^2}{2\omega}}\,\sigma\omega' = \frac{2\omega}{\pi}\,\frac{e^{\frac{\pi i\omega'}{2\omega}} - e^{\frac{-\pi i\omega'}{2\omega}}}{2i}\prod_1^\infty \frac{(1-q^{2n+1})\,(1-q^{2n-1})}{(1-q^{2n})^2}\,,$$

cioè

$$e^{\frac{-\eta\omega'^2}{2\omega}}\,\sigma\omega' = \frac{2\omega}{\pi}\,e^{\frac{-\pi i\omega'}{2\omega}}\,\frac{q-1}{2i}\,\frac{1}{1-q}\,\frac{Q_3^2}{Q_0^2} = \frac{2\omega}{\pi}\,\frac{i}{2q^{\frac{1}{2}}}\,\frac{Q_3^2}{Q_0^2}\,,$$

ed osservando che si ha

$$\frac{\eta\omega'^2}{2\omega} = \frac{\omega'}{2\omega}\left(\eta'\omega + \frac{\pi i}{2}\right)$$

ne dedurremo

$$(b)\qquad U_3 = \frac{2\omega}{\pi}\,\frac{i}{2q^{\frac{1}{4}}}\,\frac{Q^2}{Q_0^2}\,.$$

In fine per calcolare

$$U_2 = e^{\frac{-\eta_2\omega_2}{2}}\,\sigma\omega_2\,,$$

ricorriamo alla formola

$$\sigma\omega_2 = e^{\eta'\omega}\,\sigma\omega'\cdot\sigma_3\omega$$

e facendo $u=\omega$ nella quarta delle (I), coll'osservare la (b), avremo:

$$\sigma\omega_2 = e^{\eta'\omega + \frac{\eta'\omega'}{2}}\cdot\frac{2\omega}{\pi}\,\frac{i}{2q^{\frac{1}{4}}}\cdot\frac{Q_3^2}{Q_0^2}\,e^{\frac{\eta\omega}{2}}\cdot\frac{Q_2^2}{Q_3^2} =$$

$$= e^{\frac{(\eta+\eta')(\omega+\omega')}{2} - \frac{\pi i}{4}}\cdot\frac{2\omega}{\pi}\,\frac{i}{2q^{\frac{1}{4}}}\,\frac{Q_2^2}{Q_0^2}$$

onde in fine

$$U_2 = \frac{2\omega}{\pi} \, \frac{e^{\frac{\pi i}{4}}}{2 q^{\frac{1}{4}}} \, \frac{Q_2^2}{Q_0^2}. \tag{c}$$

Dopo di ciò le (2), tenendo conto della identità (4), ci daranno

$$\sqrt{e_1 - e_2} = \frac{\pi}{2\omega} Q_3^4 Q_0^2, \quad \sqrt{e_2 - e_3} = \frac{\pi}{2\omega} \, 4 q^{\frac{1}{2}} Q_1^4 Q_0^2, \tag{5}$$

$$\sqrt{e_1 - e_3} = \frac{\pi}{2\omega} Q_2^4 Q_0^2.$$

Estraendo ancora la radice quadrata, coll'adottare una delle due determinazioni di segno, avremo:

$$\sqrt[4]{e_1 - e_2} = \sqrt{\frac{\pi}{2\omega}} \, Q_3^2 Q_0, \quad \sqrt[4]{e_2 - e_3} = \sqrt{\frac{\pi}{2\omega}} \cdot 2 q^{\frac{1}{4}} Q_1^2 Q_0, \tag{5*}$$

$$\sqrt[4]{e_1 - e_3} = \sqrt{\frac{\pi}{2\omega}} \cdot Q_2^2 Q_0.$$

Di qui risulta una notevole espressione per

$$\sqrt[24]{\Delta}$$

e cioè

$$\sqrt[24]{\Delta} = \sqrt[24]{g_2^3 - 27 g_3^2} = \sqrt{\frac{\pi}{\omega}} \, q^{\frac{1}{12}} \prod_{1}^{\infty} (1 - q^{2n}). \tag{II}$$

§ 151. — Sviluppi per $\sqrt{\frac{2K}{\pi}}$, $\sqrt[4]{k}$, $\sqrt[4]{k'}$, $\sqrt[12]{k k'}$ e per le funzioni $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$.

La quantità K di Jacobi è data (§ 133) da

$$K = \omega \sqrt{e_1 - e_3},$$

e per la terza delle (5) si ha quindi la formola

$$\sqrt{\frac{2K}{\pi}} = Q_2^2 Q_0 = \prod_{1}^{\infty} (1 + q^{2n-1})^2 (1 - q^{2n}), \tag{III}$$

formola che fa conoscere il periodo $4K$ delle funzioni ellittiche di Jacobi, appena noto

$$q = e^{\pi i \tau}.$$

Dalle (5) seguono ancora le formole

$$k = 4 q^{\frac{1}{2}} \frac{Q_1^4}{Q_2^4}, \qquad k' = \frac{Q_3^4}{Q_2^4}$$

ed, estraendo le radici quarte, abbiamo le altre notevoli

$$\left\{ \begin{aligned} \sqrt[4]{k} &= \sqrt{2}\, q^{\frac{1}{8}} \frac{Q_1}{Q_2} = \sqrt{2}\, e^{\frac{\pi i \tau}{8}} \prod_{1}^{\infty} \frac{1 + e^{2n\pi i \tau}}{1 + e^{(2n-1)\pi i \tau}} \\ \sqrt[4]{k'} &= \frac{Q_3}{Q_2} = \prod_{1}^{\infty} \frac{1 - e^{(2n-1)\pi i \tau}}{1 + e^{(2n-1)\pi i \tau}}. \end{aligned} \right. \tag{IV}$$

I prodotti infiniti dei secondi membri convergono assolutamente ed in egual grado in ogni campo finito del semipiano positivo τ, l'asse reale escluso e definiscono $\sqrt[4]{k}$, $\sqrt[4]{k'}$ come funzioni uniformi in questo semipiano (funzioni modulari).

È degna ancora di nota la formola che risulta moltiplicando le (IV), il che dà

$$\sqrt[4]{k k'} = \sqrt{2}\, q^{\frac{1}{8}} \frac{Q_1 Q_3}{Q_2^2}.$$

Per l'identità (4) possiamo scrivere

$$\sqrt[4]{k k'} = \sqrt{2}\, q^{\frac{1}{8}} \frac{1}{Q_2^3}$$

ed, estraendo ancora la radice terza, abbiamo

$$\sqrt[12]{k k'} = \sqrt[6]{2}\, q^{\frac{1}{24}} \frac{1}{Q_2} = \sqrt[6]{2}\, e^{\frac{\pi i \tau}{24}} \frac{1}{\prod_{1}^{\infty} (1 + e^{(2n-1)\pi i \tau})}. \tag{V}$$

Tenendo conto delle formole precedenti e delle fondamentali (I), possiamo ora esprimere le funzioni ellittiche di Jacobi per prodotti infiniti ed otteniamo le formole seguenti :

$$
\text{(VI)}\left\{
\begin{aligned}
\operatorname{sn} v &= \frac{2\,q^{\frac{1}{4}}}{\sqrt{k}} \operatorname{sen}\left(\frac{\pi v}{2K}\right) \prod_1^{\infty} \frac{1-2\,q^{2n}\cos\left(\frac{\pi v}{K}\right)+q^{4n}}{1-2\,q^{2n-1}\cos\left(\frac{\pi v}{K}\right)+q^{4n-2}}\,,\\
\operatorname{cn} v &= 2\,q^{\frac{1}{4}} \sqrt{\frac{k'}{k}} \cos\left(\frac{\pi v}{2K}\right) \prod_1^{\infty} \frac{1+2\,q^{2n}\cos\left(\frac{\pi v}{K}\right)+q^{4n}}{1-2\,q^{2n-1}\cos\left(\frac{\pi v}{K}\right)+q^{4n-2}}\,,\\
\operatorname{dn} v &= \sqrt{k'} \prod_1^{\infty} \frac{1+2\,q^{2n-1}\cos\left(\frac{\pi v}{K}\right)+q^{4n-2}}{1-2\,q^{2n-1}\cos\left(\frac{\pi v}{K}\right)+q^{4n-2}}\,.
\end{aligned}
\right.
$$

§ 152. — **Sviluppo di una funzione periodica in serie di Fourier.**

Si ottengono sviluppi importantissimi per le funzioni ellittiche, applicando il seguente teorema generale, che permette di sviluppare ogni funzione uniforme periodica in serie trigonometriche (serie di Fourier) :

Se $f(u)$ è una funzione uniforme della variabile complessa u col periodo Ω e nell' interno della striscia del piano complesso u, compresa fra due rette parallele alla direzione del periodo Ω, non ha nessun punto singolare, essa è sviluppabile in serie di Fourier della forma

$$
(6)\qquad f(u) = a_0 + \sum_{n=1}^{n=\infty} \left\{ a_n \cos\left(\frac{2n\pi u}{\Omega}\right) + b_n \operatorname{sen}\left(\frac{2n\pi u}{\Omega}\right) \right\},
$$

convergente in egual grado in ogni spazio interno alla detta striscia.

Questo teorema è una facile conseguenza del teorema di Laurent (§ 44). Pongasi infatti

$$
z = e^{\frac{2\pi i u}{\Omega}}\,;
$$

sarà

$$
f(u) = \varphi(z)
$$

funzione *monodroma* di z, perchè per ogni cammino chiuso descritto da z la u aumenta di un multiplo di Ω ed $f(u)$ si riproduce. Inoltre mentre u, movendo da un punto u_1 del suo piano complesso, descrive una retta parallela alla direzione del periodo Ω, si ha

$$
u = u_1 + \lambda\Omega\,,
$$

essendo λ un parametro reale che varia da $-\infty$ a $+\infty$, e quindi

$$
z = e^{\frac{2\pi i u_1}{\Omega}} (\cos 2\pi\lambda + i \operatorname{sen} 2\pi\lambda)
$$

descrive un cerchio col centro in $z=0$ e di raggio $= \left| e^{\frac{2\pi i u_1}{\Omega}} \right|$. Alla striscia considerata corrisponde quindi nel piano z un anello circolare col centro in $z=0$; e poichè $\varphi(z)$ entro quest'anello è finita, continua e monodroma, varrà lo sviluppo di Laurent

$$
\varphi(z) = \sum_0^{\infty} A_n z^n + \sum_1^{\infty} B_n z^{-n}\,,
$$

onde avremo

$$
f(u) = A_0 + \sum_1^{\infty} \left\{ (A_n + B_n) \cos\left(\frac{2n\pi u}{\Omega}\right) + i\,(A_n - B_n) \operatorname{sen}\left(\frac{2n\pi u}{\Omega}\right) \right\},
$$

che ponendo

$$
a_0 = A_0\,, \quad a_n = A_n + B_n\,, \quad b_n = i\,(A_n - B_n)
$$

assumerà precisamente la forma (6) del teorema e la serie del secondo membro sarà convergente in egual grado in ogni spazio interno alla striscia.

Possiamo di più esprimere per integrali definiti i valori dei coefficienti a_n, b_n della serie (6) di Fourier. E invero le formole a I, pag. 146 ci dànno

$$
A_n = \frac{1}{2\pi i} \int_\sigma \frac{\varphi(z)\,dz}{z^{n+1}}\,, \qquad B_n = \frac{1}{2\pi i} \int_\sigma \varphi(z) \cdot z^{n-1}\,dz\,,
$$

gli integrali essendo estesi ad un cerchio σ concentrico ed intermedio ai due che limitano l'anello. Ponendo per z il suo valore, gli integrali risulteranno estesi nel piano u ad un tratto rettilineo l parallelo ed interno alla striscia considerata e di lunghezza $= |\,\Omega\,|$. Ne risultano quindi per i valori dei coefficienti della serie (6) le espressioni :

$$(7)\quad \left\{ \begin{aligned} a_0 &= \frac{1}{\Omega}\int_l f(u)\,du\,, \qquad a_n = \frac{2}{\Omega}\int_l f(u)\cos\left(\frac{2n\pi u}{\Omega}\right) du\,, \\ b_n &= \frac{2}{\Omega}\int_l f(u)\,\mathrm{sen}\left(\frac{2n\pi u}{\Omega}\right) du\,. \end{aligned} \right.$$

§ 153. — Sviluppo in serie trigonometrica della $\sigma_3 u$.

Sviluppiamo in serie trigonometriche le funzioni σ, cominciando dalla funzione $\sigma_3 u$. Per ciò sostituiamo alla $\sigma_3 u$ la funzione

$$f(u) = e^{\frac{-\eta u^2}{2\omega}}\,\sigma_3 u\,,$$

che ha il periodo $\Omega = 2\omega$ e aumentando u di $2n\omega'$ si riproduce, a causa delle (a^*), pag. 157, moltiplicata pel fattore

$$(-1)^n q^{-n^2} e^{\frac{-n\pi i u}{\omega}} \quad \left(q = e^{\frac{\pi i \omega'}{\omega}}\right);$$

si ha cioè

$$(8)\qquad f(u + 2n\omega') = (-1)^n q^{-n^2} e^{\frac{-n\pi i u}{\omega}} \cdot f(u)\,.$$

Ciò premesso, osserviamo che, essendo $f(u)$ una funzione pari, tutti i coefficienti b_n nella (6) saranno nulli e potremo calcolare

i coefficienti a_n mediante le considerazioni seguenti. Tracciamo nel piano u il parallelogrammo

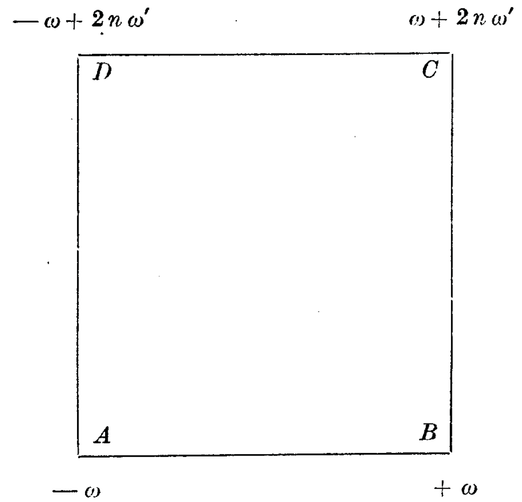

Fig. 12.

$$ABCD \equiv (-\omega\,,\quad \omega\,,\quad \omega + 2n\omega'\,,\quad -\omega + 2n\omega')$$

ed osserviamo che, essendo $f(u)$ una trascendente intera, sarà

$$\int_{ABCD} f(u)\,du = 0.$$

Accoppiando gli integrali estesi ai lati paralleli, quelli estesi a BC, DA si distruggono, perchè $f(u + 2\omega) = f(u)$, onde resta

$$\int_{AB} f(u)\,du + \int_{CD} f(u)\,du = 0\,,$$

ovvero

$$\int_{AB} f(u)\,du = \int_{AB} f(u + 2n\omega')\,du\,,$$

il che ci dà per la (8)

$$\int_{AB} f(u)\, du = (-1)^n q^{-n^2} \int_{AB} f(u)\, e^{\frac{-n\pi i u}{\omega}}\, du =$$

$$= (-1)^n q^{-n^2} \int_{AB} f(u) \cos\left(\frac{n\pi u}{\omega}\right) du ,$$

ovvero per le (7)

$$a_n = 2 a_0 (-1)^n q^{n^2} .$$

Avremo dunque

$$a) \qquad f(u) = e^{\frac{-\eta u^2}{2\omega}} \sigma_3 u = a_0 \left\{ 1 + 2 \sum_1^{\infty} (-1)^n q^{n^2} \cos\left(\frac{n\pi u}{\omega}\right) \right\},$$

e determineremo anche a_0 osservando che si ha

$$f(0) = 1 .$$

Si ha così per lo sviluppo cercato:

$$e^{\frac{-\eta u^2}{2\omega}} \sigma_3 u = \frac{1 + 2 \sum_1^{\infty} (-1)^n q^{n^2} \cos\left(\frac{n\pi u}{\omega}\right)}{1 + 2 \sum_1^{\infty} (-1)^n q^{n^2}} .$$

§ 154. — **Sviluppo delle altre σ e serie per calcolare η.**

In modo simile si potrebbe procedere per le altre σ; ma è più semplice dedurre i loro sviluppi da quello ora ottenuto per la σ_3. Si ha infatti

$$\sigma u = C e^{\eta' u} \sigma_3 (u - \omega') ,$$

e perciò

$$e^{\frac{-\eta u^2}{2\omega}} \sigma u = C' e^{\left(\eta' - \frac{\eta\omega'}{\omega}\right) u} \cdot f(u - \omega') = C' e^{\frac{-\pi i u}{2\omega}} f(u - \omega') ,$$

avendo $f(u)$ il valore a). Indicando con A un fattore costante, sarà dunque:

$$A e^{\frac{-\eta u^2}{2\omega}} \sigma u = \cos\left(\frac{\pi u}{2\omega}\right) - i \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) +$$

$$+ \sum_1^{\infty} (-1)^n q^{n^2} e^{\frac{n\pi i (u-\omega')}{\omega} - \frac{\pi i u}{2\omega}} + \sum_1^{\infty} (-1)^n q^{n^2} e^{-\frac{n\pi i (u-\omega')}{\omega} - \frac{\pi i u}{2\omega}} =$$

$$= \cos\left(\frac{\pi u}{2\omega}\right) - i \operatorname{sen}\left(\frac{\pi u}{2\pi}\right) + \sum_1^{\infty} (-1)^n q^{n^2 - n} e^{(2n-1)\frac{\pi i u}{2\omega}} +$$

$$+ \sum_1^{\infty} (-1)^n q^{n^2+n} e^{-(2n+1)\frac{\pi i u}{2\omega}} .$$

Ponendo da sè il termine della prima somma corrispondente ad $n = 1$, e cangiando in questa n in $n + 1$, otterremo

$$A e^{\frac{-\eta u^2}{2\omega}} \sigma u = -2 i \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) -$$

$$- \sum_1^{\infty} (-1)^n q^{n(n+1)} \left[e^{(2n+1)\frac{\pi i u}{2\omega}} - e^{-(2n+1)\frac{\pi i u}{2\omega}} \right]$$

e quindi

$$e^{\frac{-\eta u^2}{2\omega}} \sigma u = B \left\{ \operatorname{sen}\left(\frac{\pi u}{2\omega}\right) + \sum_1^{\infty} (-1)^n q^{n(n+1)} \operatorname{sen}\left(\frac{(2n+1)\pi u}{2\omega}\right) \right\}$$

$$= B \sum_0^{\infty} (-1)^n q^{n(n+1)} \operatorname{sen}\left(\frac{(2n+1)\pi u}{2\omega}\right) .$$

Per determinare la costante B, si divida dall' una e dall'altra parte per u e si passi al limite per $u = 0$; ne verrà

$$1 = B \frac{\pi}{2\omega} \sum_0^{\infty} (-1)^n (2n+1) q^{n(n+1)} ,$$

onde

$$\beta) \qquad e^{\frac{-\eta u^2}{2\omega}} \sigma u = \frac{2\omega}{\pi} \frac{\sum_0^\infty (-1)^n q^{n(n+1)} \operatorname{sen}(2n+1)\frac{\pi u}{2\omega}}{\sum_0^\infty (-1)^n (2n+1) q^{n(n+1)}}.$$

Come al § 150, basterà servirsi ora delle relazioni

$$\left.\begin{aligned} \sigma_2 u &= B e^{-\eta u} \sigma_3 (u+\omega) \\ \sigma_1 u &= C e^{-\eta u} \sigma (u+\omega) \end{aligned}\right\} \quad B,\ C \text{ costanti}$$

per dedurre gli sviluppi di σ_1, σ_2 e potremo riassumere le formole nel quadro :

$$(\mathrm{VII}) \left\{ \begin{aligned} e^{\frac{-\eta u^2}{2\omega}} \sigma u &= \frac{2\omega}{\pi} \frac{\sum_0^\infty (-1)^n q^{n(n+1)} \operatorname{sen}\left(\frac{(2n+1)\pi u}{2\omega}\right)}{\sum_0^\infty (-1)^n (2n+1) q^{n(n+1)}} \\ e^{\frac{-\eta u^2}{2\omega}} \sigma_1 u &= \frac{\sum_0^\infty q^{n(n+1)} \cos\left(\frac{(2n+1)\pi u}{2\omega}\right)}{\sum_0^\infty q^{n(n+1)}} \\ e^{\frac{-\eta u^2}{2\omega}} \sigma_2 u &= \frac{1 + 2\sum_1^\infty q^{n^2} \cos\left(\frac{n\pi u}{\omega}\right)}{1 + 2\sum_1^\infty q^{n^2}} \\ e^{\frac{-\eta u^2}{2\omega}} \sigma_3 u &= \frac{1 + 2\sum_1^\infty (-1)^n q^{n^2} \cos\left(\frac{n\pi u}{\omega}\right)}{1 + 2\sum_1^\infty (-1)^n q^{n^2}}. \end{aligned}\right.$$

Dallo sviluppo della σu possiamo dedurre una formola che serve al calcolo del semiperiodo di seconda specie η, dati che

siano ω, ω'. Sviluppiamo per ciò l'uno e l'altro membro della prima delle (VII) in serie di potenze di u, secondo le formole

$$\sigma u = u - \frac{g_2}{240} u^5 + \dots, \qquad e^{\frac{-\eta u^2}{2\omega}} = 1 - \frac{\eta u^2}{2\omega} + \dots.$$

$$\operatorname{sen} \frac{(2n+1)\pi u}{2\omega} = \frac{(2n+1)\pi u}{2\omega} - \frac{1}{6}\left(\frac{(2n+1) u}{2\omega}\right)^3 + \dots,$$

e paragoniamo i coefficienti di u^3. Posto

$$C = \frac{2\omega}{\pi} \frac{1}{\sum_0^\infty (-1)^n (2n+1) q^{n(n+1)}},$$

avremo

$$\frac{\eta}{2\omega} = \frac{C}{6}\left(\frac{\pi}{2\omega}\right)^3 \sum_0^\infty (-1)^n (2n+1)^3 q^{n(n+1)}$$

e quindi

$$(\mathrm{VII}^*) \qquad \eta\omega = \frac{\pi^2}{12} \frac{\sum_0^\infty (-1)^n (2n+1)^3 q^{n(n+1)}}{\sum_1^\infty (-1)^n (2n+1) q^{n(n+1)}} =$$

$$= \frac{\pi^2}{12} \frac{1 - 3^3 q^2 + 5^3 q^6 - 7^3 q^{12} + \dots}{1 - 3 q^2 + 5 q^6 - 7 q^{12} + \dots},$$

che è la formola cercata e fa conoscere η dati ω, ω'. Dalla relazione

$$\eta\omega' - \eta'\omega = \frac{\pi i}{2}$$

si potrà poi calcolare η'.

§ 155. — Le serie ϑ.

Consideriamo quelle particolari funzioni σ che rispondono ai periodi

$$2\omega = 1, \qquad 2\omega' = \tau,$$

e pei secondi membri delle formole (VII), moltiplicando nelle prime due formole numeratore e denominatore per $2q^{1/4}$, avremo le espressioni

$$a)\quad \frac{2\sum_0^\infty (-1)^n q^{\left(n+\frac{1}{2}\right)^2} \operatorname{sen}[(2n+1)\pi u]}{2\pi \sum_0^\infty (-1)^n (2n+1) q^{\left(n+\frac{1}{2}\right)^2}},$$

$$b)\quad \frac{2\sum_0^\infty q^{\left(n+\frac{1}{2}\right)^2} \cos[(2n+1)\pi u]}{2\sum_0^\infty q^{\left(n+\frac{1}{2}\right)^2}}$$

$$c)\quad \frac{1+2\sum_1^\infty q^{n^2}\cos(2n\pi u)}{1+2\sum_1^\infty q^{n^2}},\qquad d)\quad \frac{1+2\sum_1^\infty (-1)^n q^{n^2}\cos(2n\pi u)}{1+2\sum_1^\infty (-1)^n q^{n^2}}$$

Le serie al numeratore di queste espressioni possono anche scriversi rispettivamente:

$$a^*)\quad -i\sum_{-\infty}^{+\infty}(-1)^n e^{\pi i\tau\left(n+\frac{1}{2}\right)^2+2\left(n+\frac{1}{2}\right)\pi i u}$$

$$b^*)\quad \sum_{-\infty}^{+\infty} e^{\pi i\tau\left(n+\frac{1}{2}\right)^2+2\left(n+\frac{1}{2}\right)\pi i u}$$

$$c^*)\quad \sum_{-\infty}^{+\infty} e^{\pi i\tau n^2+2n\pi i u}$$

$$d^*)\quad \sum_{-\infty}^{+\infty}(-1)^n e^{\pi i\tau n^2+2n\pi i u};$$

esse rientrano nel tipo generale seguente:

$$(\gamma)\quad (-i)^{gh}\sum_{n=-\infty}^{n=+\infty}(-1)^{hn} e^{\pi i\tau\left(n+\frac{g}{2}\right)^2+2\pi i u\left(n+\frac{g}{2}\right)},$$

dove g, h sono numeri interi, che nei rispettivi casi $a^*), b^*), c^*), d^*)$ hanno i valori

$$a^*)\ (g,h)=(1,\ 1),\qquad b^*)\ (g,h)=(1,\ 0),$$
$$c^*)\ (g,h)=(0,\ 0),\qquad d^*)\ (g,h)=(0,\ 1).$$

Le serie (γ) prendono, secondo Jacobi, il nome di *serie* ϑ. Ponendo in evidenza l'argomento u, scriveremo

$$\text{(VIII)}\quad \vartheta_{g,h}(u)=(-i)^{gh}\sum_{-\infty}^{+\infty}(-1)^{hn} e^{\pi i\tau\left(n+\frac{g}{2}\right)^2+2\pi i u\left(n+\frac{g}{2}\right)}.$$

Si vede subito che sussistono le formole

$$(9)\quad \vartheta_{g+2,h}(u)=\vartheta_{g,h}(u),\qquad \vartheta_{g,h+2}(u)=(-1)^g\vartheta_{g,h}(u),$$

onde risulta che le $\vartheta_{hg}(u)$ coincidono, salvo il segno, colle quattro fondamentali

$$\vartheta_{11}(u),\quad \vartheta_{10}(u),\quad \vartheta_{00}(u),\quad \vartheta_{01}(u).$$

La notazione ora introdotta dei doppi indici è utile in molte ricerche, ma più usata è la seguente con un solo indice:

$$\text{(IX)}\quad \begin{cases} \vartheta_1(u)=\vartheta_{11}(u)=2\sum_0^\infty(-1)^n q^{\frac{1}{4}(2n+1)^2}\operatorname{sen}[(2n+1)\pi u] \\ \vartheta_2(u)=\vartheta_{10}(u)=2\sum_0^\infty q^{\frac{1}{4}(2n+1)^2}\cos[(2n+1)\pi u] \\ \vartheta_3(u)=\vartheta_{00}(u)=1+2\sum_1^\infty q^{n^2}\cos(2n\pi u) \\ \vartheta_0(u)=\theta_{01}(u)=1+2\sum_1^\infty(-1)^n q^{n^2}\cos(2n\pi u). \end{cases}$$

Dopo di ciò, denotando con ϑ' le derivate delle ϑ rapporto ad u, possiamo secondo le (VII) esprimere le σ per le ϑ colle formole:

$$\text{(X)}\quad \left.\begin{array}{ll} e^{\frac{-\eta u^2}{2\omega}}\sigma u=2\omega\dfrac{\vartheta_1(v)}{\vartheta'_1(0)}, & e^{\frac{-\eta u^2}{2\omega}}\sigma_1 u=\dfrac{\vartheta_2(v)}{\vartheta_2(0)} \\ e^{\frac{-\eta u^2}{2\omega}}\sigma_2 u=\dfrac{\vartheta_3(v)}{\vartheta_3(0)}, & e^{\frac{-\eta u^2}{2\omega}}\sigma_3 u=\dfrac{\vartheta_0(v)}{\vartheta_0(0)} \end{array}\right\}\quad v=\frac{u}{2\omega}.$$

Come si vede, ciascuna σ si esprime per la ϑ coll' indice superiore di un' unità, l' indice 4 essendo computato equivalente a 0.

Si osserverà che: *Delle quattro funzioni ϑ la $\vartheta_1(v)$ è dispari, le altre tre ϑ sono pari.*

§ 156. — Relazioni fra le ϑ.

Se nella formola (VIII) cangiamo u in $u + \frac{h' + g'\tau}{2}$, essendo g' h' due numeri interi qualunque, troviamo:

$$\vartheta_{gh}\left(u + \frac{h' + g'\tau}{2}\right) =$$

$$= (-i)^{gh} \sum_{-\infty}^{+\infty} (-1)^{hn}\, e^{\pi i \tau\left(n + \frac{g}{2}\right)^2 + 2\pi i u\left(n + \frac{g}{2}\right) + \pi i (h' + g'\tau)\left(n + \frac{g}{2}\right)},$$

ovvero

$$\vartheta_{gh}\left(u + \frac{h' + g'\tau}{2}\right) =$$

$$= (-i)^{gh} \sum_{-\infty}^{+\infty} (-1)^{hn}\, e^{\pi i \tau\left(n + \frac{g+g'}{2}\right)^2 + 2\pi i u\left(n + \frac{g+g'}{2}\right) + n i h'\left(n + \frac{g}{2}\right) - \pi i \tau \frac{g'2}{4} - \pi i u g'},$$

da cui risulta subito la formola generale

$$\text{(XI)} \qquad \vartheta_{gh}\left(u + \frac{h' + g'\tau}{2}\right) =$$

$$= (-1)^{gh'} \cdot i^{g'(h+h')}\, e^{-\frac{\pi i \tau g'^2}{4} - \pi i u g'}\, \vartheta_{g+g',\, h+h'}(u).$$

Questa ci permette di esprimere le quattro ϑ per una sola di esse, per es. per la

$$\vartheta_3(u) = \sum_{-\infty}^{+\infty} e^{\pi i \tau n^2 + \pi 2 i u \,.\, n} \quad {}^{1)}$$

[1]) Ove si ponga

$$a = \pi i \tau, \qquad b = \pi i u$$

la serie $\vartheta_3(u)$ diventa

$$\sum_{-\infty}^{+\infty} e^{a n^2 + 2 b n}$$

Dalla (XI) deduciamo in particolare l'effetto che si produce in $\vartheta_{gh}(u)$ aggiungendo all'argomento un numero intero ovvero un multiplo di τ; si ha infatti

$$\text{(XII)} \qquad \begin{cases} \vartheta_{gh}(u+1) = (-1)^g \vartheta_{gh}(u) \\ \vartheta_{gh}(u+\tau) = (-1)^h e^{-\pi i (2u+\tau)} \vartheta_{gh}(u). \end{cases}$$

Dalla semplice ispezione della serie (VIII), considerando $\vartheta_{gh}(u)$ come funzione delle due variabili u, τ, deduciamo subito l' importante risultato: *Le funzioni $\vartheta_{gh}(u, \tau)$ soddisfano l'equazione a derivate parziali del secondo ordine:*

$$\text{(XIII)} \qquad \frac{\partial^2 \vartheta}{\partial u^2} = 4\pi i\, \frac{\partial \vartheta}{\partial \tau}.$$

Dalle formole (X) facilmente deduciamo i valori delle tre quantità

$$U_1 = e^{\frac{-\eta_1\omega_1}{2}} \sigma\omega_1, \qquad U_2 = e^{\frac{-\eta_2\omega_2}{2}} \sigma\omega_2, \qquad U_3 = e^{\frac{-\eta_3\omega_3}{2}} \sigma\omega_3,$$

già considerati al § 150, espressi per i valori che assumono

$$\vartheta_0(u), \qquad \vartheta_2(u), \qquad \vartheta_3(u), \qquad \vartheta'_1(u)$$

serie sempre convergente per qualunque valore di b e pei valori di a colla parte reale negativa. Inversamente si può partire da una tale serie per costruire le ϑ e tutta la teoria delle funzioni ellittiche. Con legge analoga di formazione si costruiscono le serie con un numero qualunque p di indici $n_1, n_2 \ldots n_p$

$$\sum_{n_1=-\infty}^{n_1=+\infty} \sum_{n_2=-\infty}^{n_2=+\infty} \sum_{n_p=-\infty}^{n_p=+\infty} e^{\sum_{i,k}^{1\ldots p} a_{ik}\, n_i\, n_k + 2 \sum_i b_i\, n_i},$$

le quali convergono quando, indicando con a'_{ik} la parte reale di a_{ik}, la forma quadratica.

$$\sum_{i,k}^{1\ldots p} a'_{i,k}\, n_i\, n_k$$

è *definita negativa.* Per mezzo di queste serie si costruiscono le funzioni ϑ a più variabili $u_1\, u_2 \ldots u_p$, mediante le quali si risolve il *problema d' inversione* nella teoria degli integrali Abeliani.

per $u = 0$, valori che, per brevità, si indicano con

$$\vartheta_0, \quad \vartheta_2, \quad \vartheta_3, \quad \vartheta'_1,$$

omettendo l'argomento. A tale scopo osserviamo che dalla (XI) e dalle (9) si trae

$$\vartheta_1\left(\frac{\tau}{2}\right) = i\, e^{\frac{-\pi i \omega'}{4\omega}}\, \vartheta_0, \qquad \vartheta_1\left(\frac{1+\tau}{2}\right) = e^{\frac{-\pi i \omega'}{4\omega}}\, \vartheta_3$$

e facendo nella prima delle (X) successivamente

$$u = \omega, \quad \omega', \quad \omega + \omega',$$

indi

$$v = \frac{1}{2}, \quad \frac{\tau}{2}, \quad \frac{1+\tau}{2},$$

avremo

$$U_1 = 2\,\omega\,\frac{\vartheta_2}{\vartheta'_1}, \qquad U_2 = 2\,\omega\, e^{\frac{\pi i}{4}}\,\frac{\vartheta_3}{\vartheta'_1}, \qquad U_3 = 2\,i\,\omega\,\frac{\vartheta_0}{\vartheta'_1}$$

e quindi per le formole (2) del § 150 (pag. 161)

$$(10)\qquad \left\{\begin{aligned} \sqrt{e_1 - e_2} &= e^{\frac{-\pi i}{4}}\,\frac{U_3}{U_1 U_2} = \frac{1}{2\,\omega}\,\frac{\vartheta_0 \vartheta'_1}{\vartheta_2 \vartheta_3} \\ \sqrt{e_2 - e_3} &= -\,e^{\frac{-\pi i}{4}}\,\frac{U_1}{U_2 U_3} = \frac{1}{2\,\omega}\,\frac{\vartheta_2 \vartheta'_1}{\vartheta_0 \vartheta_3} \\ \sqrt{e_1 - e_3} &= e^{\frac{\pi i}{4}}\,\frac{U_2}{U_1 U_3} = \frac{1}{2\,\omega}\,\frac{\vartheta_3 \vartheta'_1}{\vartheta_0 \vartheta_2}\,. \end{aligned}\right.$$

Queste formole possono semplificarsi, facendo uso della identità scoperta da Jacobi

$$(\text{XIV})\qquad \vartheta'_1 = \pi\,\vartheta_0\,\vartheta_2\,\vartheta_3\,,$$

che ora dimostreremo. Esse diventano così:

$$(10^*)\qquad \sqrt{e_1 - e_2} = \frac{\pi}{2\,\omega}\,\vartheta_0^2, \quad \sqrt{e_2 - e_3} = \frac{\pi}{2\,\omega}\,\vartheta_2^2, \quad \sqrt{e_1 - e_3} = \frac{\pi}{2\,\omega}\,\vartheta_3^2.$$

§ 157. — Dimostrazione dell'identità (XIV) di Jacobi e valori in serie di $\sqrt{k}$, $\sqrt{k'}$, $\sqrt[8]{\Delta}$.

Per dimostrare l'identità Jacobiana (XIV), partiamo dalla formola

$$(r = 1, 2, 3)\quad \wp\,(u + \omega_r) = -\frac{\partial^2}{\partial u^2}\log\sigma\,(u + \omega_r) = -\frac{\partial^2 \log \sigma_r u}{\partial u^2}\,,$$

che per le (X) può scriversi

$$\wp\,(u + \omega_r) = -\frac{1}{(2\,\omega)^2}\left\{4\,\eta\,\omega + \frac{\partial^2 \log \vartheta_{r+1}(v)}{\partial v^2}\right\}$$

colla convenzione $\vartheta_4(v) = \vartheta_0(v)$. In questa facciamo $v = 0$ ed osservando che la formola (VII*), pag. 172, che dà il valore di $\eta\,\omega$, può scriversi

$$4\,\eta\,\omega = -\frac{1}{3}\,\frac{\vartheta'''_1}{\vartheta'_1}\,,$$

e d'altronde si ha

$$\frac{\partial^2 \log \vartheta\,(v)}{\partial v^2} = \frac{\vartheta''(v)}{\vartheta\,(v)} - \frac{\vartheta'^2(v)}{\vartheta^2(v)}$$

mentre $\vartheta'_0 = \vartheta'_2 = \vartheta'_3 = 0$, ne dedurremo

$$(11)\qquad e_r = -\frac{1}{(2\,\omega)^2}\left\{\frac{\vartheta''_{r+1}}{\vartheta_{r+1}} - \frac{1}{3}\,\frac{\vartheta'''_1}{\vartheta'_1}\right\}.$$

Ora dalla equazione (XIII) alle derivate parziali, cui soddisfano le ϑ, segue

$$\left\{\begin{aligned} \frac{\vartheta''_{r+1}}{\vartheta_{r+1}} &= 4\,\pi\,i\,\frac{\partial \log \vartheta_{r+1}}{\partial \tau} \\ \frac{\vartheta'''_1}{\vartheta'_1} &= 4\,\pi\,i\,\frac{\partial \log \vartheta'_1}{\partial \tau} \end{aligned}\right.$$

e quindi si ha

$$3\, e_r = -\frac{\pi i}{\omega^2}\left\{\frac{\partial \log \vartheta^3_{r+1}}{\partial \tau} - \frac{\partial \log \vartheta'_1}{\partial \tau}\right\}.$$

Per ciò l'identità

$$e_1 + e_2 + e_3 = 0$$

diventa

$$\frac{\partial}{\partial \tau} \log\left(\frac{\vartheta_0 \vartheta_2 \vartheta_3}{\vartheta'_1}\right) = 0$$

e ci dimostra che il rapporto

$$\frac{\vartheta_0\, \vartheta_2\, \vartheta_3}{\vartheta'_1}$$

è una costante assoluta. Per determinarne il valore effettivo si osservi che avendosi

$$\vartheta_0 = 1 - 2q + 2q^4 - 2q^9 + \ldots.$$

$$\vartheta_2 = 2q^{1/4}(1 + q^2 + q^6 + q^{12} + \ldots.)$$

$$\vartheta_3 = 1 + 2q + 2q^4 + 2q^9 + \ldots.$$

$$\vartheta'_1 = 2\pi q^{1/4}\left\{1 - 3q^2 + 5q^4 + \ldots.\right\}$$

se si fa crescere τ per valori puramente immaginarii all'infinito, q tende a zero e quindi $\frac{\vartheta'_1}{\vartheta_2}$ ha per limite π mentre ϑ_0, ϑ_3 tendono a 1. Si ha dunque

$$\frac{\vartheta_0 \vartheta_2 \vartheta_3}{\vartheta'_1} = \pi,$$

che è appunto l'identità (XIV).

Così sono anche dimostrate le formole (10), dalle quali risulta l'altra identità

(XV) $$\vartheta_3^4 = \vartheta_0^4 + \vartheta_2^4,$$

pure dovuta a Jacobi. È molto notevole che fra i quattro valori

$$\vartheta_0,\quad \vartheta_2,\quad \vartheta_3,\quad \vartheta'_1,$$

che sono espressioni trascendenti in τ, sussistano così due relazioni algebriche (XIV) e (XV).

Le formole (10*) conducono poi ad espressioni notevoli in serie per

$$\sqrt{k} = \sqrt{\frac{e_2 - e_3}{e_1 - e_3}},\quad \sqrt{k'} = \sqrt{\frac{e_1 - e_2}{e_1 - e_3}};$$

avremo invero

(XVI) $$\begin{cases} \sqrt{k} = \dfrac{\vartheta_2}{\vartheta_3} = 2q^{\frac{1}{4}} \dfrac{\sum_0^\infty q^{n(n+1)}}{1 + 2\sum_1^\infty q^{n^2}} \\[2ex] \sqrt{k'} = \dfrac{\vartheta_0}{\vartheta_3} = \dfrac{1 + 2\sum_1^\infty (-1)^n q^{n^2}}{1 + 2\sum_1^\infty q^{n^2}}. \end{cases}$$

Similmente per il valore di

$$\sqrt[8]{\Delta} = \sqrt{2}\, \sqrt[4]{(e_1 - e_2)(e_2 - e_3)(e_1 - e_3)}$$

troviamo l'espressione

$$\sqrt[8]{\Delta} = \sqrt{2}\, \sqrt{\left(\frac{\pi}{2\omega}\right)^3} \cdot \vartheta_0 \vartheta_2 \vartheta_3 = \frac{1}{2\omega} \sqrt{\frac{\pi}{\omega}}\, \vartheta'_1$$

ossia

(XVII) $$\sqrt[8]{\Delta} = \left(\frac{\pi}{\omega}\right)^{\frac{3}{2}} \cdot q^{\frac{1}{4}} \sum_0^\infty (-1)^n (2n+1)\, q^{n(n+1)}.$$

§ 158. — Sviluppi in prodotti infiniti delle ϑ.

Paragonando le formole (10*), che ci dànno gli sviluppi in serie di

$$\sqrt{e_1 - e_2},\quad \sqrt{e_2 - e_3},\quad \sqrt{e_1 - e_3},$$

colle (5) pag. 163 che ne dànno gli sviluppi pei prodotti infiniti

$$Q_0 = \prod_1^\infty (1 - q^{2n}), \qquad Q_1 = \prod_1^\infty (1 + q^{2n}),$$
$$Q_2 = \prod_1^\infty (1 + q^{2n-1}), \qquad Q_3 = \prod_1^\infty (1 - q^{2n-1}),$$

troviamo subito le formole

$$\vartheta_0 = \pm Q_3^2 Q_0, \qquad \vartheta_2 = \pm 2 q^{\frac{1}{4}} Q_1^2 Q_0, \qquad \vartheta_3 = \pm Q_2^2 Q_0.$$

L'incertezza del segno si toglie esaminando il caso limite $q = 0$ e si ha così:

$$\text{(XVIII)} \qquad \vartheta_0 = Q_3^2 Q_0, \qquad \vartheta_2 = 2 q^{\frac{1}{4}} Q_1^2 Q_0, \qquad \vartheta_3 = Q_2^2 Q_0,$$

dalle quali segue anche, per l'identità

$$Q_1 Q_2 Q_3 = 1,$$

$$\text{(XVIII*)} \qquad \vartheta'_1 = \pi \vartheta_0 \vartheta_2 \vartheta_3 = 2 \pi q^{\frac{1}{4}} Q_0^3 = 2 \omega \sqrt{\frac{\omega}{\pi}} \sqrt[8]{\Delta}.$$

Queste formole ci dànno le seguenti notevoli trasformazioni di serie in prodotti infiniti:

$$\begin{cases} 1 + 2 \sum_1^\infty (-1)^n q^{n^2} = \prod_1^\infty (1 - q^{2n-1})^2 (1 - q^{2n}) \\ \sum_1^\infty q^{n(n+1)} = \prod_1^\infty (1 + q^{2n})^2 (1 - q^{2n}) \\ 1 + 2 \sum_1^\infty q^{n^2} = \prod_1^\infty (1 + q^{2n-1})^2 (1 - q^{2n}) \\ \sum_1^\infty (-1)^n (2n+1) q^{n(n+1)} = \prod_1^\infty (1 - q^{2n})^3, \end{cases}$$

che valgono qualunque sia q, purchè sia $|q| < 1$.

Con ciò è anche risoluto il problema di esprimere le serie ϑ

per prodotti infiniti. Paragonando infatti le (X) pag. 174, colle (I) pag. 160, otteniamo subito intanto:

$$\begin{cases} \vartheta_1(v) = C \operatorname{sen} \pi v \prod_1^\infty (1 - 2 q^{2n} \cos 2\pi v + q^{4n}) \\ \vartheta_2(v) = C_1 \cos \pi v \prod_1^\infty (1 + 2 q^{2n} \cos 2\pi v + q^{4n}) \\ \vartheta_3(v) = C_2 \prod_1^\infty (1 + 2 q^{2n-1} \cos 2\pi v + q^{4n-2}) \\ \vartheta_0(v) = C_3 \prod_1^\infty (1 - 2 q^{2n-1} \cos 2\pi v + q^{4n-2}), \end{cases}$$

dove C, C_1, C_2, C_3 sono costanti rispetto all'argomento v. Per determinarle facciamo nelle tre ultime $v = 0$, e lo stesso facciamo nella prima dopo divisi i due membri per v; troviamo così:

$$\vartheta'_1 = C \pi Q_0^2, \qquad \vartheta_2 = C_1 Q_1^2, \qquad \vartheta_3 = C_2 Q_2^2, \qquad \vartheta_0 = C_3 Q_3^2$$

e quindi per le (XVIII), (XVIII*)

$$C = C_1 = 2 q^{\frac{1}{4}} Q_0, \qquad C_2 = C_3 = Q_0.$$

Abbiamo dunque le formole definitive:

$$\text{(XIX)} \begin{cases} \vartheta_1(v) = 2 q^{\frac{1}{4}} \sum_0^\infty (-1)^n q^{n(n+1)} \operatorname{sen}[(2n+1)\pi v] = \\ \qquad = 2 q^{\frac{1}{4}} \operatorname{sen}(\pi v) \prod_1^\infty (1 - 2 q^{2n} \cos(2\pi v) + q^{4n})(1 - q^{2n}) \\ \vartheta_2(v) = 2 q^{\frac{1}{4}} \sum_1^\infty q^{n(n+1)} \cos[(2n+1)\pi v] = \\ \qquad = 2 q^{\frac{1}{4}} \cos(\pi v) \prod_1^\infty (1 + 2 q^{2n} \cos(2\pi v) + q^{4n})(1 - q^{2n}) \\ \vartheta_3(v) = 1 + 2 \sum_1^\infty q^{n^2} \cos(2 n \pi v) = \\ \qquad = \prod_1^\infty (1 + 2 q^{2n-1} \cos(2\pi v) + q^{4n-2})(1 - q^{2n}) \\ \vartheta_0(v) = 1 + 2 \sum_1^\infty (-1)^n q^{n^2} \cos(2 n \pi v) = \\ \qquad = \prod_1^\infty (1 - 2 q^{2n-1} \cos(2\pi v) + q^{4n-2})(1 - q^{2n}). \end{cases}$$

Notiamo in fine due sviluppi in serie per

$$\sqrt{\frac{2K}{\pi}}, \qquad \sqrt{\frac{2Kk'}{\pi}},$$

che risultano dalle formole (III), (IV), pagg. 163, 164

$$\sqrt{\frac{2K}{\pi}} = Q_2^2 Q_0, \qquad \sqrt{\frac{2Kk'}{\pi}} = Q_3^2 Q_0,$$

confrontate con quelle superiori. Otteniamo così le formole molto notevoli di Jacobi:

$$\text{(XX)} \quad \left\{ \begin{aligned} \sqrt{\frac{2K}{\pi}} &= \vartheta_3 = 1 + 2\sum_1^\infty q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \dots \\ \sqrt{\frac{2Kk'}{\pi}} &= \vartheta_0 = 1 + 2\sum_1^\infty (-1)^n q^{n^2} = 1 - 2q + 2q^4 - 2q^9 + \dots \end{aligned} \right.$$

§ 159. — Trasformazioni di primo ordine per le ϑ (v, τ).

Le funzioni ϑ sono propriamente funzioni delle due variabili v, τ; volendo porre in evidenza non solo il valore dell'argomento v, ma anche quello del rapporto dei periodi si scrive:

$$\vartheta_1(v, \tau), \qquad \vartheta_2(v, \tau), \qquad \vartheta_3(v, \tau), \qquad \vartheta_0(v, \tau).$$

È importante ricercare come cangiano le ϑ quando sul rapporto τ dei periodi si eseguisca una sostituzione del gruppo modulare

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}.$$

Basterà per ciò esaminare l'effetto delle due sostituzioni generatrici del gruppo modulare

$$\tau' = \tau + 1, \qquad \tau' = -\frac{1}{\tau}.$$

Quanto all'effetto della prima la risposta è immediata, appena si osservino le loro espressioni analitiche (XIX), e si trovano così le formole:

$$\text{(XXI)} \quad \left\{ \begin{aligned} \vartheta_1(v, \tau+1) &= e^{\frac{\pi i}{4}}\,\vartheta_1(v, \tau), & \vartheta_2(v, \tau+1) &= e^{\frac{\pi i}{4}}\,\vartheta_2(v, \tau) \\ \vartheta_3(v, \tau+1) &= \vartheta_3(v, \tau), & \vartheta_0(v, \tau+1) &= \vartheta_0(v, \tau). \end{aligned} \right.$$

Per esaminare l'effetto dell'altra sostituzione

$$\tau' = -\frac{1}{\tau},$$

esprimiamo le ϑ per le σ per mezzo delle (X), pag. 174, e ricorriamo alle (XVIII), (XVIII*), che ci dànno

$$\vartheta_0 = \sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_1 - e_2}, \qquad \vartheta_2 = \sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_2 - e_3},$$

$$\vartheta_3 = \sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_1 - e_3}, \qquad \vartheta'_1 = 2\omega\sqrt{\frac{2\omega}{\pi}}\,\sqrt[8]{\Delta};$$

avremo così le formole

$$(12) \quad \left. \begin{aligned} \vartheta_1(v, \tau) &= \sqrt{\frac{\omega}{\pi}}\,\sqrt[8]{\Delta}\; e^{\frac{-\eta u^2}{2\omega}}\,\sigma u \\ \vartheta_2(v, \tau) &= \sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_2 - e_3}\; e^{\frac{-\eta u^2}{2\omega}}\,\sigma_1 u \\ \vartheta_3(v, \tau) &= \sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_1 - e_3}\; e^{\frac{-\eta u^2}{2\omega}}\,\sigma_2 u \\ \vartheta_0(v, \tau) &= \sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_1 - e_2}\; e^{\frac{-\eta u^2}{2\omega}}\,\sigma_3 u \end{aligned} \right\} \quad v = \frac{u}{2\omega}, \quad \tau = \frac{\omega'}{\omega}.$$

Consideriamo ora le funzioni $\bar\sigma$ coi nuovi periodi

$$\bar\omega = \omega', \qquad \bar\omega' = -\omega,$$

che indicheremo con

$$\bar\sigma u, \quad \bar\sigma_1 u \quad \bar\sigma_2 u, \quad \bar\sigma_3 u,$$

mentre con

$$\bar{e}_1,\quad \bar{e}_2,\quad \bar{e}_3,\quad \bar{\Delta}$$

indicheremo i nuovi valori di e_1, e_2, e_3, Δ. Per le formole della tabella (A), pag. 101, avremo

$$\bar{\sigma}u = \sigma u\,,\quad \bar{\sigma}_1 u = \sigma_3 u\,,\quad \bar{\sigma}_2 u = \sigma_2 u\,,\quad \bar{\sigma}_3 u = \sigma_1 u$$

$$\bar{e}_1 = e_3\,,\quad \bar{e}_2 = e_2\,,\quad \bar{e}_3 = e_1\,,$$

e similmente sarà

$$\bar{\eta} = \eta'\,,\qquad \bar{\eta}' = -\eta\,.$$

Ora dalle (12), ponendo

$$\bar{v} = \frac{u}{2\,\bar{\omega}} = \frac{v}{\tau}\,,$$

risulta

$$\begin{aligned}
\vartheta_1\left(\bar{v}, -\frac{1}{\tau}\right) &= \sqrt{\frac{\bar{\omega}}{\pi}}\,\sqrt[8]{\bar{\Delta}}\; e^{\frac{-\bar{\eta}u^2}{2\bar{\omega}}}\cdot \sigma u = \\
&= \varepsilon_1\sqrt{\tau}\,\sqrt{\frac{\omega}{\pi}}\,\sqrt[8]{\Delta}\; e^{\frac{-\eta' u^2}{2\omega'}}\,\sigma u \\
\vartheta_2\left(\bar{v}, -\frac{1}{\tau}\right) &= \sqrt{\frac{2\bar{\omega}}{\pi}}\,\sqrt[4]{\bar{e}_2-\bar{e}_3}\cdot e^{\frac{-\bar{\eta}u^2}{2\bar{\omega}}}\,\bar{\sigma}_1 u = \\
&= \varepsilon_2\sqrt{\tau}\,\sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_1-e_3}\; e^{\frac{-\eta' u^2}{2\omega'}}\,\sigma_3 u \\
\vartheta_3\left(\bar{v}, -\frac{1}{\tau}\right) &= \sqrt{\frac{2\bar{\omega}}{\pi}}\,\sqrt[4]{\bar{e}_1-\bar{e}_3}\; e^{\frac{-\bar{\eta}u^2}{2\bar{\omega}}}\cdot \bar{\sigma}_2 u = \\
&= \varepsilon_3\sqrt{\tau}\,\sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_1-e_3}\; e^{\frac{-\eta' u^2}{2\omega'}}\,\sigma_2 u \\
\vartheta_0\left(\bar{v}, -\frac{1}{\tau}\right) &= \sqrt{\frac{2\bar{\omega}}{\pi}}\,\sqrt[4]{\bar{e}_1-\bar{e}_2}\cdot e^{\frac{-\bar{\eta}u^2}{2\bar{\omega}}}\,\bar{\sigma}_3 u = \\
&= \varepsilon_4\sqrt{\tau}\,\sqrt{\frac{2\omega}{\pi}}\,\sqrt[4]{e_2-e_3}\; e^{\frac{-\eta' u^2}{2\omega'}}\,\sigma_1 u\,,
\end{aligned}$$

dove $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ indicano convenienti radici ottave dell'unità. Il confronto colle (12), osservando che si ha

$$\frac{\eta u^2}{2\omega} - \frac{\eta' u^2}{2\omega'} = \frac{\eta\omega' - \eta'\omega}{2\omega\omega'}\,u^2 = \frac{\pi i}{4\omega\omega'}\,u^2 = \frac{\pi i v^2}{\tau}\,,$$

ci dà

$$\begin{aligned}
\vartheta_1\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) &= \varepsilon_1\sqrt{\tau}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_1(v,\tau) \\
\vartheta_2\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) &= \varepsilon_2\sqrt{\tau}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_0(v,\tau) \\
\vartheta_3\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) &= \varepsilon_3\sqrt{\tau}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_3(v,\tau) \\
\vartheta_0\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) &= \varepsilon_4\sqrt{\tau}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_2(v,\tau)
\end{aligned}$$

Per determinare $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$, che sono indipendenti da v e τ, si faccia nelle ultime tre formole $v = 0$, $\tau = i$ e risulterà

$$\varepsilon_2 = \varepsilon_3 = \varepsilon_4 = \frac{1}{\sqrt{i}}\,,$$

mentre la prima, divisa per v, e fatto ancora $v = 0$, $\tau = i$ dà

$$\varepsilon_1 = -\frac{i}{\sqrt{i}}$$

e quindi abbiamo per le formole cercate:

$$\text{(XXII)}\quad \begin{cases}
\vartheta_1\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) = -i\sqrt{\frac{\tau}{i}}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_1(v,\tau) \\
\vartheta_2\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_0(v,\tau) \\
\vartheta_3\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_3(v,\tau) \\
\vartheta_0\left(\frac{v}{\tau}, -\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}}\; e^{\frac{\pi i v^2}{\tau}}\,\vartheta_2(v,\tau)\,.
\end{cases}$$

Per far sparire ogni ambiguità da queste formole finali resta solo da stabilirsi quale determinazione è da scegliersi per $\sqrt{\frac{\tau}{i}}$ in ciascuna di esse; dimostriamo che *in tutte e quattro le formole* (XXII) *deve prendersi per* $\sqrt{\frac{\tau}{i}}$ *quel segno che dà un valore positivo alla sua parte reale.*

Ciò ha luogo in effetto per $v = 0$, $\tau = i$, e quindi in tutti i casi perchè la parte reale di $\frac{\tau}{i}$, quindi anche quella di $\sqrt{\frac{\tau}{i}}$, non passa mai per lo zero.

Osservazione. — Il caso più importante delle applicazioni è quello in cui debbasi calcolare i valori delle σ o delle ϑ per valori puramente immaginarî di τ. Ora il caso in cui $|\tau| < 1$ si riconduce, mediante le (XXII), al caso $|\tau| > 1$, ove $q = e^{\pi i \tau} = e^{-\pi\beta}$ è reale, positiva e minore di

$$e^{-\pi} = 0,04321\ldots.$$

Le serie ϑ, per valori reali dell'argomento v, hanno allora una convergenza estremamente rapida, sicchè basta il calcolo di pochi termini della serie per ottenere con grande approssimazione il corrispondente valore delle ϑ [1]).

CAPITOLO XV.

Teoria della trasformazione delle funzioni ellittiche. — Trasformazioni di grado primo della $\wp u$ e della σu. — Trasformazione di Landen.

§ 160. — Problema della trasformazione delle funzioni ellittiche. Riduzione al caso delle trasformazioni razionali.

Nelle teorie relative alle funzioni ellittiche, che abbiamo svolto fin qui, i periodi 2ω, $2\omega'$ si riguardavano come costanti e si ricercavano le relazioni fra funzioni ellittiche di diversi argomenti coi medesimi periodi. Ma in realtà le funzioni ellittiche, e in particolare la fondamentale

$$\wp(u \mid \omega, \omega'),$$

1) Veggasi per più ampie notizie il Cap. VIII del *Traité des fonctions elliptiques*, di HALPHEN, tomo I.

sono funzioni delle tre variabili u, ω, ω' e possiamo egualmente ricercare le relazioni fra funzioni ellittiche con diversi periodi. Appartiene a questo genere di ricerche la *teoria della trasformazione* delle funzioni ellittiche, di cui ora ci andiamo ad occupare. Il problema fondamentale della teoria, limitandoci alla funzione elementare $\wp u$, si enuncia nel modo seguente:

Per quali funzioni $\wp$, costruite con diversi periodi

$$\wp u = \wp(u \mid \omega, \omega'), \qquad \bar{\wp} u = \wp(u \mid \Omega, \Omega'),$$

accade che sussista fra $\wp u$, $\bar{\wp} u$ una relazione algebrica

$$F(\wp u, \bar{\wp} u) = 0\,?$$

Possiamo dare a questo problema una forma algebrica osservando, che, posto

$$s = \wp u, \qquad S = \bar{\wp} u,$$

e indicando con g_2, g_3 gli invarianti della $\wp u$, con $\bar{g}_2$, $\bar{g}_3$ quelli della $\bar{\wp} u$, si avrà

$$du = \frac{ds}{\sqrt{4s^3 - g_2 s - g_3}} = \frac{dS}{\sqrt{4S^3 - \bar{g}_2 S - \bar{g}_3}}; \tag{1}$$

la questione proposta equivale quindi alla ricerca delle relazioni algebriche

$$F(s, S) = 0 \tag{2}$$

che trasformano l'uno nell'altro i differenziali ellittici

$$\frac{ds}{\sqrt{4s^3 - g_2 s - g_3}}, \qquad \frac{dS}{\sqrt{4S^3 - \bar{g}_2 S - \bar{g}_3}},$$

ovvero alla ricerca delle condizioni perchè l'equazione differenziale (1) ammetta un integrale (2) algebrico.

Mentre la trattazione algebrica di questo problema offrirebbe grandi difficoltà, esso può risolversi facilmente per via trascendente. Per ciò osserviamo che se nella supposta relazione algebrica

$$F(\wp u, \bar{\wp} u) = 0, \tag{2*}$$

che intendiamo già ridotta a forma razionale ed intera, accresciamo l'argomento u di $2\,r\,\omega$, essendo r un intero qualunque, la $\wp\,u$ non muta, e sarà quindi ancora

$$F(\wp\,u, \bar{\wp}(u + 2\,r\,\omega)) = 0,$$

cioè tutte le quantità

$$x_r = \bar{\wp}(u + 2\,r\,\omega)\ ,$$

saranno radici della equazione

$$F(\wp\,u, x) = 0\,,$$

e però dovrà necessariamente accadere che, per valori distinti di r, r' si abbiano eguaglianze della forma

$$\bar{\wp}(u + 2\,r\,\omega) = \bar{\wp}(u + 2\,r'\,\omega).$$

La differenza

$$2\,(r - r')\,\omega = 2\,k\,\omega$$

sarà perciò un periodo della $\bar{\wp}\,u$ e si avrà quindi

$$k\,\omega = a\,\Omega + b\,\Omega'$$

con a, b, k, numeri interi, e similmente

$$k'\,\omega' = c\,\Omega + d\,\Omega',$$

essendo ancora c, d, k' interi. Potremo quindi scrivere le relazioni

$$(3)\qquad \left\{ \begin{aligned} r\,\omega &= a_1\,\Omega + b_1\,\Omega' \\ r\,\omega' &= c_1\,\Omega + d_1\,\Omega'\,, \end{aligned} \right.$$

dove i numeri interi a_1, b_1, c_1, d_1, r si potranno supporre senza divisore comune e sarà

$$a_1\,d_1 - b_1\,c_1 \neq 0.$$

Inversamente, se fra i periodi $2\,\omega$, $2\,\omega'$ della $\wp\,u$ e quelli $2\,\Omega$, $2\,\Omega'$ della $\bar{\wp}\,u$ sussistono relazioni della forma (3), le due funzioni ellittiche $\wp\,u$, $\bar{\wp}\,u$, avendo a comune la coppia di periodi

$$2\,r\,\omega\,,\ 2\,r\,\omega'\,,$$

saranno certamente legate da una relazione algebrica (§ 107). Dunque: *La condizione necessaria e sufficiente affinchè fra* $\wp(u \mid \omega, \omega')$ *e* $\wp(u \mid \Omega, \Omega')$ *sussista una relazione algebrica è che fra i loro periodi abbiano luogo le relazioni* (3) *a coefficienti interi.*

Ma possiamo subito semplificare il nostro problema colla considerazione seguente. Se introduciamo la terza funzione ellittica

$$\wp_1\,u = \wp(u \mid r\,\omega\,,\ r\,\omega')\,,$$

tanto $\wp\,u$ che $\bar{\wp}\,u$, ammettendo i periodi di $\wp_1\,u$ ed essendo pari, saranno funzioni razionali di $\wp_1\,u$. La trasformazione *irrazionale* che da $\wp\,u$ conduce a $\bar{\wp}\,u$ si può dunque comporre con due trasformazioni *razionali*, mediante le quali tanto $\wp\,u$ che $\bar{\wp}\,u$ si esprimono razionalmente per l'ausiliaria $\wp_1\,u$ [1]).

Così il problema della trasformazione è ridotto all'altro più semplice:

Quali funzioni $\wp(u \mid \Omega, \Omega')$ *si esprimono razionalmente per* $\wp(u \mid \omega, \omega')$?

§ 161. — Trasformazioni razionali e loro grado.

Ridotto così il problema alla ricerca delle trasformazioni razionali, supponiamo dunque che si abbia

$$(A)\qquad \wp(u \mid \Omega, \Omega') = F(\wp(u \mid \omega, \omega')),$$

essendo F il simbolo di una funzione razionale. È chiaro che i periodi $2\,\omega$, $2\,\omega'$ della $\wp\,u$ dovranno pur essere periodi della

$$\bar{\wp}\,u = \wp(u \mid \Omega, \Omega'),$$

e si avrà per ciò

$$(I)\qquad \left\{ \begin{aligned} \omega &= a\,\Omega + b\,\Omega' \\ \omega' &= c\,\Omega + d\,\Omega'\,, \end{aligned} \right.$$

con a, b, c, d numeri interi. E poichè supponiamo inoltre sempre

$$R\left(\frac{\omega'}{i\,\omega}\right) > 0\,,\qquad R\left(\frac{\Omega'}{i\,\Omega}\right) > 0\,,$$

[1]) Ciò dimostra che l'equazione algebrica (2) è in ogni caso di genere *zero.*

il determinante

$$\Delta = a\,d - b\,c$$

sarà un numero intero positivo. Inversamente, se hanno luogo relazioni della forma (I), la $\bar{\wp}\,u$ ammetterà i periodi di $\wp\,u$, ed essendo pari, sarà una funzione razionale di $\wp\,u$.

Vogliamo ora stabilire il significato del determinante

$$\Delta = a\,d - b\,c\,.$$

Supponiamo che la funzione razionale $F(s)$ $(s = \wp\,u)$ sia il quoziente di due polinomi razionali interi $U(s)$, $V(s)$ primi fra loro

$$F(s) = \frac{U(s)}{V(s)}\,;$$

si dirà *grado* della trasformazione il più alto dei due gradi dei polinomii U, V. Ora il significato di D è dato dal teorema:

Il determinante $\Delta = a\,d - b\,c$ dà il grado della trasformazione.

Per dimostrarlo osserviamo che, posto

$$S = \bar{\wp}\,u\,,$$

si ha

$$S\,V(s) - U(s) = 0.$$

e, fissato S ad arbitrio, questa equazione *irriducibile* in s avrà un numero di radici eguale al grado della trasformazione. Questo grado eguaglia dunque il numero dei valori distinti di $\wp\,u$ per un medesimo valore di $\bar{\wp}\,u$.

Ora, se risolviamo le (I) rapporto ad Ω, Ω', abbiamo

$$\text{(I*)}\qquad \begin{cases} \Delta\,\Omega = d\,\omega - b\,\omega' \\ \Delta\,\Omega' = -c\,\omega + a\,\omega' \end{cases}$$

e poichè i valori di u che dànno lo stesso valore di $\bar{\wp}\,u$ sono tutti della forma

$$\pm u + 2\,m\,\Omega + 2\,n\,\Omega',$$

percorrendo m, n tutti gli interi, converrà esaminare quanti dei corrispondenti valori di $\wp\,u$:

$$\wp\,(\pm\,u + 2\,m\,\Omega + 2\,n\,\Omega') =$$

$$= \wp\left(\pm\,u + 2\,\frac{m\,d - n\,c}{\Delta}\,\omega + 2\,\frac{-m\,b + n\,a}{\Delta}\,\omega'\right),$$

ovvero di [1])

$$\wp\left(u + 2\,\frac{m\,d - n\,c}{\Delta}\,\omega + 2\,\frac{-m\,b + n\,a}{\Delta}\,\omega'\right)$$

saranno distinti.

Ora, se poniamo

$$(4)\qquad \begin{cases} m\,d - n\,c = r \\ m\,b + n\,a = s, \end{cases}$$

ed osserviamo che una nuova coppia di valori (r_1, s_1) per r, s darà nella (B) il medesimo valore allora e allora soltanto che sia

$$(r_1, s_1) \equiv (r, s) \pmod{\Delta}\,,$$

vediamo che il numero richiesto sarà il numero delle coppie (r, s) incongrue (mod Δ), definite dalle (4). Sia ε il massimo comun divisore di c, d e poniamo

$$c = \varepsilon\,c_1\,,\qquad d = \varepsilon\,d_1\,,\qquad r = \varepsilon\,r_1\,,$$

onde

$$(5)\qquad m\,d_1 - n\,c_1 = r_1\,.$$

Poichè c_1, d_1 sono primi fra loro, potrà r_1 avere qualsiasi valore e quindi

$$r = \varepsilon\,r_1$$

[1]) È inutile considerare il doppio segno di u, come si vede cangiando m, n in $-m$, $-n$.

assumerà soltanto $\frac{\Delta}{\varepsilon}$ valori incongrui (mod Δ). Per ognuno di questi valori le coppie (m, n) che soddisfano la (5) sono legate ad una fissa m', n' dalle formole

$$\left.\begin{array}{l} m = m' + t c_1 \\ n = n' + t d_1 \end{array}\right\} \quad t \text{ intero qualunque}$$

e i corrispondenti valori di s sono dati da

$$s = -m'b + n'a + t(-b c_1 + a d_1)$$

$$= -m'b + n'a + t\frac{\Delta}{\varepsilon}$$

e percorrono solo ε valori distinti (mod Δ). Il numero cercato è dunque

$$\frac{\Delta}{\varepsilon} \cdot \varepsilon = \Delta \qquad \text{c. d. d.}$$

§ 162. — **Equivalenza delle trasformazioni.**

La trasformazione razionale (A) è perfettamente determinata, noti che siano i quattro numeri a, b, c, d nelle (I); indicheremo per ciò la trasformazione stessa col simbolo

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix},$$

e la prima questione che dovremo risolvere sarà di vedere quando due diversi simboli

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \qquad \begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix}$$

rappresenteranno la medesima trasformazione, conducendo dalla medesima funzione $\wp(u \mid \omega, \omega')$ ad eguali funzioni trasformate

$$(\alpha) \qquad \wp(u \mid \Omega, \Omega') = \wp(u \mid \Omega_1, \Omega'_1).$$

Le formole (I) per la trasformazione

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

saranno

$$(6) \qquad \left\{\begin{array}{l} \omega = a'\Omega_1 + b'\Omega'_1 \\ \omega' = c'\Omega_1 + d'\Omega'_1. \end{array}\right.$$

Ora le condizioni *necessarie e sufficienti* per l'eguaglianza (α) sono contenute nelle relazioni (§ 104)

$$\left\{\begin{array}{l} \Omega = \alpha\Omega_1 + \beta\Omega'_1 \\ \Omega' = \gamma\Omega_1 + \delta\Omega'_1. \end{array}\right.$$

con $\alpha, \beta, \gamma, \delta$ interi e $\alpha\delta - \beta\gamma = 1$. Sostituendo nelle (I), e paragonando colle (6), troviamo

$$\left\{\begin{array}{ll} a' = a\alpha + b\gamma, & b' = a\beta + b\delta \\ c' = c\alpha + d\gamma, & d' = c\beta + d\delta. \end{array}\right.$$

La trasformazione $\begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix}$, che conduce da $\wp(u \mid \omega, \omega')$ a $\wp(u \mid \Omega_1, \Omega'_1)$, è quindi il risultato delle due successive

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

la prima delle quali fa passare da $\wp(u \mid \omega, \omega')$ a $\wp(u \mid \Omega, \Omega')$ e la seconda da $\wp(u \mid \Omega, \Omega')$ a $\wp(u \mid \Omega_1, \Omega'_1)$; ma per questa ultima, che è di primo grado, la corrispondente $\wp u$ non cangia [1]).

Scriviamo simbolicamente la trasformazione composta così:

$$\begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix} = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\gamma, & a\beta + b\delta \\ c\alpha + d\gamma, & c\beta + d\delta \end{pmatrix}.$$

[1]) Questa proprietà della $\wp u$ di Weierstrass di restare immutata per tutte le trasformazioni di primo grado è quella appunto che qui, nella teoria della trasformazione, rende tanto più semplice la ricerca in confronto dell'antica teoria per le funzioni di Jacobi

$$\operatorname{sn} v, \quad \operatorname{cn} v, \quad \operatorname{dn} v.$$

Due tali trasformazioni $\begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix}$, $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ legate da una relazione (7), essendo

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

una trasformazione qualunque di primo grado, si diranno fra loro *equivalenti*, come quelle che conducono alla medesima $\wp u$ trasformata. Il concetto di equivalenza è evidentemente invertibile, come si vede anche dalla formola

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} = \begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix} \begin{pmatrix} \delta, & -\beta \\ -\gamma, & \alpha \end{pmatrix}$$

e poichè inoltre due trasformazioni equivalenti ad una terza sono anche equivalenti fra loro, potremo ripartire tutte le trasformazioni

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

di un dato grado n in *classi*, ponendo nella medesima classe tutte le infinite trasformazioni equivalenti fra loro. Così due trasformazioni qualunque saranno equivalenti o no, secondo che appartengono o non appartengono alla medesima classe.

§ 163. — **Riduzione alla forma normale.**

Stabilite queste nozioni fondamentali, dimostriamo subito il teorema : *Per ogni valore del grado n il numero delle classi, cioè il numero delle trasformazioni distinte, è sempre finito.*

Per ciò dimostreremo che *in ogni classe* vi sono trasformazioni del tipo

$$\begin{pmatrix} a', & 0 \\ c', & d' \end{pmatrix}$$

col secondo coefficiente $b' = 0$. Sia infatti $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ una trasformazione qualunque della classe e sia $b \neq 0$. Se $a = 0$ basta osservare che si ha

$$\begin{pmatrix} 0, & b \\ c, & d \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -b, & 0 \\ -d, & c \end{pmatrix},$$

per conseguire lo scopo proposto.

Siano ora adunque

$$a \neq 0, \qquad b \neq 0;$$

dimostriamo che si possono assegnare quattro interi $\alpha, \beta, \gamma, \delta$ con $\alpha\delta - \beta\gamma = 1$, tali che sia

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} a', & 0 \\ c', & d' \end{pmatrix},$$

cioè con

$$a\beta + b\delta = 0. \tag{8}$$

Indichiamo con σ il massimo comun divisore di a, b, che dividerà

$$a\,d - b\,c = n\,.$$

Dovendo essere per la (8)

$$\frac{\frac{b}{\sigma}}{\frac{a}{\sigma}} = -\frac{\beta}{\delta},$$

ed essendo ambedue le frazioni ridotte ai minimi termini, sarà

$$\beta = \mp \frac{b}{\sigma}, \qquad \delta = \pm \frac{a}{\sigma},$$

e poichè un cangiamento simultaneo di segno in $\alpha, \beta, \gamma, \delta$ non altera evidentemente la trasformazione composta $\begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix}$, potremo assumere senz'altro

$$\beta = -\frac{b}{\sigma}, \qquad \delta = \frac{a}{\sigma},$$

onde risulterà

$$a' = a\,\alpha + b\,\gamma = \sigma\,(\alpha\delta - \beta\gamma) = \sigma$$

$$d' = c\,\beta + d\,\delta = \frac{a\,d - b\,c}{\sigma} = \frac{n}{\sigma}.$$

Ora da

$$\alpha\delta - \beta\gamma = \frac{a}{\sigma}\,\alpha + \frac{b}{\sigma}\,\gamma = 1\,,$$

equazione solubile in numeri interi α, γ perchè $\frac{a}{\sigma}$, $\frac{b}{\sigma}$ sono primi fra loro, si vede che indicando con α', γ' una particolare coppia di soluzioni, ogni altra sarà data dalle formole

$$\left.\begin{aligned} \alpha &= \alpha' - \varrho\,\frac{b}{\sigma} \\ \gamma &= \gamma' + \varrho\,\frac{a}{\sigma} \end{aligned}\right\}\ \text{con } \varrho \text{ intero qualunque,}$$

e sarà quindi

$$c' = c\,\alpha' + d\,\gamma' + \varrho\,\frac{n}{\sigma}\,.$$

Esistono adunque nella classe di $\begin{pmatrix} a, b \\ c, d \end{pmatrix}$ *infinite* trasformazioni col secondo coefficiente *zero*; esse hanno tutte la forma

$$\text{(II)} \qquad \begin{pmatrix} \sigma, & 0 \\ \xi, & \frac{n}{\sigma} \end{pmatrix}$$

dove il terzo coefficiente

$$\xi = c\,\alpha' + d\,\gamma' + \varrho\,\frac{n}{\sigma}$$

è determinato soltanto rispetto al modulo $\frac{n}{\sigma}$. Due trasformazioni della forma normale (II) appartengono dunque a classe diversa se il divisore σ è diverso nelle due trasformazioni ovvero se, essendo lo stesso σ, sono diversi i valori di $\xi \left(\text{mod}\ \frac{n}{\sigma}\right)$.

Ad ogni divisore σ di n corrispondono quindi $\frac{n}{\sigma}$ classi distinte, onde vediamo che *il numero totale delle classi è dato dalla somma dei divisori di n.*

§ 164. — Trasformazioni imprimitive e primitive. Trasformazioni di grado composto.

Se con una trasformazione $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ di grado n si passa dalla $\wp(u \mid \omega, \omega')$ alla $\wp(u \mid \Omega, \Omega')$, indi, con una nuova trasformazione $\begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix}$ di grado m, dalla $\wp(u \mid \Omega, \Omega')$ alla $\wp(u \mid \overline{\Omega}, \overline{\Omega}')$, si ha infine

$$\wp(u \mid \overline{\Omega}, \overline{\Omega}')$$

espressa razionalmente per $\wp(u \mid \omega, \omega')$ colla trasformazione composta di grado $m\,n$

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix} = \begin{pmatrix} a\,a' + b\,c', & a\,b' + b\,d \\ c\,a' + d\,c', & c\,b' + d\,d' \end{pmatrix}.$$

Ora osserviamo che una trasformazione di grado n^2 della forma

$$\begin{pmatrix} n, & 0 \\ 0, & n \end{pmatrix}$$

si riduce propriamente ad una moltiplicazione dell'argomento giacchè, per la formola di omogeneità della $\wp\,u$,

$$\wp\left(u \mid \frac{\omega}{n}, \frac{\omega'}{n}\right) = n^2\,\wp\,(n\,u \mid \omega, \omega')$$

si esprime razionalmente per $\wp\,u$ colle formole di moltiplicazione dell'argomento. Ne risulta che se in una trasformazione $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ i quattro numeri a, b, c, d hanno un divisore comune r, avendosi

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} = \begin{pmatrix} r, & 0 \\ 0, & r \end{pmatrix} \begin{pmatrix} \frac{a}{r}, & \frac{b}{r} \\ \frac{c}{r}, & \frac{d}{r} \end{pmatrix}.$$

la trasformazione risulta dal comporre una moltiplicazione per r dell'argomento con una trasformazione. Una trasformazione $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$

in cui i numeri a, b, c, d hanno un divisore comune dicesi per ciò *imprimitiva*. È chiaro che basterà limitarsi allo studio delle trasformazioni primitive, le formole di moltiplicazione dell'argomento essendo già note.

Possiamo già ora determinare quante trasformazioni *primitive* distinte esistono in un dato grado n, che sia la potenza esatta q^α di un numero primo q. Esse sono infatti tutte comprese nel simbolo

$$\begin{pmatrix} q^r, & 0 \\ \xi, & q^{\alpha-r} \end{pmatrix} \quad r = 0, 1, 2, \ldots, \alpha,$$

dove ξ percorre un sistema completo di resti (mod $q^{\alpha-r}$) esclusi, per valori di r diversi da 0 e da α, quelli divisibili per q. Indicando dunque con N il numero cercato delle trasformazioni primitive distinte, avremo

$$N = q^\alpha + q^{\alpha-2}(q-1) + q^{\alpha-3}(q-1) + \ldots + (q-1) + 1$$

ossia

$$N = q^{\alpha-1}(q+1).$$

Dimostriamo ora il seguente teorema, che riduce sostanzialmente la ricerca delle trasformazioni a quelle il cui grado è un numero *primo*: *Ogni trasformazione, il cui grado n si decompone nel prodotto di due numeri P, Q, è il risultato di due successive trasformazioni, l'una di grado P, l'altra di grado Q.*

Consideriamo una trasformazione di grado $n = PQ$, già ridotta alla forma normale

$$\begin{pmatrix} \sigma, & 0 \\ \xi, & \dfrac{n}{\sigma} \end{pmatrix},$$

e cerchiamo di comporla con due trasformazioni normali

$$\begin{pmatrix} \tau, & 0 \\ \eta, & \dfrac{P}{\tau} \end{pmatrix}, \qquad \begin{pmatrix} \tau', & 0 \\ \zeta, & \dfrac{Q}{\tau'} \end{pmatrix}$$

l'una di grado P, l'altra di grado Q; dovremo avere

$$\sigma = \tau\tau', \quad \xi = \eta\tau' + \frac{P}{\tau}\zeta, \qquad \frac{n}{\sigma} = \frac{PQ}{\tau\tau'}.$$

Perchè, per qualunque ξ, si possano determinare η, ζ dall'equazione

$$\eta\tau' + \frac{P}{\tau}\zeta = \xi \tag{9}$$

basterà che $\tau' = \dfrac{\sigma}{\tau}$ e $\dfrac{P}{\tau}$ siano primi fra loro, cioè che τ sia il massimo comun divisore di σ, P ed avremo senz'altro

$$\begin{pmatrix} \sigma, & 0 \\ \xi, & \dfrac{n}{\sigma} \end{pmatrix} = \begin{pmatrix} \tau, & 0 \\ \eta, & \dfrac{P}{\tau} \end{pmatrix} \begin{pmatrix} \dfrac{\sigma}{\tau}, & 0 \\ \zeta, & \dfrac{Q\tau}{\sigma} \end{pmatrix};$$

il nostro teorema è così già dimostrato.

Ma supponiamo ora di più che P, Q siano primi fra loro. Allora potremo soddisfare la (9) con un valore di η multiplo di $\dfrac{Q}{\tau'} = \dfrac{Q\tau}{\sigma}$. E infatti, posto

$$\eta = \frac{Q}{\tau'}\eta',$$

la (9) diventa

$$Q\eta' + \frac{P}{\tau}\zeta = \xi, \tag{9*}$$

che si può sempre soddisfare, essendo Q primo con $\dfrac{P}{\tau}$. Inoltre vediamo che dalla (9*) η', e quindi anche η, è perfettamente determinato rispetto al modulo $\dfrac{P}{\tau}$ dalla congruenza

$$Q\eta' \equiv \xi \left(\mathrm{mod}\ \frac{P}{\tau}\right),$$

e similmente ζ è perfettamente determinato rispetto al modulo Q, e a più forte ragione rispetto a $\dfrac{Q}{\tau'}$, da

$$\frac{P}{\tau}\zeta \equiv \xi \ (\mathrm{mod}\ Q).$$

Ne risulta che: *in questo modo di decomposizione*

$$\begin{pmatrix} \sigma, & 0 \\ \xi, & \frac{n}{\sigma} \end{pmatrix} = \begin{pmatrix} \tau, & 0 \\ \frac{Q}{\tau'}\eta', & \frac{P}{\tau} \end{pmatrix} \begin{pmatrix} \tau', & 0 \\ \zeta, & \frac{Q}{\tau'} \end{pmatrix}$$

la classe della trasformazione composta determina completamente quelle delle componenti.

Di più è facile vedere che la trasformazione composta sarà imprimitiva solo quando tale sia una delle componenti. Supponiamo infatti che un numero primo p divida simultaneamente

$$\sigma = \tau \cdot \tau', \quad \frac{n}{\sigma} = \frac{P}{\tau} \cdot \frac{Q}{\tau'}, \quad \xi = Q\eta' + \frac{P}{\tau}\zeta;$$

uno solo dei due numeri τ, τ' sarà divisibile per p. Allora se p divide τ, sarà primo con $\frac{Q}{\tau'}$ e dividerà anche $\frac{P}{\tau}$ e però anche η', per cui la prima trasformazione sarà imprimitiva. Se invece p divide τ', si vedrà similmente che è imprimitiva la seconda.

Di qui risulta che il numero delle trasformazioni primitive di grado $n = PQ$, con P, Q primi fra loro, è il prodotto dei numeri analoghi pei gradi P, Q. Dopo di ciò possiamo subito determinare il numero N delle trasformazioni primitive di un dato grado n. Decomponiamo infatti n nei suoi fattori primi distinti e sia

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r};$$

ricordando che vi sono

$$p^{\alpha-1}(p+1)$$

trasformazioni proprie distinte di grado p^α, avremo pel numero richiesto:

$$N = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_r^{\alpha_r-1} (p_1+1)(p_2+1) \dots (p_r+1).$$

§ 165. — **Trasformazioni di grado primo.**

Ci proponiamo ora di stabilire le formole effettive per le trasformazioni il cui grado n è un numero primo, essendo queste, come si è visto, le trasformazioni elementari colle quali tutte le altre possono comporsi.

Per n primo vi sono soltanto $n+1$ trasformazioni distinte (§ 164), che potremo scrivere sotto forma normale

$$\begin{pmatrix} n, & 0 \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} 1, & 0 \\ -\nu, & n \end{pmatrix},$$

dove ν percorre un sistema completo di resti (mod n), per es. i numeri

$$0,\ 1,\ 2,\ \dots,\ n-1.$$

Le formole (I), (I*) (§ 161), che legano i semi-periodi primitivi ω, ω' ai trasformati Ω, Ω', diventano:

$$\left.\begin{aligned} \omega &= n\Omega, & \omega' &= \Omega' \\ \Omega &= \frac{\omega}{n}, & \Omega' &= \omega' \end{aligned}\right\} \text{ per } \begin{pmatrix} n, & 0 \\ 0, & 1 \end{pmatrix}$$

$$\left.\begin{aligned} \omega &= \Omega, & \omega' &= -\nu\Omega + n\Omega' \\ \Omega &= \omega, & \Omega' &= \frac{\nu\omega + \omega'}{n} \end{aligned}\right\} \text{ per } \begin{pmatrix} 1, & 0 \\ -\nu, & n \end{pmatrix}.$$

Si osservi in particolare che le due trasformazioni

$$\begin{pmatrix} n, & 0 \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}$$

corrispondono rispettivamente alla divisione per n del primo o del secondo periodo.

Gli infiniti non equivalenti della funzione

$$\wp(u \mid \Omega, \Omega')$$

saranno nel primo caso nei punti

$$0,\ \frac{2\omega}{n},\ 2 \cdot \frac{2\omega}{n},\ \dots,\ (n-1)\frac{2\omega}{n}$$

e nel secondo nei punti

$$0,\ \frac{2\nu\omega + 2\omega'}{n},\ 2 \cdot \frac{2\nu\omega + 2\omega'}{n},\ \dots,\ (n-1)\frac{2\nu\omega + 2\omega'}{n}.$$

Se, facendo uso di una notazione già introdotta per le formole di divisione dell'argomento (§ 114), poniamo

$$\tilde{\omega}_\infty = \frac{2\,\omega}{n}\,, \quad \tilde{\omega}_\nu = \frac{2\,\nu\,\omega + 2\,\omega'}{n}\,,$$

vediamo che nel primo caso gli infiniti della $\wp$ trasformata che indicheremo con

$$\wp_\infty\, u\,,$$

sono nei punti

$$r\,\tilde{\omega}_\infty \quad (r = 0, 1, 2 \ldots, n-1)$$

e nel secondo caso la $\wp$ trasformata, che indicheremo con $\wp_\nu u$, avrà gli infiniti nei punti

$$r\,\tilde{\omega}_\nu \; (r = 0, 1, 2, \ldots, n-1).$$

Se di più osserviamo che questi infiniti sono tutti del secondo ordine, col termine d'infinito

$$\frac{1}{(u - r\,\tilde{\omega}_\nu)^2}\,,$$

la formola generale (I) § 105, pag. 37, di decomposizione di una funzione ellittica in elementi semplici ci darà immediatamente

$$(10) \qquad \wp_\nu\, u = C + \wp\, u + \sum_{r=1}^{r=n-1} \wp\,(u - r\,\tilde{\omega}_\nu),$$

dove C è una costante e ν prende gli $n+1$ valori

$$\infty\,,\ 0,\ 1,\ 2,\ \ldots,\ n-1.$$

Indichiamo con g_2, g_3 gli invarianti della primitiva $\wp\, u$ e con

$$G_2^{(\nu)}\,,\quad G_3^{(\nu)}$$

quelli della trasformata $\wp_\nu u$; potremo determinare dalla (10) i valori di C e dei nuovi invarianti $G_2^{(\nu)}$, $G_3^{(\nu)}$ sviluppando i due membri in serie nell'intorno dell'origine e paragonando i coefficienti. Abbiamo così:

$$\frac{1}{u^2} + \frac{G_2^{(\nu)}}{20}\,u^2 + \frac{G_3^{(\nu)}}{28}\,u^4 + \ldots = C + \frac{1}{u^2} + \frac{g_2}{20}\,u^2 + \frac{g_3}{28}\,u^4 + \ldots +$$

$$+ \sum_1^{n-1} \wp\,(r\,\tilde{\omega}_\nu) + \frac{u^2}{2} \sum_1^{n-1} \wp''\,(r\,\tilde{\omega}_\nu) + \frac{u^4}{24} \sum_1^{n-1} \wp^{\mathrm{IV}}\,(r\,\tilde{\omega}_\nu) + \ldots$$

e il paragone dei termini scritti ci dà

$$C = -\sum_r^{1\ldots(n-1)} \wp\,(r\,\tilde{\omega}_\nu)\,, \qquad G_2^{(\nu)} = g_2 + 10 \sum_r^{1\ldots(n-1)} \wp''\,(r\,\tilde{\omega}_\nu)\,,$$

$$G_3^{(\nu)} = g_3 + \frac{7}{6} \sum_r^{1\ldots(n-1)} \wp^{\mathrm{IV}}\,(r\,\tilde{\omega}_\nu)\,,$$

per cui la (10) può scriversi

$$(\mathrm{II}) \qquad \wp_\nu\, u = \wp\, u + \sum_r^{1\ldots(n-1)} [\wp\,(u - r\,\tilde{\omega}_\nu) - \wp\,(r\,\tilde{\omega}_\nu)]\,,$$

mentre per gli invarianti $G_2^{(\nu)}$, $G_3^{(\nu)}$ si hanno le formole

$$(\mathrm{III}) \quad \begin{cases} G_2^{(\nu)} = 60 \displaystyle\sum_r^{1\ldots(n-1)} \wp^2\,(r\,\tilde{\omega}_\nu) - (5\,n - 6)\,g_2 \\ G_3^{(\nu)} = 140 \displaystyle\sum_r^{1\ldots(n-1)} \wp^3\,(r\,\tilde{\omega}_\nu) - 21\,g_2 \sum_r^{1\ldots(n-1)} \wp\,(r\,\tilde{\omega}_\nu) - (14\,n - 15)\,g_3 \end{cases}$$

§ 166. — Distinzione del caso di $n = 2$ e di n dispari.

Il secondo membro della formola di trasformazione (II) deve potersi cangiare in una funzione razionale di $\wp\, u$, ciò che ora vogliamo fare. Per ciò distinguiamo il caso di $n = 2$ da quello in cui n è un numero primo dispari.

a) Trasformazioni di secondo grado : Per $n = 2$, ponendo in evidenza nella (II) i periodi 2Ω, $2\Omega'$ della $\wp$ trasformata, avremo le tre formole :

$$
(11)\qquad
\left\{
\begin{aligned}
&\begin{pmatrix}2, & 0\\ 0, & 1\end{pmatrix} \quad \wp_\infty u = \wp\left(u \mid \frac{\omega}{2}, \omega'\right) = \wp u + \wp(u-\omega) - \wp\omega = \\
&\qquad\qquad = \wp u + \frac{(e_1-e_2)(e_1-e_3)}{\wp u - e_1} \\
&\begin{pmatrix}1, & 0\\ 0, & 2\end{pmatrix} \quad \wp_0 u = \wp\left(u \mid \omega, \frac{\omega'}{2}\right) = \wp u + \wp(u-\omega') - \wp\omega' = \\
&\qquad\qquad = \wp u + \frac{(e_3-e_1)(e_3-e_2)}{\wp u - e_3} \\
&\begin{pmatrix}1, & 0\\ -1, & 2\end{pmatrix} \quad \wp_1 u = \wp\left(u \mid \omega, \frac{\omega+\omega'}{2}\right) = \wp u + \wp(u-\omega-\omega') - \\
&\qquad\qquad - \wp(\omega+\omega') = \wp u + \frac{(e_2-e_1)(e_2-e_3)}{\wp u - e_2},
\end{aligned}
\right.
$$

in cui i secondi membri sono appunto razionali di secondo grado in $\wp u$.

Ritornando sui risultati del Cap. XIII relativi all'andamento della $\wp(u\,;\, g_2, g_3)$ per valori reali degli invarianti, *possiamo utilizzare le trasformazioni del secondo ordine per ridurre il calcolo delle funzioni $\wp u$ con discriminante negativo a quello delle $\wp u$ con discriminante positivo.* Per una funzione

$$\bar{\wp} u = \wp(u \mid \omega_1, \omega_3)$$

con invarianti reali e discriminante negativo possiamo infatti scegliere i periodi fondamentali $2\omega_1$, $2\omega_3$ in guisa che siano coniugati (§ 142, pag. 138). Se poniamo allora

$$\wp u = \wp(u \mid \omega, \omega'),$$

essendo

$$\left\{\begin{aligned} \omega &= \omega_1 + \omega_3 \\ \omega' &= -\omega_1 + \omega_3, \end{aligned}\right.$$

la $\wp u$ sarà ad invarianti reali e discriminante positivo e sarà legata alla $\bar{\wp} u$ dalla trasformazione di secondo ordine

$$\begin{pmatrix}1, & 1\\ -1, & 1\end{pmatrix} = \begin{pmatrix}1, & 0\\ -1, & 2\end{pmatrix} \begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix},$$

cioè dalla terza delle (11) :

$$\bar{\wp} u = \wp u + \frac{(e_2-e_1)(e_2-e_3)}{\wp u - e_2},$$

formola che raggiunge lo scopo prefisso.

b) Trasformazioni d'ordine primo dispari. — Sia ora n un numero primo dispari.

In tal caso la (II) può scriversi :

$$\wp_\nu(u) = \wp u - \sum_r^{1\ldots(n-1)} \wp(r\tilde{\omega}_\nu) + \sum_s^{1\ldots\frac{n-1}{2}} \left\{ \wp(u - s\tilde{\omega}_\nu) + \wp(u-(n-s)\tilde{\omega}_\nu \right\}$$

$$\wp_\nu(u) = \wp u - \sum_r^{1\ldots(n-1)} \wp(r\tilde{\omega}_\nu) + \sum_s^{1\ldots\frac{n-1}{2}} \left\{ \wp(u - s\tilde{\omega}_\nu) + \wp(u + s\tilde{\omega}_\nu) \right\},$$

ovvero per le formole d'addizione della $\wp u$:

$$
\text{(IV)}\qquad \wp_\nu u = \wp u - \sum_r^{1\ldots(n-1)} \wp(r\tilde{\omega}_\nu) +
$$
$$
+ \sum_s^{1\ldots\frac{n-1}{2}} \frac{(2\wp u\, \wp(s\tilde{\omega}_\nu) - \tfrac{1}{2} g_2)(\wp u + \wp(s\tilde{\omega}_\nu)) - g_2}{[\wp u - \wp(s\tilde{\omega}_\nu)]^2}.
$$

In questa formola di trasformazione il secondo membro è evidentemente una funzione razionale di $\wp u$ di grado n, e precisamente di grado n al numeratore, di grado $n-1$ al denominatore.

Rispetto ai coefficienti di questa funzione razionale, si osservi che essi sono composti razionalmente con g_2, g_3 e con $\wp(\omega_\nu)$, poichè, per le formole di moltiplicazione, $\wp(r\,\omega_\nu)$ è razionale in $\wp\,\omega_\nu$, e siccome $\wp\,\omega_\nu$ è una radice dell'equazione per la divisione dei periodi, vediamo che i detti coefficienti sono funzioni algebriche di g_2, g_3. Essi saranno noti appena risoluta la risolvente di grado $n+1$ dell'equazione per la divisione dei periodi (§ 115).

§ 167. — Risolubilità per radicali dell'equazione di trasformazione.

Data la $\wp u$, ciascuna delle $n+1$ $\wp_\nu u$ trasformate si esprime razionalmente per $\wp u$ secondo la formola (IV). Ora vogliamo ricercare inversamente come data la $\wp u$, per un valore fisso di ν, si può determinare la $\wp u$. Abbiamo per ciò dalla (IV) un'equazione di grado n in $\wp u$, di cui è facile assegnare le radici. Data infatti $\wp_\nu u$, l'argomento u è determinato solo a meno del segno e di multipli dei periodi 2Ω, $2\Omega'$; cioè tutti i valori di u che dànno il medesimo valore di $\wp_\nu u$ sono della forma

$$\pm u + k\,\bar{\omega}_\nu + 2\,r\,\omega + 2\,s\,\omega' \quad \left\{ \begin{array}{l} k = 0,\ 1,\ 2,\ \ldots,\ n-1 \\ r,\ s \text{ interi qualunque}, \end{array} \right.$$

onde le radici della (IV) sono

$$\wp u, \quad \wp(u - \bar{\omega}_\nu), \quad \wp(u - 2\,\bar{\omega}_\nu) \ldots\ \wp(u - (n-1)\,\bar{\omega}_\nu).$$

Ora una qualunque di esse

$$y_r = \wp(u - r\,\bar{\omega}_\nu)$$

è esprimibile razionalmente, colle formole d'addizione, per $\wp u$, $\wp' u$, e d'altronde, derivando la (IV), si ha

$$\wp'_\nu u = \wp' u\, F(\wp u),$$

essendo F razionale in $\wp u$. Dunque se, oltre $\wp_\nu u$, consideriamo come nota anche $\wp'_\nu u$, ogni radice y_r della (IV) è razionalmente esprimibile per la prima $y_0 = \wp u$. Siamo per ciò in presenza di un'equazione Abeliana di grado primo n e la risoluzione si effettua estraendo un radicale d'indice n. Quanto alle quantità che compariranno razionalmente sotto il radicale $\sqrt[n]{\ }$, saranno evidentemente

$$g_2, \quad g_3, \quad \wp\,\bar{\omega}_\nu, \quad \wp_\nu u, \quad \wp'_\nu u.$$

È facile anche dare la effettiva formola di risoluzione; ma noi qui osserveremo soltanto ancora che la risoluzione delle equazioni di trasformazione include quella delle equazioni per la divisione dell'argomento. Per vederlo basta ricordare che la moltiplicazione per n dell'argomento si compone delle due successive trasformazioni $\begin{pmatrix} n, & 0 \\ 0, & 1 \end{pmatrix}$, $\begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}$. Così la teoria della trasformazione riduce effettivamente la risoluzione dell'equazione Abeliana composta di grado n^2, che si presenta nel problema della divisione per n dell'argomento, a quella di due successive equazioni Abeliane semplici di grado n.

§ 168. — Esistenza dell'equazione modulare fra gli invarianti assoluti.

Indichiamo con

$$J(\tau) = \frac{g_2^3}{g_2^3 - 27\,g_3^2}, \qquad \tau = \frac{\omega'}{\omega}$$

l'invariante assoluto J della $\wp u$ primitiva e con

$$J' = \frac{G_2^3}{G_2^3 - 27\,G_3^2}$$

l'invariante assoluto di una qualunque delle $n+1$ $\bar{\wp} u$ trasformate, sicchè sarà

$$J' = J\left(\frac{\Omega'}{\Omega}\right),$$

e chiamando J'_ν l'invariante assoluto della $\wp_\nu v$ sarà dunque

$$J'_\infty = J(n\,\tau), \quad J'_0 = J\left(\frac{\tau}{n}\right),$$

$$J'_1 = J\left(\frac{\tau+1}{n}\right) \ldots\ J'_{n-1} = J\left(\frac{\tau+(n-1)}{n}\right).$$

Ora sussiste l'importante teorema:

Fra l'invariante J della $\wp u$ primitiva e l'invariante J' di una qualunque $\wp u$, ottenuta per trasformazione d'ordine primo n, sussiste un'equazione algebrica

$$\text{(V)} \qquad f(J, J') = 0$$

di grado $n+1$ in J', le cui $n+1$ radici in J' sono date da

$$J'_\infty = J(n\,\tau), \qquad J'_0 = J\left(\frac{\tau}{n}\right),$$

$$J'_1 = J\left(\frac{\tau+1}{n}\right) \ldots\ J'_{n-1} = J\left(\frac{\tau+(n-1)}{n}\right).$$

È questa l'equazione che prende il nome di *equazione modulare* (fra gli invarianti assoluti).

Per dimostrare il teorema, basta osservare che, secondo le formole (III) § 165 che dànno i valori degli invarianti G_2, G_3 trasformati, l'invariante J'_ν è una funzione razionale simmetrica di

$$\wp\,\tilde{\omega}_\nu,\quad \wp\,(2\,\tilde{\omega}_\nu)\ldots.\ \wp\left(\frac{n-1}{2}\;\tilde{\omega}_\nu\right), \tag{12}$$

che sono radici di una medesima orizzontale dell'equazione per la divisione dell'argomento nel quadro (C) del § 114 (pag. 63). Questa funzione razionale simmetrica dei valori (12) ha quindi appunto $n+1$ valori distinti

$$J'_\infty,\ J'_0\ J'_1\ J'_2\ \ldots.\ J'_{n-1},$$

che sono dunque radici di una risolvente di grado $n+1$

$$F(J',\ g_2,\ g_3)=0 \tag{13}$$

con coefficienti razionali in g_2, g_3. Ma se osserviamo che cangiando ω, ω' in $i\,\omega$, $i\,\omega'$ l'argomento τ e g_2 non cangiano, mentre g_3 cangia segno, si vede che nella (13) figurerà solo razionalmente g_3^2 e similmente, poichè cangiando ω, ω' in $\varepsilon\,\omega$, $\varepsilon\,\omega'$ $\left(\varepsilon=e^{\frac{2\pi i}{3}}\right)$ g_3 non muta, e g_2 si cangia in $\varepsilon^2\,g_2$, dovrà nella (13) g_2 comparire solo nelle potenze di g_2^3. Eliminando ora dalla (13) g_3^2 per mezzo della relazione

$$J=\frac{g_2^3}{g_2^3-27\,g_3^2},$$

la (13) acquisterà la forma

$$\psi(J',\ J,\ g_2)=0, \tag{14}$$

essendo ψ razionale nei tre argomenti.

Ma è facile vedere che in questa equazione g_2 non può figurare esplicitamente, che cioè coll'eliminazione di g_3 dalla (13) viene eliminato anche g_2. E infatti se cangiamo ω, ω' in $\lambda\,\omega$, $\lambda\,\omega'$, con λ qualunque, nella (14) J, J' restano inalterati, mentre g_2 si cangia in $\frac{g_2}{\lambda^4}$ e però g_2 deve necessariamente sparire.

Così è provata l'esistenza dell'equazione modulare (V).

Studieremo fra breve più da vicino ed in modo diretto le proprietà dell'equazione modulare (V). Ma fin d'ora osserviamo che, secondo i risultati del § 116, siamo in grado di assegnare il suo gruppo di monodromia, che è definito dalle sostituzioni lineari

$$\nu'\equiv\frac{\alpha\nu+\beta}{\gamma\nu+\delta}\quad(\alpha\delta-\beta\gamma\equiv 1\ \ (\mathrm{mod}\ n))$$

sugli indici degli $n+1$ rami J'_ν

$$J'_\infty,\quad J'_0,\quad J'_1\ \ldots.\ J'_{n-1}.$$

§ 169. — Formole di trasformazione per la $\sigma\,u$.

Cerchiamo ora di esprimere anche le $\sigma\,u$ coi periodi trasformati

$$\sigma\left(u\,|\,\frac{\omega}{n},\ \omega'\right),\ \sigma\left(u\,|\,\omega,\ \frac{\nu\,\omega+\omega'}{n}\right)$$

per la $\sigma\,u$ primitiva. Se osserviamo che si ha

$$\sigma\left(u\,|\,\omega,\ \frac{\nu\,\omega+\omega'}{n}\right)=\sigma\left(u\,|-\frac{\nu\,\omega+\omega'}{n},\ \omega\right)$$

$$\sigma(u\,|\,\omega,\ \omega')=\sigma(u\,|-(\nu\,\omega+\omega'),\ \omega),$$

vediamo che tutto si riduce a trovare la formola che esprime $\sigma\left(u\,|\,\frac{\omega}{n},\ \omega'\right)$ per $\sigma\,u$, cioè la formola che dà per la $\sigma\,u$ l'effetto della divisione per n del primo periodo.

Ora la σ trasformata,

$$\bar{\sigma}\,u=\sigma\left(u\,|\,\frac{\omega}{n},\ \omega'\right)$$

può anche considerarsi, secondo il § 101, come una funzione intera periodica di terza categoria coi periodi $2\,\omega$, $2\,\omega'$ e si può quindi esprimere per la $\sigma\,u$, appena se ne determinino nel primo parallelogrammo dei periodi gli infinitesimi. Questi sono nei punti

$$u_0=0,\ \frac{2\,\omega}{n},\ 2\,.\,\frac{2\,\omega}{n},\ \ldots.\ (n-1)\,.\,\frac{2\,\omega}{n}$$

e si ha per ciò :

$$(15) \qquad \bar{\sigma} u = e^{G(u)} \prod_{r=0}^{r=n-1} \sigma\left(u - r\,.\,\frac{2\omega}{n}\right),$$

dove $G(u)$ è un polinomio di secondo grado in u.

Supponiamo dapprima n dispari e scriviamo la (15) così :

$$\bar{\sigma} u = e^{G_1(u)}\,.\,\sigma u \prod_{s=1}^{s=\frac{n-1}{2}} \sigma\left(s\,.\,\frac{2\omega}{n} - u\right) \sigma\left(s\,.\,\frac{2\omega}{n} + u\right),$$

dove $G_1(u)$ sarà nuovamente un polinomio di secondo grado in u e poichè $\bar{\sigma} u$, σu sono dispari, mentre il prodotto nel secondo membro è pari, sarà

$$G_1(u) = \frac{1}{2} a u^2 + b \quad (a, b \text{ costanti}),$$

onde avremo

$$\bar{\sigma} u = C e^{\frac{1}{2} a u^2} \sigma u \prod_{s=1}^{s=\frac{n-1}{2}} \sigma\left(s\,.\,\frac{2\omega}{n} - u\right) \sigma\left(s\,.\,\frac{2\omega}{n} + u\right).$$

Per determinare la costante C, basta dividere dall' una e dall'altra parte per u e passare al limite per $u = 0$; si ottiene così :

$$(\mathrm{VI}) \qquad \bar{\sigma} u = e^{\frac{1}{2} a u^2} \sigma u \prod_{s=1}^{s=\frac{n-1}{2}} \frac{\sigma\left(s\,.\,\frac{2\omega}{n} - u\right) \sigma\left(s\,.\,\frac{2\omega}{n} + u\right)}{\sigma^2\left(s\,.\,\frac{2\omega}{n}\right)}$$

In fine, per determinare la costante a, si indichino con $\bar{\eta}$, $\bar{\eta}'$ i semiperiodi di seconda specie della $\bar{\sigma} u$ coi periodi di prima specie $2\bar{\omega} = \frac{2\omega}{n}$, $2\bar{\omega}' = 2\omega'$, talchè sarà

$$\bar{\eta}\bar{\omega}' - \bar{\eta}'\bar{\omega} = \frac{\pi i}{2},$$

cioè

$$(16) \qquad n\bar{\eta}\,\omega' - \bar{\eta}'\,\omega = n\frac{\pi i}{2}.$$

Cangiando allora nella (VI) successivamente u in $u + 2\omega = u + 2n\bar{\omega}$ ed in $u + 2\omega' = u + 2\bar{\omega}'$, si ricava subito

$$(17) \qquad a = \frac{n(\bar{\eta} - \eta)}{\omega} = \frac{\bar{\eta}' - n\eta'}{\omega'}$$

e la coincidenza di questi due valori per a risulta subito dalla (16).

Alla (VI) si può dare un differente aspetto, ricordando la formola

$$\frac{\sigma\left(s\,.\,\frac{2\omega}{n} - u\right) \sigma\left(s\,.\,\frac{2\omega}{n} + u\right)}{\sigma^2\left(s\,.\,\frac{2\omega}{n}\right)\sigma^2 u} = \wp u - \wp\left(s\,.\,\frac{2\omega}{n}\right),$$

e scrivendola quindi

$$(\mathrm{VI}^*) \qquad \bar{\sigma} u = e^{\frac{1}{2} a u^2} \sigma^n u \prod_{r=1}^{r=\frac{n-1}{2}} \left\{\wp u - \wp\left(s\,.\,\frac{2\omega}{n}\right)\right\}.$$

Dalle (VI), (VI*) si potrebbero ora dedurre le formole di trasformazione per le σ pari

$$\sigma_1 u, \quad \sigma_2 u, \quad \sigma_3 u,$$

e combinando per divisione le formole così ottenute, si avrebbero le formole di trasformazione per

$$\mathrm{sn}\, v, \quad \mathrm{cn}\, v, \quad \mathrm{dn}\, v,$$

come furono poste da Jacobi nei *Fundamenta nova*.

§ 170. — **Trasformazione di Landen.**

Ci limiteremo a dedurre le formole di trasformazione di secondo ordine per sn v, a stabilire cioè per questa funzione ellittica la formola di duplicazione del rapporto τ dei periodi. Interpretata per l' integrale ellittico di prima specie, questa conduce alla celebre trasformazione scoperta dal matematico inglese Landen (1775-1780), scoperta che ha preceduto la costruzione della teoria degli integrali ellittici di Legendre ed è stata la sorgente dell' intera teoria della trasformazione.

Ritorniamo alla formola (15) di trasformazione per σu e supponiamo ora $n = 2$. Avremo

$$\bar{\sigma} u = \sigma\left(u \mid \frac{\omega}{2}\,,\ \omega'\right) = e^{G(u)}\,\sigma u\ \sigma(u-\omega)\,,$$

che, per la formola

$$\sigma_1 u = e^{\eta u}\,\frac{\sigma(\omega - u)}{\sigma\omega}\,,$$

possiamo scrivere :

$$\bar{\sigma} u = e^{G_1(u)}\,\sigma u\,.\,\sigma_1 u.$$

Il polinomio di secondo grado $G_1(u)$ deve essere pari e si ha quindi

$$\bar{\sigma} u = C\,e^{\frac{1}{2} a u^2}\,\sigma u\ \sigma_1 u\,,$$

con C, a costanti. Si trova subito

$$C = 1\,,\quad a = \frac{\bar{\eta} - \eta}{\omega}\,,$$

onde

(VII) $$\sigma\left(u \mid \frac{\omega}{2}\,,\ \omega'\right) = e^{\frac{\bar{\eta}-\eta}{\omega}u^2}\,\sigma u\ \sigma_1 u.$$

Mutando in questa u in $u + \omega'$, si trova la formola di trasformazione per $\sigma_3 u$:

(VII*) $$\sigma_3\left(u \mid \frac{\omega}{2}\,,\ \omega'\right) = e^{\frac{\bar{\eta}-\eta}{\omega}u^2}\,\sigma_2 u\ \sigma_3 u\,,$$

ed analogamente si dedurrebbero le formole per $\sigma_1 u$, $\sigma_2 v$.

Indichiamo con $\bar{e}_1\,,\ \bar{e}_2\,,\ \bar{e}_3$ i valori di $e_1\,,\ e_2\,,\ e_3$ rispondenti ai nuovi periodi

$$2\,\bar{\omega} = \omega\,,\quad 2\,\bar{\omega}' = 2\,\omega'$$

e dividendo la (VII) per la (VII*), col ricordare le formole (C) § 133 (pag. 113) avremo

$$\frac{1}{\sqrt{\bar{e}_1 - \bar{e}_3}}\operatorname{sn}(v_1\,,\ 2\tau) = \frac{1}{\sqrt{e_1 - e_3}}\,\frac{\operatorname{sn}(v\,,\tau)\operatorname{cn}(v\,,\tau)}{\operatorname{dn}(v\,,\tau)}$$

con

$$v_1 = \sqrt{\bar{e}_1 - \bar{e}_3}\,.\,u,\quad v = \sqrt{e_1 - e_3}\,.\,u\,.$$

Se poniamo

$$M = \frac{\sqrt{\bar{e}_1 - \bar{e}_3}}{\sqrt{e_1 - e_3}}\,,$$

potremo scrivere la formola così :

(18) $$\operatorname{sn}(M v\,,\ 2\tau) = M\,\frac{\operatorname{sn} v\ \operatorname{cn} v}{\operatorname{dn} v}\,.$$

Indicando con $4\,\bar{K}\,,\ 2\,i\,\bar{K}'$ i periodi di $\operatorname{sn}(v\,,2\tau)$ corrispondenti a $4\,K\,,\ 2\,i\,K'$ per $\operatorname{sn}(v\,,\tau)$, abbiamo

(19) $$\begin{cases} \bar{K} = \bar{\omega}\,\sqrt{\bar{e}_1 - \bar{e}_2} = M\,\dfrac{K}{2} \\ i\,\bar{K}' = \bar{\omega}'\,\sqrt{\bar{e}_1 - \bar{e}_3} = M\,i\,K' \end{cases}$$

e potremo determinare il *moltiplicatore* M della (18) e il modulo $\bar{k} = k\,(2\,\tau)$ colle considerazioni seguenti. Pongasi nella (18) $v = \dfrac{K}{2}$ e poichè $\operatorname{sn}(\bar{K}\,,2\,\tau) = 1$, avremo

$$M = \frac{\operatorname{dn}\dfrac{K}{2}}{\operatorname{sn}\dfrac{K}{2}\ \operatorname{cn}\dfrac{K}{2}}\,.$$

Ma dalle formole

$$\mathrm{sn}\,(v+K)=\frac{\mathrm{cn}\,v}{\mathrm{dn}\,v},\quad \mathrm{dn}\,(v+K)=\frac{k'}{\mathrm{dn}\,v},$$

ponendo $v=-\frac{K}{2}$, deduciamo

$$\mathrm{sn}\,\frac{K}{2}=\frac{\mathrm{cn}\,\frac{K}{2}}{\mathrm{dn}\,\frac{K}{2}},\quad \mathrm{dn}^2\frac{K}{2}=k',$$

onde

$$M=\frac{\mathrm{dn}^2\frac{K}{2}}{\mathrm{cn}^2\frac{K}{2}}=1+k'.$$

Ora moltiplichiamo i due membri della (18) per

$$v-i\,K'=\frac{1}{M}(M\,v-i\,\bar{K}')$$

e ricordando che i residui di $\mathrm{sn}\,v$, $\mathrm{cn}\,v$, $\mathrm{dn}\,v$ in $v=i\,K'$ sono rispettivamente $\frac{1}{k}$, $\frac{-i}{k}$, $-i$, troveremo

$$\bar{k}=\frac{1-k'}{1+k'}\ ^{1)}.$$

Ed ora, ponendo in evidenza nella (18) i moduli anzichè i periodi, avremo la formola di trasformazione

$$\text{(VIII)}\quad \mathrm{sn}\left[(1+k')\,v,\frac{1-k'}{1+k'}\right]=(1+k')\,\frac{\mathrm{sn}\,(v,k)\,\mathrm{cn}\,(v,k)}{\mathrm{dn}\,(v,k)}$$

che è la formola della trasformazione di Landen.

1) Rispetto alla funzione modulare $k(\tau)$, possiamo scrivere la formola

$$k(2\tau)=\frac{1-\sqrt{1-k^2(\tau)}}{1+\sqrt{1-k^2(\tau)}},$$

formola che dà l'effetto della duplicazione dell'argomento.

§ 171. — Applicazione della trasformazione di Landen.

La trasformazione di Landen si può utilmente applicare al calcolo numerico degli integrali ellittici di prima specie. Poniamo per ciò

$$y=\mathrm{sn}\,[\,(1+k')\,v,\bar{k}\,],\quad x=\mathrm{sn}\,(v,k),\quad \bar{k}'=\frac{1-k'}{1+k'}$$

ed avremo

$$\frac{d\,y}{\sqrt{(1-y^2)\,(1-\bar{k}^2y^2)}}=(1+k')\,d\,v,\quad \frac{d\,x}{\sqrt{(1-x^2)\,(1-k^2x^2)}}=d\,v.$$

Supponiamo il caso ordinario delle applicazioni in cui k, quindi anche $\bar{k}$, è reale positivo e minor d'uno ed, osservando che y si annulla con x, avremo

$$\text{(20)}\quad \int_0^x\frac{d\,x}{\sqrt{(1-x^2)\,(1-k^2x^2)}}=\frac{1}{1+k'}\int_0^y\frac{d\,y}{\sqrt{(1-y^2)(1-\bar{k}^2y^2)}}$$

e la (VIII) diverrà

$$\text{(21)}\quad y=(1+k')\,\frac{x\sqrt{1-x^2}}{\sqrt{1-k^2x^2}}.$$

Con questa trasformazione irrazionale si cangia dunque un integrale ellittico di prima specie di modulo k in un altro di modulo

$$\text{(22)}\quad \bar{k}=\frac{1-k'}{1+k'}=\frac{k^2}{(1+k')^2},$$

e si avranno ancora le formole

$$\text{(22*)}\quad k=\frac{2\sqrt{\bar{k}}}{1+\bar{k}},\quad 1+k'=\frac{2}{1+\bar{k}},$$

onde la (20) potrà scriversi

$$(20^*)\quad \int_0^y \frac{dy}{\sqrt{(1-y^2)\ (1-\bar{k}^2 y^2)}} = \frac{2}{1+\bar{k}} \int_0^x \frac{dx}{\sqrt{(1-x^2)\ (1-k^2 x^2)}}$$

Essendo $0 < k < 1$, il modulo trasformato

$$\bar{k} = \frac{k^2}{(1+k')^2}$$

sarà $< k^2$ e quindi più vicino a zero. Ripetendo n volte la trasformazione (20), si arriverà ad un modulo $< k^{2n}$, vicino quindi a zero quanto ci piace.

Colla trasformazione inversa (20*) passiamo dal modulo $\bar{k}$ al modulo

$$k = \frac{2}{1+\bar{k}} \sqrt{\bar{k}} > \sqrt{\bar{k}}$$

e, ripetendola n volte, ad un modulo così vicino ad uno quanto ci piace. Nelle applicazioni numeriche converrà fare uso della scala discendente o ascendente dei moduli, secondo che k è più prossimo a 0 ovvero ad 1, e nel primo caso si ridurrà il calcolo dell' integrale a quello di un arco circolare, nel secondo al calcolo di logaritmi o funzioni iperboliche.

§ 172. — La trasformazione di Landen nelle amplitudini.

Rendiamo le formole precedenti atte al calcolo logaritmico, introducendo le amplitudini degli integrali ellittici col porre

$$y = \operatorname{sen} \psi, \quad x = \operatorname{sen} \varphi,$$

e la (21) diventerà :

$$\operatorname{sen} \psi = (1+k') \frac{\operatorname{sen} \varphi \cos \varphi}{\sqrt{1-k^2 \operatorname{sen}^2 \varphi}},$$

da cui si ottiene subito

$$\cos \psi = \frac{\cos^2 \varphi - k' \operatorname{sen}^2 \varphi}{\sqrt{1-k^2 \operatorname{sen}^2 \varphi}}\ ^{1)},$$

e quindi

$$(23)\quad \operatorname{tang} \psi = \frac{(1+k') \operatorname{tang} \varphi}{1-k' \operatorname{tang}^2 \varphi}.$$

Derivando otteniamo

$$\frac{d\psi}{d\varphi} = (1+k') \frac{1+k' \operatorname{tang}^2 \varphi}{(1-k' \operatorname{tang}^2 \varphi)^2} \frac{\cos^2 \psi}{\cos^2 \varphi},$$

il che dimostra che ψ è sempre crescente per φ crescente, e inoltre ai valori

$$0, \ \frac{\pi}{2}, \ \pi, \ 3\frac{\pi}{2}, \dots \text{ per } \varphi$$

corrispondono i valori duplicati

$$0, \ \pi, \ 2\pi, \ 3\pi, \dots \text{ per } \psi.$$

Ora la (23), ridotta a forma intera, ci dà l'altra

$$(24)\quad \operatorname{tang}(\psi - \varphi) = k' \operatorname{tang} \varphi,$$

che si presta al calcolo logaritmico di ψ, dato che sia φ. Scrivendo poi questa formola così

$$(1+\bar{k}) \operatorname{tang}(\psi - \varphi) = (1-\bar{k}) \operatorname{tang} \varphi,$$

ovvero

$$\operatorname{sen}(\psi-\varphi)\cos\varphi - \operatorname{sen}\varphi\cos(\psi-\varphi) = -\bar{k}\{\operatorname{sen}\varphi\cos(\psi-\varphi) + \cos\varphi \operatorname{sen}(\psi-\varphi)\},$$

ne deduciamo

$$(24^*)\quad \operatorname{sen}(2\varphi - \psi) = \bar{k} \operatorname{sen} \psi,$$

1) La determinazione del segno risulta da ciò, che per $\varphi = 0$ è $\psi = 0$.

formola che si presta al calcolo di φ dato ψ. Le (20), (20*) diventano allora

$$(25)\qquad \int_0^\varphi \frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}} = \frac{1}{1+k'}\int_0^\psi \frac{d\psi}{\sqrt{1-\bar{k}^2\operatorname{sen}^2\psi}}$$

$$(25^*)\qquad \int_0^\psi \frac{d\psi}{\sqrt{1-\bar{k}^2\operatorname{sen}^2\psi}} = \frac{2}{1+\bar{k}}\int_0^\varphi \frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}},$$

e si farà uso della prima o della seconda, secondo che si vorrà passare da k a $\bar{k}$, o viceversa.

Supponiamo ora di ripetere n volte la trasformazione (25) e indichiamo con

$$\psi,\ \psi_1,\ \psi_2,\ \ldots,\ \psi_{n-1}$$

le successive amplitudini e con

$$\bar{k},\ \bar{k}_1,\ \bar{k}_2,\ \ldots,\ \bar{k}_{n-1}$$

i successivi moduli trasformati; avremo:

$$\int_0^\varphi \frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}} = \frac{1+\bar{k}}{2}\cdot\frac{1+\bar{k}_1}{2}\cdots\frac{1+\bar{k}_{n-1}}{2}\int_0^{\psi_{n-1}} \frac{d\psi}{\sqrt{1-\bar{k}^2_{n-1}\operatorname{sen}^2\psi}},$$

ove le ψ_i si calcoleranno successivamente dalle formole

$$\operatorname{tang}(\psi_i-\psi_{i-1}) = \bar{k}'_{i-1}\operatorname{tang}\psi_{i-1},$$

essendo $\bar{k}'_{i-1}$ il modulo complementare di $\bar{k}_{i-1}$. Ora si osservi che il prodotto infinito

$$(1+\bar{k})\ (1+\bar{k}_1)\ (1+\bar{k}_2)\ \ldots\ (1+\bar{k}_n)\ \ldots$$

è certamente convergente perchè $\bar{k}_n < \bar{k}^2_{n-1}$, e quindi esisterà pure un limite determinato per $n=\infty$ dell'integrale

$$\frac{1}{2^n}\int_0^{\psi_{n-1}} \frac{d\psi}{\sqrt{1-\bar{k}^2_{n-1}\operatorname{sen}^2\psi}},$$

e poichè

$$\frac{\psi_{n-1}}{2^n} < \frac{1}{2^n}\int_0^{\psi_{n-1}} \frac{d\psi}{\sqrt{1-\bar{k}^2_{n-1}\operatorname{sen}^2\psi}} < \frac{\psi_{n-1}}{2^n}\,\frac{1}{\bar{k}'_{n-1}},$$

si vede che $\dfrac{\psi_{n-1}}{2^n}$ ha lo stesso limite.

Ora se, fra i limiti d'approssimazione voluta, è

$$(1+\bar{k})\ (1+\bar{k}_1)\ \ldots\ (1+\bar{k}_{n-1})\frac{\psi_{n-1}}{2^n}\left(1-\frac{1}{\bar{k}'_{n-1}}\right) = 0$$

si avrà pure, entro i medesimi limiti d'approssimazione:

$$(26)\qquad \int_0^\varphi \frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}} = (1+\bar{k})\ (1+\bar{k}_1)\ \ldots\ (1+\bar{k}_{n-1})\ \frac{\psi_{n-1}}{2^n},$$

formola molto adatta al calcolo numerico, a causa della rapida convergenza del prodotto infinito. Se facciamo nella (26) $\varphi=\dfrac{\pi}{2}$, avremo anche

$$\frac{\psi}{2} = \frac{\psi_1}{2^2} = \frac{\psi_2}{2^3} = \ldots = \frac{\psi_{n-1}}{2^n} = \frac{\pi}{2}$$

e ne otterremo quindi il notevole sviluppo in prodotto infinito

$$(26^*)\qquad \frac{2K}{\pi} = (1+\bar{k})\ (1+\bar{k}_1)\ (1+\bar{k}_2)\ \ldots\ (1+\bar{k}_n)\ \ldots,$$

onde la (26) si scriverà

$$\int_0^\varphi \frac{d\varphi}{\sqrt{1-k^2\operatorname{sen}^2\varphi}} = \frac{2K}{\pi}\lim_{n=\infty}\frac{\psi_{n-1}}{2^n}.$$

I successivi moduli trasformati $\bar{k}$, $\bar{k}_1$ .... si calcoleranno facilmente, coll'uso delle ordinarie tavole trigonometriche, ponendo

$$k=\operatorname{sen}\theta,\quad \bar{k}=\operatorname{sen}\theta_1,\quad \bar{k}_1=\operatorname{sen}\theta_2,\ \ldots,\quad \bar{k}_{n-1}=\operatorname{sen}\theta_n,$$

per cui avremo

$$\bar{k} = \frac{1-k'}{1+k'} = \frac{1-\cos\theta}{1+\cos\theta}, \quad \bar{k}_1 = \frac{1-\cos\theta_1}{1+\cos\theta_1} \ldots,$$

e cioè

$$\operatorname{sen}\theta_1 = \operatorname{tang}^2\frac{\theta}{2}, \quad \operatorname{sen}\theta_2 = \operatorname{tang}^2\frac{\theta_1}{2}, \quad \operatorname{sen}\theta_3 = \operatorname{tang}^2\frac{\theta_2}{2} \ldots.$$

Formole analoghe potrebbero stabilirsi per l'applicazione ripetuta della trasformazione inversa.

§ 173. — Media aritmetico-geometrica $M(a, b)$ secondo Lagrange e Gauss.

La scala dei moduli nell'applicazione ripetuta della trasformazione di Landen sta in una semplice relazione colla teoria della *media aritmetico-geometrica*, della quale si occuparono Lagrange e Gauss. Daremo ancora un cenno di questo argomento storicamente molto importante, che ha segnato la via per la quale Gauss, prevenendo le ricerche di Abel e Jacobi, aveva già costruito la teoria delle funzioni ellittiche senza dare pubblicità alcuna ai risultati conseguiti [1]).

Siano a, b due numeri reali positivi e supponiamo per es.

$$a > b.$$

Costruiamo le due medie, aritmetica e geometrica di a, b :

$$\bar{a} = \frac{a+b}{2}, \quad \bar{b} = \sqrt{a\,b} \text{ [2])}$$

e da $\bar{a}$, $\bar{b}$ deduciamo nello stesso modo

$$\bar{a}_1 = \frac{\bar{a}+\bar{b}}{2}, \quad \bar{b}_1 = \sqrt{\bar{a}\,\bar{b}},$$

1) Gauss, *Werke*, Bd. III, Nachlass.

2) Per questo radicale e tutti i seguenti s'intendono scelti i valori positivi

e così continuiamo costruendo

$$\bar{a}_2 = \frac{\bar{a}_1+\bar{b}_1}{2}, \quad \bar{b}_2 = \sqrt{\bar{a}_1\bar{b}_1},$$

. . . .

$$a_n = \frac{\bar{a}_{n-1}+\bar{b}_{n-1}}{2}, \quad \bar{b}_n = \sqrt{\bar{a}_{n-1}\bar{b}_{n-1}},$$

. . . .

Le due serie di numeri positivi

$$(27) \qquad \begin{cases} a, \ \bar{a}, \ \bar{a}_1, \ \bar{a}_2, \ldots, \bar{a}_n \ldots \\ b, \ \bar{b}, \ \bar{b}_1, \ \bar{b}_2, \ldots, \bar{b}_n \ldots \end{cases}$$

sono decrescente la prima, crescente la seconda, e convergono ambedue verso il medesimo limite, che si dice la media aritmetico-geometrica dei due numeri a, b e si indica con Gauss col simbolo

$$M(a, b).$$

Per dimostrare quanto sopra è asserito basta osservare che, ponendo

$$k = \frac{\sqrt{a^2-b^2}}{a}, \quad \text{indi } k' = \frac{b}{a},$$

e ritenendo le notazioni del paragrafo precedente, si ha

$$\begin{cases} \bar{a} = a\dfrac{1+k'}{2} = \dfrac{a}{1+\bar{k}} \\ \bar{b} = \sqrt{a\,b} = a\sqrt{k'} \end{cases}$$

e in generale

$$\bar{a}_n = \frac{\bar{a}_{n-1}}{1+\bar{k}_n} = \frac{a}{(1+\bar{k})\,(1+\bar{k}_1)\ldots(1+\bar{k}_n)}$$

$$\bar{b}_n = \bar{a}_{n-1}\sqrt{\bar{k}'_{n-1}}.$$

Per la formola (26*) si ha quindi subito

$$\lim_{n=\infty} \bar{a}_n = \frac{\pi a}{2K}$$

e d'altronde

$$\lim_{n=\infty} \frac{\bar{b}_n}{\bar{a}_{n-1}} = \lim \sqrt{k'_{n-1}} = 1\,,$$

quindi

$$M(a, b) = \lim_{n=\infty} \bar{a}_n = \lim_{n=\infty} \bar{b}_n = \frac{\pi a}{2K}$$

Così sono dimostrate le nostre asserzioni ed è inoltre trovata la formola

$$\text{(IX)} \qquad \frac{1}{M(a, b)} = \frac{2K}{\pi a} = \frac{2}{\pi a} \int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{1 - k^2 \operatorname{sen}^2 \varphi}}\,,$$

che esprime l'inversa della media aritmetico-geometrica per un integrale completo ellittico di prima specie a modulo

$$k = \frac{\sqrt{a^2 - b^2}}{a}\,.$$

La proprietà delle due serie (27) di convergere verso un limite comune $M(a, b)$ si può del resto dimostrare colle seguenti considerazioni elementari [1]). Essendo

$$(\bar{a} - \bar{b})\,(\bar{a} + \bar{b}) = \bar{a}^2 - \bar{b}^2 = \frac{1}{4}\,(a - b)^2$$

si vede che $\bar{b} < \bar{a}$ e così

$$\bar{b} < \bar{a}\,,\ \bar{b}_1 < \bar{a}_1\,,\ \bar{b}_2 < \bar{a}_2\,, \ldots, \bar{b}_n < \bar{a}_n \ldots,$$

cioè ogni termine della serie inferiore è minore del corrispondente della superiore.

[1]) Gauss, loc. cit.

Si ha poi evidentemente

$$\bar{a} < a\,,\quad \bar{a}_1 < \bar{a}\,,\quad \bar{a}_2 < \bar{a}_1\,, \ldots.$$

$$\bar{b} > b\,,\quad \bar{b}_1 > \bar{b}\,,\quad \bar{b}_2 > \bar{b}_1\,, \ldots.$$

e però la prima serie è continuamente decrescente, la seconda crescente; di più si ha

$$\frac{\bar{a} - \bar{b}}{a - b} = \frac{a - b}{4(\bar{a} + \bar{b})} = \frac{a - b}{2(a + b) + 4\bar{b}} < \frac{1}{2}\,,$$

indi

$$\bar{a} - \bar{b} < \frac{1}{2}\,(a - b)$$

$$\bar{a}_1 - \bar{b}_1 < \frac{1}{2}\,(\bar{a} - \bar{b}) < \frac{1}{4}\,(a - b)$$

$$\cdots\cdots\cdots\cdots$$

$$\bar{a}_n - \bar{b}_n < \frac{1}{2^{n+1}}\,(a - b)\,,$$

dopo di che risulta evidente l'esistenza di un limite comune $M(a, b)$ per le due serie.

Se nella formola (IX) cangiamo b in $c = \sqrt{a^2 - b^2}$, manifestamente k si cangia in k' e perciò K in K', onde abbiamo:

$$\text{(IX*)} \qquad \frac{1}{M(a, c)} = \frac{2K'}{\pi a} = \frac{2}{\pi a} \int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{1 - k'^2 \operatorname{sen}^2 \varphi}}\,.$$

La quantità $q = e^{\pi i \tau} = e^{\frac{-\pi K'}{K}}$ di Jacobi si può quindi anche scrivere

$$q = e^{-\pi \frac{M(a, b)}{M(a, c)}}$$

e, se introduciamo coi simboli di Gauss le tre quantità

$$P = \sqrt{\frac{a}{M(a, b)}}\,,\quad Q = \sqrt{\frac{b}{M(a, b)}}\,,\quad R = \sqrt{\frac{c}{M(a, b)}}\,,$$

avremo evidentemente

$$P = \sqrt{\frac{2K}{\pi}}, \quad Q = \sqrt{\frac{2KK'}{\pi}}, \quad R = \sqrt{\frac{2Kk}{\pi}},$$

e varranno gli sviluppi in serie di potenze di q, già dati da Gauss:

$$P = 1 + 2\sum_1^\infty q^{n^2}, \quad Q = 1 + 2\sum_1^\infty (-1)^n q^{n^2}, \quad R = 2\sum_1^\infty q^{\frac{(2n+1)^n}{4}}$$

che per noi risultano già dalle formole dimostrate al § 158.

CAPITOLO XVI.

Funzioni modulari ellittiche.

§ 174. — Definizione delle funzioni modulari. — Loro sottogruppo.

Strettamente connessa colla teoria delle funzioni ellittiche è la teoria delle funzioni modulari (ellittiche), la quale a sua volta non è che un capitolo della grande teoria delle funzioni automorfe. Già in vari punti di questo corso (cfr. particolarmente i Cap. XI, XII, XV) abbiamo toccato delle proprietà di due funzioni fondamentali nella classe delle funzioni modulari, e cioè dell' invariante assoluto $J(\tau)$ e del quadrato del modulo di Legendre $k^2(\tau)$. Ora ci proponiamo di dare alcune poche nozioni sulla teoria generale delle funzioni modulari, rimandando per uno studio effettivo dell' interessante argomento all'opera di Klein-Fricke: *Theorie der elliptischen Modulfunctionen*.

Definiamo le funzioni modulari (algebriche) nel modo seguente: *Ogni funzione algebrica $J(\tau)$ che, considerata come funzione di τ, sia uniforme dicesi una funzione modulare (algebrica).*

Oltre le funzioni modulari *algebriche*, si considerano anche delle funzioni modulari *trascendenti*; ma noi qui parleremo soltanto delle prime e le diremo senz'altro *funzioni modulari*.

Sia $\varphi = \varphi(\tau)$ una funzione modulare e sia

(1) $$f(\varphi, J) = 0,$$

dove f indica una funzione razionale intera nei due argomenti, l'equazione algebrica *irriducibile* che la lega all'invariante assoluto $J(\tau)$. Osserviamo in primo luogo che essendo, per un assegnato valore di τ, $\varphi(\tau)$ una radice della (1), tutte le altre radici saranno date dalle espressioni

(2) $$\varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right),$$

dove $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ è una qualunque sostituzione del gruppo modulare. Che tutte le espressioni (2) siano radici della (1) si vede subito osservando che se nel semipiano positivo tracciamo una linea continua, che vada da τ al punto equivalente $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$, l'invariante assoluto $J(\tau)$ descrive un cammino chiuso e $\varphi(\tau)$ si cangia con continuità in $\varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right)$. D'altronde *tutte* le radici della (1) sono date da espressioni (2) poichè, la (1) essendo per ipotesi irriducibile, se facciamo descrivere a J un conveniente cammino chiuso, passiamo da una radice $\varphi(\tau)$ ad un'altra qualunque; ora, come si è visto al § 121, possiamo far descrivere a $J(\tau)$ un cammino chiuso qualunque facendo muovere τ da τ ad un punto equivalente $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ per un conveniente cammino.

Supponiamo ora che la (1) sia di grado m rispetto alla φ e siano

$$\varphi_1, \varphi_2, \ldots, \varphi_m$$

le sue radici. Ogni valore (2) dovrà eguagliare uno di questi m, e siccome se le due sostituzioni

$$U = \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}, \quad U' = \begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix},$$

eseguite sull'argomento τ di $\varphi(\tau)$, danno eguali risultati

$$\varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \varphi\left(\frac{\alpha'\tau+\beta'}{\gamma'\tau+\delta'}\right),$$

la sostituzione $U'^{-1}U$ lascia $\varphi(\tau)$ invariata, si conclude: *Esistono nel gruppo modulare Γ infinite sostituzioni*

$$g_1 = 1, \; g_2, \; g_3, \ldots$$

che lasciano $\varphi(\tau)$ invariata; esse formano evidentemente in Γ un sottogruppo G. Diremo per ciò che la funzione modulare $\varphi(\tau)$ appartiene al sottogruppo G, od anche che G è il sottogruppo riproduttivo di $\varphi(\tau)$.

Di più se

$$t_1 = 1\,,\ t_2\,,\ t_3\,,\ \ldots,\ t_m$$

sono m particolari sostituzioni di Γ che cangiano $\varphi(\tau)$ in

$$\varphi_1 = \varphi(\tau)\,,\quad \varphi_2 = \varphi\left(\frac{\alpha_2\tau+\beta_2}{\gamma_2\tau+\delta_2}\right) \ldots\ \varphi_m = \varphi\left(\frac{\alpha_m\tau+\beta_m}{\gamma_m\tau+\delta_m}\right),$$

osservando che da $\varphi_\gamma = \varphi t_r$ segue che la $t_r^{-1}\gamma$ lascia invariata $\varphi(\tau)$ ed è perciò una g_i, cioè $\gamma = t_r g_i$, vediamo subito che qualunque sostituzione γ di Γ si potrà porre sotto la forma

$$\gamma = t_r g_i \begin{pmatrix} r = 1,\ 2,\ \ldots\ m \\ i = 1, 2, 3 \ldots \infty \end{pmatrix},$$

onde concludiamo: *Il sottogruppo G di Γ che lascia invariata la funzione modulare $\varphi(\tau)$ ha indice finito in Γ e precisamente eguale al grado m a cui φ comparisce nell'equazione* (1), *che la lega all'invariante assoluto.*

Dobbiamo subito osservare che mentre per l'eguaglianza

$$J(\tau) = J(\tau')$$

è *necessario* e *sufficiente* che τ, τ' siano equivalenti rispetto a Γ, per la eguaglianza

$$\varphi(\tau) = \varphi(\tau')$$

è bensì sufficiente, *ma non in generale necessario* che τ, τ' siano equivalenti rispetto al sottogruppo G, cui φ appartiene.

E invero, se la (1) è di grado n in J, per ogni valore assegnato di $\varphi(\tau)$ si hanno n valori distinti di $J(\tau)$ e se

$$\tau_1\,,\ \tau_2\,,\ \ldots,\ \tau_n$$

sono n corrispondenti valori di τ, fra questi non ve ne saranno due equivalenti rispetto a Γ, e tanto meno rispetto a G. Questo

numero n, che indica quante volte la funzione modulare $\varphi(\tau)$ riprende il medesimo valore in punti *non* equivalenti rispetto al sottogruppo riproduttivo G, si dirà la *valenza* di $\varphi(\tau)$. Se $n = 1$, allora $J(\tau)$ è funzione razionale di $\varphi(\tau)$ e questa è monovalente; tale è per esempio la funzione modulare $k^2(\tau)$.

Osserviamo ora che tutte le radici

$$\varphi_1\,,\ \varphi_2\,,\ \ldots,\ \varphi_m$$

della (1) sono, come è chiaro, altrettante funzioni modulari e se il sottogruppo riproduttivo della prima è G, quelli di $\varphi_2, \varphi_3, \ldots, \varphi_m$ saranno i rispettivi sottogruppi trasformati

$$G_2 = t_2 G t_2^{-1}\,,\quad G_3 = t_3 G t_3^{-1}\,,\ \ldots,\ G_m = t_m G t_m^{-1}$$ [1]).

In particolare si osservi che: *Se il sottogruppo riproduttivo G della funzione modulare $\varphi_1 = \varphi(\tau)$ è invariante in Γ, le altre funzioni modulari $\varphi_2(\tau), \ldots, \varphi_m(\tau)$, radici della* (1), *apparterranno al medesimo sottogruppo G.*

Dai teoremi generali sulle funzioni algebriche segue allora che ogni radice φ_r della (1) è razionalmente esprimibile per φ_1 e J, giacchè ad ogni coppia di valori φ_1, J corrisponde *un solo* valore di φ_r.

§ 175. — **Diramazione di una funzione modulare $\varphi(\tau)$ rispetto all'invariante assoluto $J(\tau)$.**

Fino ad ora abbiamo senz'altro supposto che l'equazione algebrica (1) sia tale che φ, considerata come funzione di τ, risulti *monodroma*. Vogliamo ora ricercare quali sono le condizioni necessarie e sufficienti cui deve soddisfare la (1) perchè ciò accada.

[1]) Pongasi invero

$$\varphi_r(\tau) = \varphi(\tau_r)\,,\quad \tau_r = \frac{\alpha_r\tau+\beta_r}{\gamma_r\tau+\delta_r}$$

e sia

$$\varphi(\tau_r) = \varphi_r(\tau) = \varphi_r(\tau') = \varphi(\tau'_r),\quad \tau'_r = \frac{\alpha_r\tau'+\beta_r}{\gamma_r\tau'+\delta_r}$$

sarà τ'_r legata a τ_r da una sostituzione g di G e però τ a τ' appunto da $t_r g t_r^{-1}$.

La risposta viene facilmente fornita dalle proprietà dell' invariante assoluto, stabilite al Cap. X (vedi particolarmente § 121), mediante le considerazioni seguenti. Supponiamo adunque che $\varphi(\tau)$ sia monodroma in τ e funzione algebrica di J definita dalla (1). Consideriamo un punto qualunque $J = J_1$ del piano complesso J, *diverso da uno dei tre valori* $0, 1, \infty$, che corrispondono ai vertici della rete modulare. Se facciamo descrivere a J un piccolo circuito chiuso attorno a J_1 e, scelto per valore di τ corrispondente al valore J_1 di J uno qualunque degli infiniti valori equivalenti corrispondenti, esaminiamo il corrispondente cammino descritto da τ, vediamo che sarà questo un cammino chiuso attorno a τ_1 e perciò gli m rami

$$\varphi_1, \varphi_2, \ldots, \varphi_m$$

della funzione algebrica φ, essendo per ipotesi monodromi in τ, ritorneranno ciascuno col proprio valore. Dunque :

I punti di diramazione della funzione modulare $\varphi(\tau)$, considerata come funzione algebrica di $J(\tau)$, si potranno presentare soltanto per i tre valori

$$J = 0, \quad J = 1, \quad J = \infty .$$

Esaminiamo ora quali specie di diramazione si avranno in questi punti. Per vederlo basta osservare che per un circuito chiuso descritto da J, che giri *tre* volte attorno a $J_1 = 0, \tau$ descrive un giro semplice attorno ad un vertice della rete modulare, equivalente al vertice $\varepsilon = e^{\frac{2\pi i}{3}}$, e similmente per un circuito chiuso di J, che giri *due* volte attorno a $J_1 = 1, \tau$ gira una volta attorno ad un vertice della rete, equivalente al vertice $i = e^{\frac{\pi i}{2}}$; onde vediamo: *Attorno a $J = 0$ quei rami della funzione algebrica φ che non corrono isolati si permutano ciclicamente tre a tre ; e similmente attorno a $J = 1$ ogni ramo, o corre isolato, o subisce una trasposizione con un altro ramo.*

Quanto alla diramazione in $J = \infty$, non occorre ulteriormente specificarla, poichè essa risulta già fissata dalle diramazioni attorno a $J = 0$, $J = 1$ [1]).

[1]) E infatti, avendosi i tre soli punti critici $J = 0$, $J = 1$, $J = \infty$, un giro attorno a $J = \infty$ equivale a un giro complessivo attorno ai due punti $J = 0$ $J = 1$.

Ora è bene importante che le condizioni, così trovate come necessarie, siano anche sufficienti, come viene precisato dalla proposizione seguente, che costituisce il così detto *teorema di diramazione* (Verzweigungssatz) di Klein :

Affinchè l'equazione algebrica irriducibile

$$f(\varphi, J) = 0 \tag{1}$$

definisca una funzione modulare $\varphi(\tau)$ è necessario e sufficiente che siano soddisfatte le condizioni seguenti :

1ª *la funzione algebrica φ di J sia diramata soltanto per* $J = 0, 1, \infty$;

2ª *per $J = 0$ i rami restino isolati, o si permutino ciclicamente tre a tre ;*

3ª *per $J = 1$ ogni ramo corra isolato, o si permuti per trasposizione con un altro.*

Che le condizioni siano necessarie si è già visto ; resta ora a dimostrarsi che sono sufficienti. Dobbiamo provare cioè che, soddisfatte queste condizioni, se per un particolare valore τ_1 di τ fissiamo uno dei rami φ_1 e lo continuiamo analiticamente, ne risulterà una funzione *monodroma* di τ :

$$\varphi_1 = \varphi(\tau).$$

Consideriamo nel semipiano positivo τ un cammino finito chiuso e privo di nodi s, che non passi per alcun vertice della rete modulare e racchiuda quindi un'area semplice finita, che conterrà nel suo interno un numero finito di vertici, e dimostriamo che per un tale cammino s le m determinazioni di φ :

$$\varphi_1, \varphi_2, \ldots, \varphi_m$$

ritornano ciascuna col valore iniziale. E infatti, per considerazioni analoghe a quelle del § 80, vediamo che se s producesse un'effettiva permutazione di $\varphi_1, \varphi_2, \ldots, \varphi_m$ potremmo decomporre l'area in due aree minori, inserendo una linea semplice interna, che eviti ancora il passaggio pei vertici, e l'uno o l'altro dei due contorni chiusi s_1, s_2 delle aree parziali dovrebbero produrre una permutazione di $\varphi_1, \varphi_2, ..., \varphi_m$. Così continuando, come al § 80, troveremmo contorni chiusi, piccoli a piacere, che permuterebbero $\varphi_1, \varphi_2, ..., \varphi_m$.

Ora ciò è impossibile perchè se un tale contorno non gira attorno ad un vertice della rete, J descrive un piccolo contorno chiuso, che non gira attorno nè a $J=0$ nè a $J=1$, e però $\varphi_1, \varphi_2, ..., \varphi_m$ singolarmente si riproducono. Ma, quando anche τ giri attorno ad un vertice della rete, J girerà attorno a $J=0$ o a $J=1$ tre o due volte rispettivamente e però, per le ipotesi fatte, $\varphi_1, \varphi_2, ..., \varphi_m$ riprenderanno con continuità i valori iniziali. Dopo ciò è evidente che per qualunque cammino chiuso descritto da τ, comunque intrecciato, $\varphi_1, \varphi_2, ..., \varphi_m$ si riproducono. Il teorema di diramazione è così dimostrato.

Ora i teoremi generali di esistenza delle funzioni algebriche, corrispondenti a superficie *Riemanniane* date *a priori*, permettono di asserire, che, assegnando ad arbitrio il modo di diramazione della funzione algebrica φ di J, tali funzioni esisteranno effettivamente, e, purchè siano soddisfatte le condizioni del teorema di diramazione, condurranno ad altrettante funzioni modulari.

I teoremi ora indicati ci permettono dunque di riconoscere l'esistenza di infiniti sottogruppi d'indice finito nel gruppo modulare e di costruirli effettivamente.

Per altro è da osservarsi che ogni equazione algebrica (1), soddisfacente alle condizioni del teorema di diramazione, definisce propriamente non un solo sottogruppo G del gruppo modulare Γ, ma insieme anche tutti i sottogruppi affini

$$G_1 = G\,,\quad G_2 = t_2\,G\,t_2^{-1},\ ...,\ G_m = t_m\,G\,t_m^{-1}.$$

§ 176. — Sottogruppi d'indice finito e loro poligono fondamentale.

Ogni funzione modulare appartiene, come si è visto, ad un sottogruppo G d'indice finito m del gruppo modulare Γ. Per dimostrare inversamente che per un sottogruppo G del gruppo modulare Γ, il cui indice in Γ sia finito, esistono funzioni modulari a gruppo riproduttivo G, occorre premettere alcune nozioni generali sui sottogruppi d'indice finito del gruppo modulare e sui loro campi fondamentali.

Sia dunque G un sottogruppo d'indice finito m in Γ e distribuiamo tutte le sostituzioni di Γ, rispetto al sottogruppo G, nel quadro:

$$a)\qquad \Gamma = \begin{cases} g_1\,,\ g_2\,,\ g_3\ .... \\ t_2 g_1\,,\ t_2 g_2\,,\ t_2 g_3\ .... \\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ . \\ t_m g_1\,,\ t_m g_2\,,\ t_m g_3\ ...\,; \end{cases}$$

coi medesimi simboli delle sostituzioni indicheremo i (doppî) triangoli della rete relativa al gruppo Γ, considerandoli come derivati, per es., dal triangolo fondamentale, che indicheremo col simbolo 1 [1]).

Due sostituzioni di Γ

$$\gamma\,,\ \gamma'\,,$$

o i due corrispondenti triangoli, si diranno *relativamente equivalenti*, od equivalenti rispetto al sottogruppo G, quando l'un triangolo deriva dall'altro con una sostituzione g_i di G, quando si abbia cioè

$$\gamma' = \gamma\, g_i\,,$$

sicchè due sostituzioni, o triangoli, saranno relativamente equivalenti o no, secondo che nel quadro $a)$ figurano nella medesima linea orizzontale, o in orizzontali diverse. Se prendiamo adunque da ciascuna orizzontale del quadro $a)$ un triangolo ad arbitrio, avremo un sistema di m triangoli

$$T_1\,,\ T_2\,,\ ...,\ T_m\,,$$

che si può dire un *sistema completo di triangoli non equivalenti*, giacchè qualunque altro triangolo della rete sarà equivalente ad uno e ad uno solo di questi.

Ora dimostriamo che possiamo scegliere i triangoli $T_1, T_2, ..., T_m$ in guisa che ciascuno sia aderente ad un altro almeno di essi per un lato e il loro insieme formi quindi un'area connessa. Per ciò prendiamo ad arbitrio un triangolo, per es., il fondamentale T',

[1]) Cfr. Cap. II, pag. 69.

e associamovi quei triangoli aderenti a T' che non sono relativamente equivalenti a T' nè fra loro; per ciascuno dei triangoli aggiunti si proceda nel medesimo modo, aggiungendo al complesso dei triangoli già prima ottenuti ogni nuovo triangolo aderente, quando non trovi il suo equivalente, rispetto a G, nei triangoli del complesso. Siccome fra $m+1$ triangoli presi ad arbitrio ve ne sono almeno due relativamente equivalenti, il processo descritto condurrà ad un insieme di un numero finito $r \leq m$ di triangoli aderenti

$$(3) \qquad T', \quad T'', \ldots, T^{(r)},$$

così costituito che ogni triangolo aderente ad uno di questi r triangoli trovi il suo equivalente, rispetto a G, in uno dei triangoli stessi. È ben facile ora vedere che si ha necessariamente $r=m$, onde risulta la verità della proposizione enunciata. E infatti osserviamo che se un triangolo qualunque U della rete è equivalente, rispetto a G, ad uno dei triangoli (3) per es. a $T^{(i)}$, anche un triangolo U', aderente ad U per un lato, sarà equivalente ad un triangolo in (3). In vero quella sostituzione g di G, che porta U in $T^{(i)}$, porterà U' in un triangolo aderente a $T^{(i)}$ e quindi relativamente equivalente ad uno della serie stessa (3). E siccome in fine possiamo passare da un triangolo qualsiasi V al fondamentale per una serie finita di triangoli successivamente aderenti, ne risulta appunto che V sarà relativamente equivalente ad un triangolo (3).

L' insieme di triangoli così scelti

$$T', \quad T'', \quad T''', \ldots, T^{(m)}$$

forma un poligono P, limitato da archi di circoli di riflessione del gruppo modulare, ed in questo poligono P riconosciamo il campo o *poligono fondamentale* del sottogruppo G; diciamo cioè che: *Ogni punto del semipiano positivo è equivalente, rispetto al sottogruppo G, ad un punto del poligono P, mentre due punti del poligono non sono fra loro relativamente equivalenti, fatta eccezione dai punti del contorno, che si ordinano in coppie di punti equivalenti.*

La prima cosa è subito evidente, poichè ogni punto del semipiano positivo appartiene ad un triangolo della rete, che è relativamente equivalente ad un triangolo di P. Supponiamo ora che

M, N siano due punti di P relativamente equivalenti; essi dovranno necessariamente trovarsi sul contorno di P. E infatti se per es. M fosse interno a P, sia che si trovasse sopra un lato interno o in un vertice della rete modulare, la sostituzione di G che porta M in N porterebbe un triangolo di P, contenente M, in un altro triangolo di P, ciò che è assurdo. Prendiamo invece un punto M sul contorno di P, cioè sopra un lato esterno l di P. Quel triangolo della rete che è aderente esternamente a P lungo l trova il suo equivalente in un triangolo $T^{(i)}$ di P ed è chiaro, per quanto precede, che il lato l' di $T^{(i)}$ equivalente a l sarà pure un lato esterno di P. Vediamo adunque che: *I lati esterni del poligono P si ordinano a coppie di lati coniugati, cioè relativamente equivalenti rispetto al sottogruppo G.*

Per ciò anche i punti del contorno di P si ordinano a coppie di punti equivalenti, e si vede subito che ogni punto del contorno ne ammette così uno ed uno solo relativamente equivalente sul contorno stesso.

Osserviamo però che, nell'ordinamento dei lati del poligono fondamentale in coppie di lati coniugati, può darsi benissimo che un lato l risulti coniugato a sè stesso, il che significa allora che il triangolo di P, che ha l per lato, è relativamente equivalente a quello aderente lungo l esternamente. In tal caso, la sostituzione di G che cangia l in sè stesso è ellittica a periodo 2 ed ha su l un punto fisso, che divide l in due tratti coniugati; allora riguardiamo l come costituito di due lati per diritto e il detto punto fisso come nuovo vertice, a cui corrisponde un angolo piatto. In generale è da osservarsi che se un punto P percorre un lato l del contorno in verso positivo, l'equivalente P' percorre il lato coniugato nel senso opposto.

Applicando al poligono fondamentale P di G tutte le sostituzioni di G stesso otteniamo una rete di poligoni, come P, che ricopre una ed una sola volta tutto il semipiano positivo, come risulta da quanto sopra abbiamo dimostrato. Ora se consideriamo le μ coppie di lati coniugati di P e le μ sostituzioni di G

$$(4) \qquad g_1, \quad g_2, \ldots, g_\mu,$$

che portano un lato nel coniugato, insieme alle loro inverse

$$g_1^{-1}, \, g_2^{-1}, \ldots, g_\mu^{-1},$$

facilmente vediamo che: *L' intero sottogruppo si genera combinando le μ sostituzioni* (4) *e le loro potenze.* E invero le μ sostituzioni (4) e le loro inverse bastano già a trasportare P in tutti i poligoni aderenti della rete ora considerata e d'altra parte si può passare dal poligono fondamentale P ad uno qualunque della rete per una successione di poligoni l'uno all'altro aderenti. (Cfr. Cap. II).

§ 177. — Esistenza di funzioni modulari appartenenti ad un dato sottogruppo.

Immaginiamo ora di tagliare dal semipiano positivo l'area poligonale P ed, assoggettando quest'area ad una deformazione continua [1]) nello spazio, di saldare insieme i lati coniugati sì che ciascuna coppia di punti equivalenti dia luogo ad un unico punto. Ne risulterà una superficie chiusa R tale che, supponendo dapprima l'esistenza della corrispondente funzione modulare $\varphi(\tau)$, ad ogni punto della superficie corrisponderà una ed una sola coppia di valori φ, J per la funzione modulare φ e l' invariante assoluto J, e viceversa ad ogni coppia di valori φ, J soddisfacente all'equazione (1) $f(\varphi, J) = 0$ uno ed un solo punto della superficie R. La prima cosa è evidente, per la monodromia di $\varphi(\tau)$, $J(\tau)$; la seconda poi risulta da ciò che, se si ha simultaneamente

$$J(\tau) = J(\tau_1), \quad \varphi(\tau) = \varphi(\tau_1),$$

i valori τ, τ_1 sono legati da una sostituzione del sottogruppo G cioè sono relativamente equivalenti, e per ciò i due punti supposti su R necessariamente coincidono.

Secondo quanto abbiamo detto al § 83, la superficie chiusa R non è altro che la superficie Riemanniana per l'equazione algebrica

$$f(\varphi, J) = 0;$$

soltanto gli m fogli, che nell'ordinaria rappresentazione sono collocati l' uno sull' altro, qui si trovano l' uno accanto all'altro e sono rappresentati dagli m triangoli di P, in ciascuno dei quali $J(\tau)$ ripete appunto tutti i suoi valori.

[1]) Come nella teoria della connessione si riguarda l'area come formata da un velo perfettamente flessibile ed estendibile, che può traversare liberamente sè stesso.

Il genere p della superficie Riemanniana si valuta subito, applicando la nota formola d' Eulero generalizzata, citata al § 92 (pag. 271, vol. I):

$$F + V = C + 2 - 2p.$$

Da queste considerazioni e dai teoremi d'esistenza delle funzioni algebriche, corrispondenti a superficie Riemanniane date *a priori*, si può ora dedurre l' importante teorema: *Dato ad arbitrio un sottogruppo di indice finito m del gruppo modulare Γ, esistono sempre funzioni modulari appartenenti al sottogruppo G.*

E infatti costruiamo il poligono fondamentale P di G e, nel modo descritto al principio del presente paragrafo, conformiamolo a superficie chiusa R. Sopra ciascuno degli m triangoli in cui R è diviso sono distesi una volta i valori di $J(\tau)$ e possiamo riguardare R come una superficie Riemanniana a m fogli. Soltanto attorno ai vertici, ove per J si hanno i valori

$$J = 0, \quad J = 1, \quad J = \infty,$$

avviene scambio dei fogli e, come subito si vede, il modo dello scambio corrisponde appunto alle condizioni del teorema di diramazione. Se ora prendiamo una funzione algebrica φ di J appartenente alla superficie Riemanniana R, della cui esistenza ci assicurano i teoremi generali, essa, considerata come funzione di τ, sarà monodroma come c' insegna il teorema di diramazione, cioè sarà una funzione modulare. Per dimostrare poi che la $\varphi(\tau)$ rimarrà invariata per tutte le sostituzioni di G basterà provare la cosa per le μ sostituzioni (4) generatrici di G. Sia $\begin{pmatrix} a, b \\ c, d \end{pmatrix}$ una tale sostituzione, che cangia dunque un lato l di P nel lato coniugato l'. Le due funzioni

$$\varphi(\tau), \quad \varphi\left(\frac{a\tau + b}{c\tau + d}\right)$$

coincidono lungo l perchè, mentre τ percorre l, $\dfrac{a\tau+b}{c\tau+d}$ percorre l' e in punti corrispondenti di l, l' (che sulla superficie chiusa R coincidono in un medesimo punto) la φ ha il medesimo valore, onde si conclude che è sempre $\varphi\left(\dfrac{a\tau+b}{c\tau+d}\right) = \varphi(\tau)$.

In fine per essere certi che nessun'altra sostituzione di Γ, oltre quelle di G, lascia φ invariata, cioè che $\varphi(\tau)$ appartiene realmente al sottogruppo G e non ad un sottogruppo più ampio, basterà scegliere la funzione algebrica φ di J in guisa che pel medesimo valore generico di J la φ assuma m valori distinti, ciò che è sempre possibile.

§ 178. — Il poligono fondamentale del sottogruppo $G \equiv \begin{pmatrix}1,0\\0,1\end{pmatrix}$ (mod 2).

Limitandoci ai principî fondamentali, esposti nei paragrafi precedenti, per quanto riguarda la teoria generale delle funzioni modulari, tratteremo ora di alcune poche funzioni modulari, che furono le prime studiate e diedero il nome all' intera classe. E in primo luogo riprenderemo lo studio della funzione modulare $k^2(\tau)$ (§ 135), appartenente al sottogruppo

$$G \equiv \begin{pmatrix}1,0\\0,1\end{pmatrix} \pmod 2,$$

e legata all' invariante assoluto $J(\tau)$ dalla relazione

$$J = \frac{4}{27}\,\frac{(1-k^2+k^4)^3}{k^4(1-k^2)^2}, \tag{5}$$

per determinarne il poligono fondamentale, che consisterà di 6 triangoli della rete del gruppo modulare Γ. Potremmo a questo oggetto applicare il processo generale descritto al § 176, ma preferiamo procedere, come già al Cap. II per lo studio del gruppo modulare, ampliando il gruppo G colla riflessione $z' = -z_0$ e considerando quindi il gruppo ampliato G_0, composto delle sostituzioni di prima e seconda specie della forma

$$\begin{cases} z' = \dfrac{\alpha z+\beta}{\gamma z+\delta}, & \begin{pmatrix}\alpha,\beta\\ \gamma,\delta\end{pmatrix} \equiv \begin{pmatrix}1,0\\0,1\end{pmatrix} \pmod 2 \\[2mm] z' = \dfrac{\alpha z_0-\beta}{\gamma z_0-\delta}\,. \end{cases}$$

Le riflessioni contenute nel sottogruppo G_0 hanno la forma

$$z' = \frac{\alpha z_0-\beta}{\gamma z_0-\alpha}, \quad \alpha^2-\beta\gamma = 1$$

con $\alpha \equiv 1$, $\beta \equiv \gamma \equiv 0 \pmod 2$ e perciò le rette e i circoli di riflessione saranno dati dalle equazioni (cfr. § 18) :

$$x = n, \quad \left(x-\frac{\alpha}{\gamma}\right)^2 + y^2 = \frac{1}{\gamma^2},$$

dove n è un intero qualunque e si ha $\gamma \equiv 0 \pmod 2$ con $\alpha^2 \equiv 1 \pmod\gamma$. Consideriamo il triangolo T del semipiano positivo, limitato entro la striscia compresa fra le due rette successive di riflessione

$$x = 0, \quad x = -1,$$

esternamente al circolo di riflessione

$$\left(x-\frac{1}{2}\right)^2 + y^2 = \left(\frac{1}{2}\right)^2 \text{ (vedi fig. 13).}$$

Questo triangolo T, coi tre angoli nulli, non è attraversato da alcun altro circolo o retta di riflessione di G_0 e rappresenta il triangolo fondamentale del gruppo G_0, come si dimostra con considerazioni del tutto simili a quelle dei §§ 18 e 19. Ogni punto del semipiano positivo è equivalente, rispetto a G_0, ad uno e *ad un solo* punto di T ; l' ultima cosa risultando da ciò che nessuna sostituzione di G_0 trasforma T in sè medesimo. E infatti cerchiamo in generale le sostituzioni di prima e seconda specie che lasciano fisso T, senza nemmeno esigere che appartengano al gruppo modulare. In primo luogo troviamo fra queste la sostituzione ellittica a periodo 3

$$U)\ z' = -\frac{1}{z+1},$$

che produce sui vertici $0, -1, \infty$ di T la permutazione ciclica $(0, -1, \infty)$, e il suo quadrato $U^2)\ z' = -\dfrac{z+1}{z}$ che produce la permutazione $(0, \infty, -1)$. Nessun'altra sostituzione di prima specie può lasciar fisso T, perchè dovrebbe lasciar fisso uno dei tre vertici e permutare gli altri due e componendola con U o con U^2

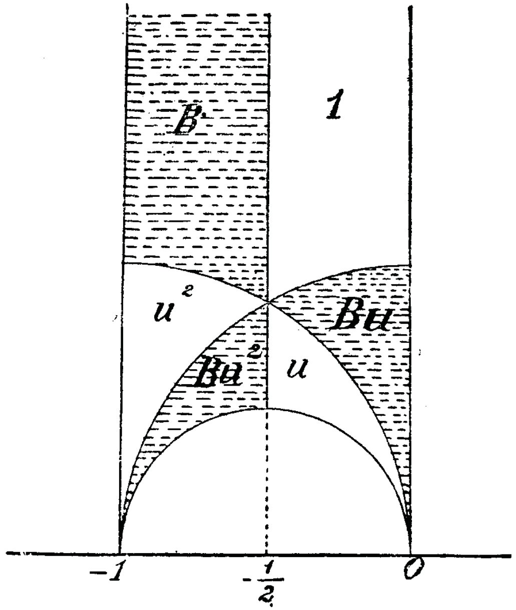

Fig. 13.

si avrebbe una sostituzione che lascerebbe fisso ∞ e permuterebbe $(0, -1)$. Ora una tale sostituzione esiste effettivamente ed è

$$z' = -(z+1);$$

ma, essendo a determinante -1, scambia i due semipiani e, invece di lasciar fisso T, lo cangia nel suo simmetrico rispetto all'asse reale. Così adunque di sostituzioni di prima specie che lascino fisso T vi sono solo le tre

$$1, \quad U, \quad U^2,$$

appartenenti al gruppo modulare Γ. Vi ha poi anche la riflessione B

$$B) \; z' = -z_0 - 1$$

che lascia fisso T, e quindi le tre di seconda specie

$$B, \quad BU, \quad BU^2;$$

nè ve ne possono essere altre. Tutte sei queste sostituzioni appartengono al gruppo modulare ampliato Γ, ma non a G_0, onde segue quanto sopra è asserito [1]). Nella figura 13 sono rappresentati i 6 triangoli della rete modulare in cui T si decompone; i nomi di questi 6 triangoli sono appunto quelli

$$1, \quad U, \quad U^2, \quad B, \quad BU, \quad BU^2$$

delle 6 sostituzioni di Γ_0, che costituiscono il gruppo riproduttivo di T.

Volendo ora ottenere il poligono fondamentale del gruppo $G \equiv \begin{pmatrix}1, 0\\0, 1\end{pmatrix}$ (mod 2), basterà associare al triangolo T il suo simmetrico rispetto all'asse immaginario e nel quadrilatero così formato, racchiuso dalle due rette $x = \pm 1$ all'esterno dei due circoli

$$\left(x \pm \frac{1}{2}\right)^2 + y^2 = \frac{1}{4},$$

avremo appunto il poligono fondamentale di G (vedi fig. 14). Ogni punto del semipiano positivo è equivalente, rispetto al sottogruppo G, ad un punto e ad un solo di questo poligono P, a meno che il punto non trovisi sul contorno, nel qual caso esso è equivalente al punto del contorno, simmetrico rispetto all'asse immaginario (cfr. § 21). I lati del quadrilatero P sono due a due coniugati, i rettilinei fra loro, i circolari fra loro; le rispettive sostituzioni di G, che cangiano l'uno nell'altro i lati coniugati, sono

$$\begin{pmatrix}1, \pm 2\\0, \;\; 1\end{pmatrix}, \quad \begin{pmatrix}1 & 0\\\pm 2, & 1\end{pmatrix}.$$

Se ne conclude (§ 176): *Il sottogruppo G del gruppo modulare Γ, definito dalla congruenza* $\begin{pmatrix}\alpha, \beta\\\gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\0, 1\end{pmatrix}$ (mod 2), *si genera mediante le due sostituzioni elementari (paraboliche)*:

$$\begin{pmatrix}1, 2\\0, 1\end{pmatrix}, \quad \begin{pmatrix}1, 0\\2, 1\end{pmatrix}\text{ [2]}.$$

[1]) Risulta di più: *Il gruppo modulare Γ_0 è il più ampio, nel quale G_0 sia contenuto come sottogruppo invariante.*

[2]) Si osservi che il sottogruppo G contiene soltanto sostituzioni paraboliche ed iperboliche, ma nessuna ellittica.

Se, conformemente a quanto si è detto nel paragrafo precedente, si saldano insieme i lati coniugati di P, si ha una superficie

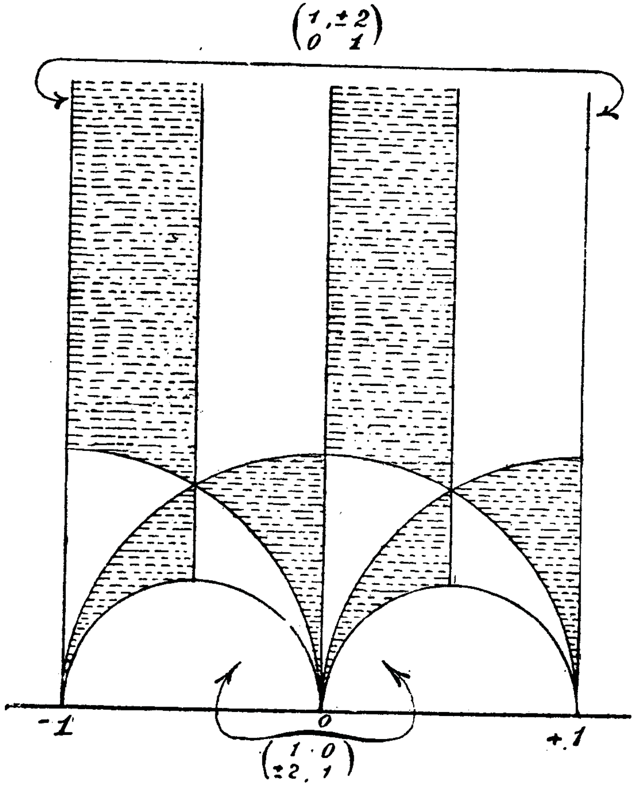

Fig. 14.

Riemanniana (di genere zero) a 6 fogli che si diramano in $J = 0$ tre a tre, in $J = 1$ due a due e medesimamente in $J = \infty$. Essa è la superficie di Riemann per l'equazione algebrica (5).

§ 179. — **Distribuzione dei valori di $k^2(\tau)$ nel suo poligono fondamentale.**

Esaminiamo ora la distribuzione dei valori di $k^2(\tau)$ nel suo poligono fondamentale. Dalle espressioni analitiche per prodotti infiniti e per serie, date al Cap. XIII, in particolare ad es. dalle (IV),

pag. 164, e dalle (XVI), pag. 180, risulta che $k^2(\tau)$ è reale su tutto l'asse immaginario e quindi in punti simmetrici rispetto all'asse immaginario (come pure in punti simmetrici rispetto ad ogni circolo di riflessione di G_0) assume valori coniugati. Basterà dunque esaminarne l'andamento sul contorno del triangolo fondamentale di G_0, ove $k^2(\tau)$ sarà sempre reale e non potrà passare due volte pel medesimo valore. All' infinito sull'asse immaginario $q = e^{\pi i \tau}$ si annulla e perciò anche $k^2(i\infty) = 0$. In virtù della formola (pag. 118).

$$k^2\left(-\frac{1}{\tau}\right) = 1 - k^2(\tau),$$

si ha

$$k^2(i) = \frac{1}{2}, \quad k^2(0) = 1,$$

sicchè sull'asse immaginario da ∞ a 0 $k^2(\tau)$ va sempre crescendo per valori reali da 0 a 1. Ora la sostituzione

$$U) \quad \tau' = -\frac{1}{\tau + 1}$$

cangia l'asse immaginario nel lato semi-circolare

$$\left(x + \frac{1}{2}\right)^2 + y^2 = \frac{1}{4},$$

sul quale, movendo τ da 0 a -1, $k^2(\tau)$, a causa della formola (pag. 118)

$$k^2\left(\frac{-1}{\tau + 1}\right) = \frac{1}{1 - k^2(\tau)},$$

andrà crescendo da 1 a ∞. In fine se si osserva che la sostituzione

$$U^2) \quad \tau' = -\frac{\tau + 1}{\tau},$$

cangia l'asse immaginario nel lato rettilineo $x = -1$ e d'altronde si ha

$$k^2\left(-\frac{\tau + 1}{\tau}\right) = \frac{k^2(\tau) - 1}{k^2(\tau)},$$

si vede che sul lato $x = -1$, $k^2(\tau)$ va crescendo per valori negativi da $-\infty$ a 0 (vedi fig. 15). In tutto l' interno del triangolo fondamentale T di G_0 il coefficiente dell' immaginario in $k^2(\tau)$ serba sempre lo stesso segno (perchè ivi $k^2(\tau)$ non è mai reale), e poichè nel triangolo simmetrico rispetto all' asse immaginario prende i valori coniugati e d'altronde nel quadrilatero fonda-

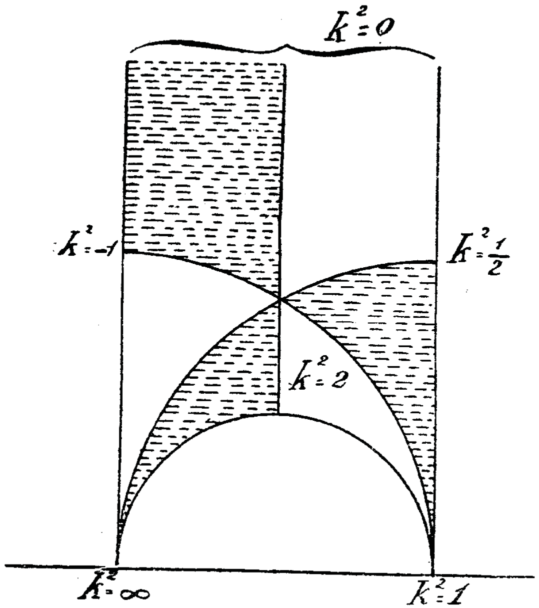

Fig. 15.

mentale di G assume (una volta) ogni possibile valore [1]), ne risulta che nell' interno di T $k^2(\tau)$ prenderà una ed una sola volta tutti i valori col coefficiente dell' immaginario di un medesimo segno, che si riconosce subito essere il negativo dall'andamento di $k^2(\tau)$ sul contorno.

Se distendiamo i valori di $k^2(\tau)$ nel suo piano complesso, abbiamo il risultato: *La funzione modulare $k^2(\tau)$ dà la rappresentazione biunivoca conforme del triangolo fondamentale di G_0 sul semipiano negativo.*

[1]) Basta osservare che $k^2(\tau)$ è legato a $J(\tau)$ dalla (5) e ricordare quanto si dimostrò al § 120 riguardo all' invariante assoluto.

§ 180. — La funzione $k^2(\tau)$ come uniformizzante.

Osserviamo che nel semipiano positivo, a distanza finita, $k^2(\tau)$ non prende mai uno dei tre valori

$$0, \quad 1, \quad \infty,$$

valori che assume soltanto, o meglio verso i quali converge, andando ai punti limiti del campo, che sono il punto $\tau = \infty$ e i punti razionali dell'asse reale. E siccome con una sostituzione

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}, \quad \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} \equiv \begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix} \pmod 2$$

del gruppo G riproduttivo di $k^2(\tau)$ si passa da $\tau = \infty$ a tutti i punti razionali dell'asse reale della forma $\dfrac{\alpha}{\gamma}$ con $(\alpha, \gamma) \equiv (1, 0)$ (mod 2), dal punto $\tau = 0$ a tutti i punti $\dfrac{\beta}{\delta}$ con $(\beta, \delta) \equiv (0, 1)$ (mod 2) e infine da $\tau = -1$ a tutti i punti $\dfrac{\beta - \alpha}{\delta - \gamma} = \dfrac{r}{s}$ con $(r, s) \equiv (1, 1)$ (mod 2) ne concludiamo:

La funzione modulare $k^2(\tau)$ assume i valori $0, 1, \infty$ (o meglio converge verso di essi) soltanto all' infinito e nei punti razionali $\dfrac{r}{s}$ dell'asse reale con r, s interi primi fra loro e precisamente converge verso i valori $0, 1, \infty$ secondo che

$$(r, s) \equiv (1, 0), \equiv (0, 1), \equiv (1, 1) \pmod 2.$$

Questa proprietà della funzione modulare $k^2(\tau)$, di *non* prendere i valori

$$k^2 = 0, \quad 1, \quad \infty,$$

dà luogo ad un' importante applicazione, che vogliamo ora accennare. Sia

$$w = F(z)$$

una funzione analitica di z comunque polidroma, ma così costituita che soltanto girando attorno ad uno dei tre punti

$$z = 0, \quad 1, \quad \infty,$$

avvenga scambio dei rami, che sia cioè diramata soltanto in $z = 0, 1, \infty$ e quivi del resto in modo affatto arbitrario. Se poniamo $z = k^2(\tau)$, e riguardiamo $w = F(z)$ come funzione di τ, diciamo $w = \varphi(\tau)$, basterà fissare per un valore iniziale τ_0 di τ la scelta fra uno dei valori di $F(k^2(\tau_0))$ per avere completamente fissata la funzione analitica $w = \varphi(\tau)$. Ora diciamo che *essa è in ogni caso una funzione monodroma di* τ. Per vederlo basta ripetere le considerazioni fatte al § 175, a proposito del teorema di diramazione, e ricordare che per un cammino chiuso descritto da τ la $z = k^2(\tau)$ non può girare attorno a $z = 0, 1, \infty$.

Questo risultato si esprime anche dicendo che per la relazione funzionale $w = F(z)$, ove la w si diRami, in modo del resto arbitrario, attorno a $z = 0, 1, \infty$ soltanto, la variabile ausiliaria τ è una variabile *uniformizzante*, cioè tale che per essa si esprimono ad un tempo la variabile indipendente $z = k^2(\tau)$ e la funzione $w = \varphi(\tau)$ quali funzioni uniformi. Suppongasi in particolare che la w sia funzione algebrica di z, e diramata soltanto nei punti $z = 0, 1, \infty$; applicando il teorema generale precedente ed osservando che in tal caso, essendo w legata algebricamente a $k^2(\tau)$, lo è anche all' invariante assoluto $J(\tau)$, otteniamo il teorema:

Qualunque funzione algebrica di $k^2(\tau)$, *che sia diramata soltanto per*

$$k^2 = 0, \quad k^2 = 1, \quad k^2 = \infty,$$

e quivi del resto in modo affatto arbitrario, è una funzione modulare algebrica di τ.

§ 181. — Le funzioni modulari $\sqrt[n]{k^2(\tau)}$, $\sqrt[n]{1-k^2(\tau)}$.

Da quanto abbiamo ora detto risulta in particolare che, indicando con n un numero intero positivo qualunque, le funzioni

$$\sqrt[n]{k^2(\tau)}, \quad \sqrt[n]{1-k^2} = \sqrt[n]{k'^2}$$

sono funzioni modulari; le fisseremo perfettamente convenendo di prendere per $\tau = i$ il valore aritmetico del radicale $\dfrac{1}{\sqrt[n]{2}}$.

I poligoni fondamentali delle funzioni modulari

$$\Phi(\tau) = \sqrt[n]{k^2(\tau)}, \quad \Psi(\tau) = \sqrt[n]{k'^2(\tau)},$$

che constano di $6n$ triangoli del gruppo modulare Γ, sono facili a determinarsi. Basta per ciò considerare che la superficie Riemanniana, corrispondente ad es. alla prima equazione algebrica

$$\Phi^n = k^2,$$

consta di n fogli sopra ognuno dei quali sono distesi una volta i valori di k^2 ed ha i due punti di diramazione $k^2 = 0$, $k^2 = \infty$, ove gli n fogli si riuniscono in un ciclo. Ora se consideriamo il poligono fondamentale di k^2, che consta di due successivi triangoli di G_0 (§ 178) e rappresenta un foglio della superficie Riemanniana, basterà prendere n successivi di questi poligoni derivati dal fondamentale colla ripetuta applicazione della traslazione $S^2 = \begin{pmatrix} 1, 2 \\ 0, 1 \end{pmatrix}$ e saldare quindi i due lati rettilinei estremi mediante la sostituzione S^{2n} e i circolari nel modo indicato dalle frecce nella figura (vedi fig. 16), ove è rappresentato il caso $n = 3$ [1]). Effettivamente, con questa corrispondenza dei lati, si vede subito che in $k^2 = 0$, $k^2 = \infty$ i tre fogli sono riuniti ciclicamente, laddove per $k^2 = 1$ non vi ha diramazione.

Calcoliamo subito le $n + 1$ sostituzioni generatrici del sottogruppo di $\Phi(\tau)$. Una di esse sarà la $S^{2n} = \begin{pmatrix} 1, 2n \\ 0, 1 \end{pmatrix}$ che congiunge i lati rettilinei e un'altra la sostituzione

$$U = \begin{pmatrix} 4n-1, & -2n \\ 2 \quad , & -1 \end{pmatrix},$$

che congiunge i lati estremi circolari. Quanto alle intermedie $n - 1$, esse debbono trasformare il lato circolare cogli estremi nei due punti $2r - 1$, $2r$ nel contiguo cogli estremi $2r + 1$, $2r$ (per $r = 1, 2, 3, \ldots, n - 1$). Una tale sostituzione si compone della riflessione sulla retta $x = 2r$ e della riflessione sull' ultimo circolo, e si trova quindi per la sua espressione

$$\begin{pmatrix} 4r+1, & -8r^2 \\ 2 \quad , & -(4r-1) \end{pmatrix} \quad \left[(r = 1, 2, 3, \ldots, n-1)\right].$$

[1]) È da notarsi che tutti questi lati circolari sono fra loro equivalenti non solo rispetto a G_0 ma anche rispetto a G, e per ciò le sostituzioni che congiungono i lati appartengono al gruppo $G \equiv \begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix}$ (mod 2), come è confermato dai calcoli del testo.

Concludiamo adunque che: *Le sostituzioni generatrici del sottogruppo riproduttivo della funzione modulare*

$$\Phi(\tau) = \sqrt[n]{k^2(\tau)}$$

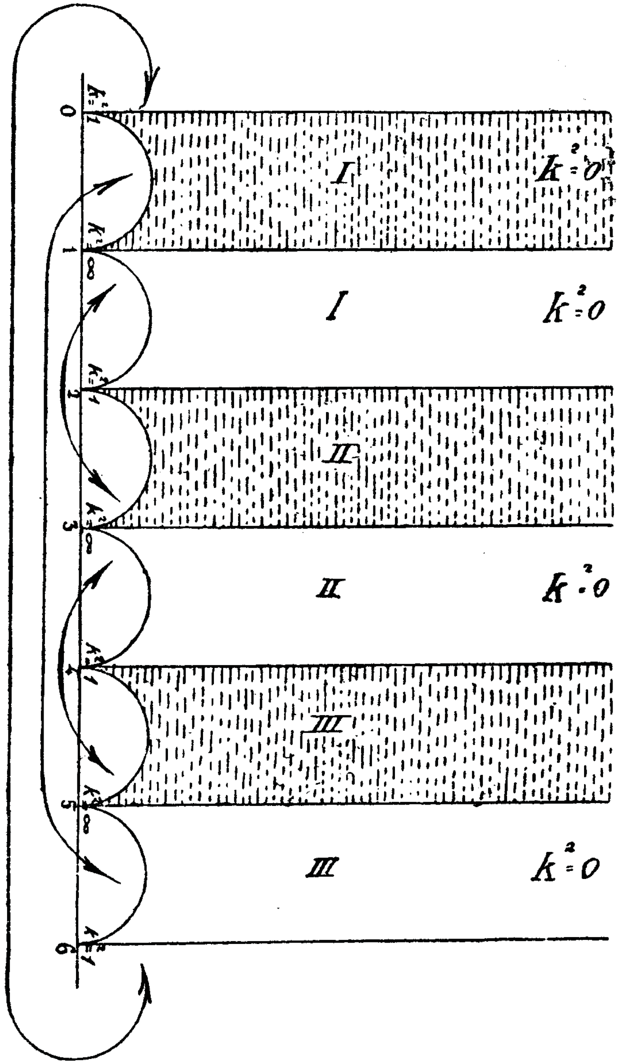

Fig. 16.

sono le $n+1$ sostituzioni seguenti

$$S^{2n} = \begin{pmatrix} 1, & 2n \\ 0, & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 4n-1, & -2n \\ 2\ \ , & -1 \end{pmatrix},$$

$$U_r = \begin{pmatrix} 4r+1, & -8r^2 \\ 2\ \ , & -(4r-1) \end{pmatrix} \ (r = 1, 2, \ldots, n-1).$$

Analogamente si determinerebbero le $n+1$ sostituzioni generatrici del gruppo riproduttivo di

$$\Psi(\tau) = \sqrt[n]{k'^2(\tau)}\,.$$

Ma del resto basta osservare che si ha

$$k'^2(\tau) = k^2\left(-\frac{1}{\tau}\right),$$

per vedere che si otterranno le sostituzioni domandate trasformando le precedenti per mezzo della

$$T = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}.$$

Potremmo ora domandarci come si possono definire *aritmeticamente* le sostituzioni di questi gruppi riproduttivi di $\Phi(\tau)$, $\Psi(\tau)$, di cui conosciamo le sostituzioni generatrici. Ma nello stato attuale della teoria vi è una sola specie di sottogruppi del gruppo modulare che siamo in grado di definire aritmeticamente e questi sono i sottogruppi *congruenziali*, le cui sostituzioni sono perfettamente caratterizzate da congruenze cui debbono soddisfare i coefficienti (cfr. § 128). Ora i gruppi superiori non sono mai gruppi congruenziali, salvo i casi

$$n = 8, \quad 4, \quad 2,$$

come si può vedere dimostrato nell'opera di Klein-Fricke [1]). Ci limiteremo pertanto allo studio delle funzioni modulari

$$\sqrt[4]{k}, \quad \sqrt[4]{k'},$$

[1]) Bd. I, pag. 659 sgg.

che, colle loro potenze seconda e quarta sono, come si è detto, le uniche radici di $k^2(\tau)$, $k'^2(\tau)$ appartenenti a sottogruppi congruenziali.

Queste furono in effetto le prime funzioni modulari studiate; e noi vogliamo ora caratterizzarne perfettamente il sottogruppo riproduttivo con congruenze (mod 16), secondo le formole che Hermite per primo fece conoscere.

§ 182. — Le funzioni modulari $\varphi(\tau)=\sqrt[4]{k}$, $\psi(\tau)=\sqrt[4]{k'}$.

Poniamo con Hermite

$$\varphi(\tau)=\sqrt[4]{k}\,,\quad \psi(\tau)=\sqrt[4]{k'}$$

e precisiamo il valore che prenderemo per la radice quarta, ricorrendo alle formole (IV), pag. 164, con che avremo:

$$(6)\qquad \begin{cases} \varphi(\tau)=\sqrt{2}\,e^{\frac{\pi i \tau}{8}} \displaystyle\prod_{n=1}^{n=\infty} \frac{1+e^{2n\pi i\tau}}{1+e^{(2n-1)\pi i\tau}} \\ \psi(\tau) \quad = \quad \displaystyle\prod_{1}^{\infty} \frac{1-e^{(2n-1)\pi i\tau}}{1+e^{(2n-1)\pi i\tau}}. \end{cases}$$

Ricerchiamo l'effetto che una sostituzione qualunque $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ del gruppo modulare Γ produce su $\varphi(\tau)$, $\psi(\tau)$, per il che già basterebbe conoscere quello delle sostituzioni elementari

$$\begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix},\quad \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}.$$

Intanto dalle espressioni analitiche (6), indicando con r un intero qualunque, deduciamo immediatamente le formole:

$$(7)\begin{cases} \varphi(\tau+2r)=e^{\frac{\pi i r}{4}}\varphi(\tau) \\ \psi(\tau+2r)=\psi(\tau) \end{cases}\qquad (7^*)\begin{cases} \varphi(\tau+2r+1)=e^{\frac{(2r+1)\pi i}{8}}\cdot\dfrac{\varphi(\tau)}{\psi(\tau)} \\ \psi(\tau+2r+1)=\dfrac{1}{\psi(\tau)}, \end{cases}$$

che dànno in particolare l'effetto prodotto da $\begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}$.

D'altronde avendosi

$$k^2\left(-\frac{1}{\tau}\right)=k'^2(\tau)\,,\quad k'^2\left(-\frac{1}{\tau}\right)=k^2(\tau)\,,$$

cioè

$$\varphi^8\left(-\frac{1}{\tau}\right)=\psi^8(\tau),\quad \psi^8\left(-\frac{1}{\tau}\right)=\varphi^8(\tau)\,,$$

risulta che

$$\varphi\left(-\frac{1}{\tau}\right),\quad \psi\left(-\frac{1}{\tau}\right)$$

non possono differire da $\psi(\tau)$, $\varphi(\tau)$ rispettivamente che per radici ottave dell'unità. Ma, per τ puramente immaginario, $\varphi(\tau)$, $\psi(\tau)$ sono reali e positive, e perciò abbiamo senz'altro le formole

$$(8)\qquad \varphi\left(-\frac{1}{\tau}\right)=\psi(\tau)\,,\quad \psi\left(-\frac{1}{\tau}\right)=\varphi(\tau).$$

Ciò premesso, possiamo stabilire le formole generali richieste distinguendo le sostituzioni $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ del gruppo modulare Γ nelle solite 6 classi rispetto al sottogruppo $G=\begin{pmatrix}1, 0\\ 0, 1\end{pmatrix}$ (mod 2). Consideriamo dapprima una sostituzione $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$ di G, supponiamo cioè $\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}\equiv\begin{pmatrix}1, 0\\ 0, 1\end{pmatrix}$ (mod 2); dico che sussisterà la formola:

$$(9)\qquad \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right)=e^{\frac{\pi i}{8}(\alpha^2+\alpha\beta-1)}\varphi(\tau)\quad \left(\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}\equiv\begin{pmatrix}1, 0\\ 0, 1\end{pmatrix} \atop \text{(mod 2)}\right)$$

Per dimostrare questa formola, osserviamo che essa sussiste per le due sostituzioni generatrici di G (§ 178)

$$\begin{pmatrix}1, \pm 2\\ 0, \ \ 1\end{pmatrix},\quad \begin{pmatrix}1, 0\\ \pm 2, 1\end{pmatrix},$$

cioè si ha

$$\varphi(\tau\pm 2)=e^{\pm\frac{\pi i}{4}}\varphi(\tau).\quad \varphi\left(\frac{\tau}{\pm 2\tau+1}\right)=\varphi(\tau)\,,$$

poichè la prima è un caso particolare delle (7) e la seconda risulta dalle (7), (8), osservando che si ha

$$\begin{pmatrix}1, & 0\\ \pm 2, & 1\end{pmatrix} = \begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}\begin{pmatrix}1, & \mp 2\\ 0, & 1\end{pmatrix}\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$$

Per dimostrare che la (9) sussiste in generale basterà dunque provare che, supposta vera per la sostituzione $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, essa sussiste anche per le due sostituzioni

$$\begin{pmatrix}\alpha_1, & \beta_1\\ \gamma_1, & \delta_1\end{pmatrix} = \begin{pmatrix}1, & 0\\ \pm 2, & 1\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}\alpha \pm 2\beta, & \beta\\ \gamma \pm 2\delta, & \delta\end{pmatrix}$$

$$\begin{pmatrix}\alpha_2, & \beta_2\\ \gamma_2, & \delta_2\end{pmatrix} = \begin{pmatrix}1, & \pm 2\\ 0, & 1\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}\alpha, & \pm 2\alpha + \beta\\ \gamma, & \pm 2\gamma + \delta\end{pmatrix}.$$

Ma si ha per ipotesi

$$\varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\alpha\beta+\alpha^2-1)}\varphi(\tau)$$

e quindi

$$\varphi\left(\frac{\alpha_1\tau+\beta_1}{\gamma_1\tau+\delta_1}\right) = e^{\frac{\pi i}{8}(\alpha\beta+\alpha^2-1)}\varphi\left(\frac{\tau}{\pm 2\tau+1}\right) = e^{\frac{\pi i}{8}(\alpha\beta+\alpha^2-1)}\varphi(\tau)$$

$$\varphi\left(\frac{\alpha_2\tau+\beta_2}{\gamma_2\tau+\delta_2}\right) = e^{\frac{\pi i}{8}(\alpha\beta+\alpha^2-1)}\varphi(\tau\pm 2) = e^{\frac{\pi i}{8}(\alpha\beta+\alpha^2-1\pm 2)}\varphi(\tau),$$

onde basterà verificare le congruenze

$$\left.\begin{aligned}(\alpha\pm 2\beta)\beta + (\alpha\pm 2\beta)^2 &\equiv \alpha\beta+\alpha^2\\ \alpha(\pm 2\alpha+\beta) + \alpha^2 &\equiv \alpha\beta+\alpha^2\pm 2\end{aligned}\right\}\ (\text{mod } 16);$$

tale verifica è immediata, ove si rifletta che α è dispari, β pari.

2° caso $\qquad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1\\ 1, & 0\end{pmatrix}$ (mod 2).

Poichè

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}-\beta, & \alpha\\ -\delta, & \gamma\end{pmatrix}$$

e si ha

$$\begin{pmatrix}-\beta, & \alpha\\ -\delta, & \gamma\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \ (\text{mod. } 2),$$

risulterà per la (9)

$$\varphi\left(\frac{-\beta\tau+\alpha}{-\delta\tau+\gamma}\right) = e^{\frac{\pi i}{8}(\beta^2-\alpha\beta-1)}\varphi(\tau)$$

e, cangiando τ in $-\frac{1}{\tau}$, avremo dunque

$$(10)\qquad \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\beta^2-\alpha\beta-1)}\psi(\tau)\left[\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1\\ 1, & 0\end{pmatrix}\right].$$

3° caso $\qquad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}$ (mod 2).

Si ha

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix}\begin{pmatrix}\alpha, & \alpha+\beta\\ \gamma, & \gamma+\delta\end{pmatrix}$$

ed è

$$\begin{pmatrix}\alpha, & \alpha+\beta\\ \gamma, & \gamma+\delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \ (\text{mod } 2),$$

onde per la (9)

$$\varphi\left(\frac{\alpha\tau+(\alpha+\beta)}{\gamma\tau+(\gamma+\delta)}\right) = e^{\frac{\pi i}{8}(\alpha\beta+1)}\varphi(\tau)$$

e, mutando τ in $\tau - 1$, segue per le (7*)

$$(11)\qquad \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}\alpha\beta}\cdot\frac{\varphi(\tau)}{\psi(\tau)}\left[\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}\right].$$

4° caso $\qquad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 1\\ 1, & 0\end{pmatrix}$ (mod 2).

Essendo

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}-\beta, & \alpha\\ -\delta, & \gamma\end{pmatrix}, \quad \begin{pmatrix}-\beta, & \alpha\\ -\delta, & \gamma\end{pmatrix} \equiv \begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix},$$

siamo subito ridotti al caso precedente ed abbiamo

$$(12)\qquad \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{-\pi i}{8}\alpha\beta}\frac{\psi(\tau)}{\varphi(\tau)}, \text{ per } \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 1\\ 1, & 0\end{pmatrix} \ (\text{mod } 2).$$

5° caso
$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1\\ 1, & 1\end{pmatrix} \pmod 2.$$

Colla formola
$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix} \begin{pmatrix}\alpha, & \alpha+\beta\\ \gamma, & \gamma+\delta\end{pmatrix}$$

si riduce al secondo caso e si trova

$$\text{(12*)} \quad \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\alpha\beta+\beta^2-1)} \frac{1}{\psi(\tau)}, \text{ per } \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1\\ 1, & 1\end{pmatrix} \pmod 2.$$

6° caso
$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix} \pmod 2.$$

Si riduce al precedente, osservando che
$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}0, & -1\\ +1, & 0\end{pmatrix} \begin{pmatrix}-\beta, & \alpha\\ -\delta, & \gamma\end{pmatrix},$$
e si ha quindi

$$\text{(13)} \qquad \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(-\alpha\beta+\alpha^2-1)} \cdot \frac{1}{\varphi(\tau)}.$$

Riepiloghiamo le formole trovate nel quadro seguente :

$$\text{(A)} \begin{cases}
\text{I)} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix};\ \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\alpha^2+\alpha\beta-1)} \cdot \varphi(\tau)\\
\text{II)} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}0, 1\\ 1, 0\end{pmatrix};\ \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\beta^2-\alpha\beta-1)} \cdot \psi(\tau)\\
\text{III)} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 1\\ 0, 1\end{pmatrix};\ \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}\alpha\beta} \frac{\varphi(\tau)}{\psi(\tau)}\\
\text{IV)} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 1\\ 1, 0\end{pmatrix};\ \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{-\pi i}{8}\alpha\beta} \frac{\psi(\tau)}{\varphi(\tau)}\\
\text{V)} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}0, 1\\ 1, 1\end{pmatrix};\ \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\alpha\beta+\beta^2-1)} \frac{1}{\psi(\tau)}\\
\text{VI)} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 1, 1\end{pmatrix};\ \varphi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(-\alpha\beta+\alpha^2-1)} \cdot \frac{1}{\varphi(\tau)},
\end{cases}$$

ove le congruenze s'intendono prese rispetto al modulo 2. Si hanno subito le formole analoghe per $\psi(\tau)$ osservando che
$$\psi(\tau) = \varphi\left(-\frac{1}{\tau}\right);$$
per tal modo si trovano le formole :

$$\text{(A*)} \begin{cases}
\text{I)} & \psi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\delta^2-\gamma\delta-1)} \psi(\tau)\\
\text{II)} & \psi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\gamma^2+\gamma\delta-1)} \varphi(\tau)\\
\text{III)} & \psi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(\gamma\delta+\delta^2-1)} \frac{1}{\psi(\tau)}\\
\text{IV)} & \psi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}(-\gamma\delta+\gamma^2-1)} \frac{1}{\varphi(\tau)}\\
\text{V)} & \psi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}\gamma\delta} \frac{\varphi(\tau)}{\psi(\tau)}\\
\text{VI)} & \psi\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{-\pi i}{8}\gamma\delta} \frac{\psi(\tau)}{\varphi(\tau)},
\end{cases}$$

in corrispondenza alle formole egualmente numerate nella tabella A.

Da queste formole si trae immediatamente l'enunciato teorema che i sottogruppi riproduttivi di $\varphi(\tau)$, $\psi(\tau)$ sono perfettamente definiti da congruenze. E invero la tabella (A) dimostra che la funzione modulare $\varphi(\tau) = \sqrt[4]{k}$ si riproduce per tutte e sole le sostituzioni $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ che soddisfano alle congruenze

$$\text{(14)} \qquad \begin{cases} \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \pmod 2\\ \alpha\beta+\alpha^2 \equiv 1 \pmod{16}, \end{cases}$$

la quale ultima può anche surrogarsi colle due seguenti

$$\text{(15)} \qquad \begin{cases} \beta \equiv 0 \pmod{16} \quad \text{con } \alpha \equiv \pm 1 \pmod 8\\ \beta \equiv 8 \pmod{16} \quad \text{con } \alpha \equiv \pm 3 \pmod 8. \end{cases}$$

Quanto al sottogruppo riproduttivo di $\psi(\tau)$, esso non è altro che il trasformato del precedente per mezzo della sostituzione $T = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$ e può definirsi analogamente per congruenze.

CAPITOLO XVII.

Equazioni modulari per l'invariante assoluto e per la funzione modulare $\sqrt[4]{k}$. – Metodo di Hermite per la risoluzione dell'equazione generale di quinto grado.

§ 183. — Considerazioni preliminari.

Una delle più importanti proprietà delle funzioni modulari è di dar luogo alle così dette *equazioni modulari*, che possono considerarsi sia come formole di moltiplicazione, sia come formole di divisione dell'argomento per un numero intero n e, più in generale, come formole di trasformazione di ordine n.

Già al § 168 abbiamo dimostrato l'esistenza dell'equazione modulare per l'invariante assoluto $J(\tau)$, deducendola dalle formole di trasformazione della funzione ellittica $\wp u$. Ci proponiamo ora di stabilire in modo più diretto l'esistenza e le proprietà delle equazioni modulari, fondandoci unicamente sulle proprietà delle funzioni modulari.

Dobbiamo per ciò in primo luogo ritornare allo sviluppo di $J(\tau)$ per potenze di

$$q = e^{\pi i \tau},$$

che già al § 119 abbiamo visto possedere la forma

$$J(\tau) = \frac{A}{q^2} + a_0 + a_1 q^2 + a_2 q^4 + \dots + a_n q^{2n} + \dots,$$

per precisare la natura dei coefficienti in questo sviluppo. A tale scopo ricorriamo all'espressione di $J(\tau)$ per k^2:

$$J(\tau) = \frac{4}{27} \frac{(1 - k^2 k'^2)^3}{(k^2 k'^2)^2},$$

osservando che secondo le formole (XVI), pag. 180 si ha

$$\sqrt{k} = 2 q^{\frac{1}{4}} \frac{\sum_1^\infty q^{n(n+1)}}{1 + 2\sum_1^\infty q^{n^2}} = 2 q^{\frac{1}{4}} \frac{1 + q^2 + q^6 + q^{12} + \dots}{1 + 2q + 2q^4 + 2q^9 + \dots}.$$

Eseguendo il quoziente delle due serie del secondo membro, col determinare i coefficienti di questo quoziente colle note formole ricorrenti, vediamo subito che questi coefficienti sono tutti numeri interi e si ha

$$\sqrt{k} = 2 q^{\frac{1}{4}} (1 - 2q + 5q^2 - 10q^3 + \dots)$$

da cui

$$k^2 = 2^4 q (1 - 8q + 44 q^2 - 152 q^3 + \dots)$$

$$k'^2 = 1 - 16 q + 128 q^2 - 704 q^3 + \dots,$$

e sostituendo in $J(\tau)$ avremo

$$J(\tau) = \frac{1}{12^3 q^2} (1 + a_1 q^2 + a_2 q^4 + a_3 q^6 + \dots),$$

dove le a sono tutti numeri interi [1]) e la serie contiene solo le potenze pari di q, a causa della formola $J(\tau + 1) = J(\tau)$. In ciò che segue, per evitare coefficienti frazionari è conveniente sostituire a $J(\tau)$, come invariante assoluto, la funzione

$$j(\tau) = 12^3 J(\tau),$$

che non ne differisce che pel fattore numerico 12^3; avremo così per lo sviluppo di $j(\tau)$

$$\text{(I)} \qquad j(\tau) = \frac{1}{q^2} (1 + 744 q^2 + 196844 q^4 + \dots)$$

gli altri coefficienti della serie ordinata per potenze di q^2 essendo numeri interi. Ricordiamo che questo sviluppo vale per tutto il campo d'esistenza della funzione, cioè in tutto il semipiano positivo τ.

A fondamento delle ricerche sulle equazioni modulari porremo le osservazioni seguenti. Supponiamo che sia $F(\tau)$ una funzione *finita, continua e monodroma* di τ in tutto il semipiano positivo e che inoltre $F(\tau)$ rimanga, come $j(\tau)$, invariata per *tutte* le so-

[1]) **In particolare si ha**

$$a_1 = 744, \quad a_2 = 196884.$$

stituzioni del gruppo modulare Γ. Allora $F(\tau)$, considerata come funzione di $j(\tau)$, sarà monodroma in j, perchè per ogni cammino chiuso descritto da j nel suo piano, τ subisce appunto una sostituzione del gruppo modulare. Poichè inoltre, per ogni valore finito di j, la funzione $F(\tau) = \Theta(j)$ per ipotesi è finita, sarà in generale $\Theta(j)$ una trascendente intera in j; e viceversa è chiaro che ogni trascendente intera di j è una funzione finita, continua e monodroma di τ nel semipiano positivo e rimane invariata per qualunque sostituzione del gruppo modulare. Ma supponiamo di più che la funzione $\Theta(j)$ si comporti per $j = \infty$ come una potenza intera e positiva j^n di j, che cioè $\frac{\Theta(j)}{j^n}$ converga per $j = \infty$ verso un valore determinato e finito; ne concluderemo subito che $\Theta(j)$ è un polinomio razionale intero in j. Si ha dunque il teorema fondamentale:

Ogni funzione finita, continua e monodroma di τ nel semipiano positivo, che si riproduca per ogni sostituzione $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ del gruppo modulare, e per $j = \infty$ si comporti come una potenza di j, è una funzione razionale intera dell'argomento j.

§ 184. — Esistenza dell'equazione modulare per $j(\tau)$.

Perveniamo direttamente alla teoria delle equazioni modulari proponendoci il seguente problema: *Come cangia $j(\tau)$ quando sull'argomento τ si eseguisca una sostituzione lineare*

$$\frac{a\tau+b}{c\tau+d}$$

a coefficienti interi e a determinante

$$ad - bc = n$$

positivo [1]) *qualunque?*

Per risolvere questo problema cerchiamo in primo luogo quanti valori distinti assume

$$j\left(\frac{a\tau+b}{c\tau+d}\right)$$

[1]) Il determinante $ad-bc$ deve essere positivo, affinchè $\frac{a\tau+b}{c\tau+d}$ resti nel semipiano positivo.

per tutte le possibili sostituzioni $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ col medesimo determinante n. Se $\begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix}$ è un'altra sostituzione col medesimo determinante n, avremo

$$j\left(\frac{a'\tau+b'}{c'\tau+d'}\right) = j\left(\frac{a\tau+b}{c\tau+d}\right)$$

allora e allora soltanto che si abbia

$$\frac{a'\tau+b'}{c'\tau+d'} = \frac{\alpha\frac{a\tau+b}{c\tau+d}+\beta}{\gamma\frac{a\tau+b}{c\tau+d}+\delta}$$

cioè

$$(2) \qquad \begin{pmatrix} a', & b' \\ c', & d' \end{pmatrix} = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} a\alpha+c\beta, & b\alpha+d\beta \\ a\gamma+c\delta, & b\gamma+d\delta \end{pmatrix},$$

essendo $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ una qualunque sostituzione del gruppo modulare. Diremo allora che le due sostituzioni $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ sono equivalenti. Con un processo affatto analogo a quello usato nei §§ 162, 163 si vedrà che ad ogni sostituzione $\begin{pmatrix} a, & b \\ c, & b \end{pmatrix}$ se ne potrà sostituire una equivalente del tipo normale

$$\begin{pmatrix} \sigma, & \nu \\ 0, & \frac{n}{\sigma} \end{pmatrix},$$

dove σ è un divisore di n e ν è determinato soltanto rispetto al modulo $\frac{n}{\sigma}$. Ne risulta che il numero dei valori distinti di

$$j\left(\frac{a\tau,+b}{c\tau,+d}\right),$$

per tutte le possibili sostituzioni $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ di un dato determinante, è sempre un numero finito. E siccome valgono anche qui i teoremi del § 164 rispetto alla composizione delle sostituzioni, potremo limitare la nostra ricerca al caso in cui n sia eguale ad un numero primo p. Allora i valori distinti di

$$j\left(\frac{a\tau+b}{c\tau+d}\right),\quad ad-bc=p$$

saranno $p+1$ soltanto e cioè

$$(3)\qquad j(p\tau),\ j\left(\frac{\tau}{p}\right),\ j\left(\frac{\tau+1}{p}\right)\ \dots\ j\left(\frac{\tau+p-1}{p}\right).$$

D'altronde per una sostituzione qualunque $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare, eseguita su τ, questi $p+1$ valori di $j\left(\frac{a\tau+b}{c\tau+d}\right)$ si permutano semplicemente fra loro, poichè da

$$j\left(\frac{a\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}+b}{c\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}+d}\right)=j\left(\frac{a'\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}+b'}{c'\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}+d'}\right)$$

segue anche

$$j\left(\frac{a\tau+b}{c\tau+d}\right)=j\left(\frac{a'\tau+b'}{c'\tau+d'}\right).$$

Ora, essendo r un intero positivo qualunque, poniamo

$$(4)\quad F_r(\tau)=j^r(p\tau)+j^r\left(\frac{\tau}{p}\right)+j^r\left(\frac{\tau+1}{p}\right)+\dots+j^r\left(\frac{\tau+p-1}{p}\right)$$

e sarà evidentemente $F_r(\tau)$ una funzione finita, continua e monodroma di τ in tutto il semipiano positivo, che resterà inoltre invariata per tutte le sostituzioni del gruppo modulare, avendo queste per effetto di permutare fra loro i termini della somma nel secondo membro della (4). Ma dallo sviluppo in serie (1) per $j(\tau)$ abbiamo

$$(\mathrm{II})\ \begin{cases} j(p\tau)=q^{-2p}(1+744\,q^{2p}+196844\,q^{4p}+\dots)\\[4pt] j\left(\dfrac{\tau+\tau}{p}\right)=\varepsilon^{-\nu}q^{-\frac{2}{p}}\left(1+743\,\varepsilon^{\nu}q^{\frac{2}{p}}+196844\,\varepsilon^{2\nu}q^{\frac{4}{p}}+\dots\right)\end{cases}$$

$$\varepsilon=e^{\frac{2\pi i}{p}},$$

onde si vede che $F_r(\tau)$ per $j=\infty$ si comporta come j^{rp}, cioè il quoziente

$$\frac{F_r(\tau)}{j^{rp}}$$

ha un limite finito e diverso da zero per $j=\infty$. Dunque $F^r(\tau)$ è un polinomio razionale intero in j (§ 183). Se poniamo

$$j_\infty=j(p\tau),\ j_0=j\left(\frac{\tau}{p}\right),\ j_1=j\left(\frac{\tau+1}{p}\right)\ \dots\ j_{p-1}=j\left(\frac{\tau+(p-1)}{p}\right),$$

e costruiamo il polinomio di grado $p+1$ nella variabile j'

$$(j'-j_\infty)\ (j'-j_0)\ (j'-j_1)\ \dots\ (j'-j_{p-1})=$$
$$=j'^{p+1}+a_1j'^{p}+a_2j'^{p-1}+\dots+a_pj'+a_{p+1},$$

i coefficienti a saranno polinomii razionali interi in $j(\tau)$. Siamo così direttamente arrivati all'esistenza dell'equazione modulare col teorema:

Se $\begin{pmatrix}a, & b\\ c, & d\end{pmatrix}$ *è una sostituzione a coefficienti interi e a determinante primo p, fra le funzioni di τ*

$$j'=j\left(\frac{a\tau+b}{c\tau+d}\right),\ j=j(\tau)$$

sussiste un'equazione algebrica di grado $p+1$ in j':

$$(\mathrm{1II})\quad f(j',j)=j'^{p+1}+a_1j'^{p}+a_2j'^{p-1}+\dots+a_pj'+a_{p+1}=0,$$

i cui coefficienti a sono polinomî razionali interi in j.

Questa è l'equazione modulare fra j, j' e le sue $p+1$ radici in j' sono

$$j_\infty=j(p\tau),\ j_0=j\left(\frac{\tau}{p}\right),\ j_1=j\left(\frac{\tau+1}{p}\right)\ \dots\ j_{p-1}=j\left(\frac{\tau+(p-1)}{p}\right).$$

§ 185. — Gruppo di monodromia dell'equazione modulare.

Vogliamo ora determinare direttamente il gruppo di monodromia dell'equazione modulare, confermando così i risultati ottenuti alla fine del § 168. Dobbiamo per ciò far percorrere a $j(\tau)$, nel suo piano complesso, un cammino chiuso qualunque ed esaminare come si permutano corrispondentemente i $p+1$ rami

$$j_\infty, \; j_0, \; j_1, \dots, j_{p-1}$$

della funzione algebrica j' di j. Un cammino chiuso qualsiasi, descritto da $j(\tau)$, produce su τ una sostituzione $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare e basterà per ciò esaminare l'effetto sui $p+1$ rami delle sostituzioni elementari

$$\begin{pmatrix}1, & 1 \\ 0, & 1\end{pmatrix}, \quad \begin{pmatrix}0, & 1 \\ -1, & 0\end{pmatrix}.$$

Per la prima $j_\infty = j(p\tau)$ non cangia, mentre

$$j_\nu = j\left(\frac{\tau+\nu}{p}\right)$$

si cangia in

$$j\left(\frac{\tau+\nu+1}{p}\right) = j_{\nu+1};$$

dunque gli indici ν dei $p+1$ rami subiscono la sostituzione lineare

$$a) \qquad \nu' \equiv \nu + 1 \pmod{p}$$

Per l'altra sostituzione

$$\tau' = -\frac{1}{\tau}$$

i due rami

$$j_\infty = j(p\tau), \quad j_0 = j\left(\frac{\tau}{p}\right)$$

si permutano fra loro, giacchè

$$j\left(-\frac{p}{\tau}\right) = j\left(\frac{\tau}{p}\right), \quad j\left(-\frac{1}{p\tau}\right) = j(p\tau).$$

E se indichiamo con $j_{\nu'}$ il ramo in cui va j_ν per ν diverso da $0, \infty$, dovremo avere

$$j\left(\frac{-\frac{1}{\tau}+\nu}{p}\right) = j\left(\frac{\nu\tau-1}{p\tau}\right) = j\left(\frac{\tau+\nu'}{p}\right),$$

e perciò

$$\frac{\nu\tau-1}{p\tau} = \frac{\alpha\,\frac{\tau+\nu'}{p}+\beta}{\gamma\,\frac{\tau+\nu'}{p}+\delta} = \frac{\alpha\tau+(\alpha\nu'+\beta p)}{\gamma\tau+(\gamma\nu'+\delta p)},$$

essendo $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ una sostituzione del gruppo modulare. Il paragone dei coefficienti in queste due sostituzioni lineari a determinante p dà

$$\alpha = \pm\nu, \quad \alpha\nu' + \beta p = \mp 1,$$

onde

$$\nu\nu' \equiv -1 \pmod{p},$$

formola che vale anche per $\nu \equiv 0, \infty$ come sopra si è visto. Dunque la sostituzione $\begin{pmatrix}0, & 1 \\ -1, & 0\end{pmatrix}$ produce sugli indici dei rami la sostituzione

$$b) \qquad \nu' \equiv -\frac{1}{\nu} \pmod{p}.$$

E siccome colle due sostituzioni $a)$, $b)$ si genera, come sappiamo, l' intero gruppo modulare (mod p)

$$\text{(IV)} \qquad \nu' \equiv \frac{a\nu+b}{c\nu+d} \pmod{p}, \quad ad - bc \equiv 1,$$

si conclude che questo è il gruppo richiesto di monodromia.

Del resto è anche facile vedere quale sostituzione del gruppo di monodromia (IV) si produce per una sostituzione qualsiasi $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ del gruppo modulare. Supposto invero

$$j_\nu\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = j_{\nu'}(\tau),$$

avremo

$$j\left(\frac{\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}+\nu}{p}\right)=j\left(\frac{(\alpha+\gamma\nu)\tau+(\beta+\delta\nu)}{p\gamma\tau+p\delta}\right)=j\left(\frac{\tau+\nu'}{p}\right),$$

quindi

$$\frac{(\alpha+\gamma\nu)\tau+(\beta+\delta\nu)}{p\delta\tau+p\delta}=\frac{\alpha'\dfrac{\tau+\nu'}{p}+\beta'}{\gamma'\dfrac{\tau+\nu'}{p}+\delta'}=\frac{\alpha'\tau+(\alpha'\nu'+\beta' p)}{\gamma'\tau+(\gamma'\nu'+\delta' p)},$$

essendo $\begin{pmatrix}\alpha', & \beta' \\ \gamma', & \delta'\end{pmatrix}$ un' altra sostituzione del gruppo modulare. Se ne trae

$$\alpha+\gamma\nu=\pm\alpha', \quad \beta+\delta\nu=\pm(\alpha'\nu'+\beta' p)$$

onde

$$\nu'\equiv\frac{\delta\nu+\beta}{\gamma\nu+\alpha} \pmod p$$

e se ne conclude: *La sostituzione* $\dfrac{\alpha\tau+\beta}{\gamma\tau+\delta}$ *del gruppo modulare produce sui* $p+1$ *indici dei rami della funzione algebrica* j' *la sostituzione*

(5) $$\nu'\equiv\frac{\delta\nu+\beta}{\gamma\nu+\alpha} \pmod p.$$

Siccome questo gruppo sui $p+1$ rami è transitivo (anzi doppiamente transitivo), si vede che: *L'equazione modulare* (III) *è irriducibile.*

§ 186. — Diramazione di j' rapporto a j e poligono fondamentale di $j\left(\frac{\tau}{p}\right)$.

Mediante i risultati ora conseguiti è facile studiare l'effettiva diramazione della funzione modulare j' rapporto a j, ciò che ci fornirà un esempio semplice ed istruttivo della teoria generale al § 175. Se $j=a$ è punto qualunque del piano complesso j, e τ_1

il punto corrispondente del triangolo fondamentale, per un giro di j attorno ad a, supposto dapprima $a \neq 0, 12^3, \infty$, sopra una piccola curva chiusa, τ girerà una sola volta attorno a τ_1 e ciascun ramo j_ν tornerà col proprio valore, cioè non vi sarà diramazione di j'. Se poi $a=0$, ovvero $a=12^3$, o infine $a=\infty$, avremo corrispondentemente

$$\tau_1=e^{\frac{2\pi i}{3}}, \quad \tau_1=i, \quad \tau_1=\infty,$$

e un giro positivo di j attorno ad a produrrà rispettivamente le sostituzioni

$$-\frac{\tau+1}{\tau}, \quad -\frac{1}{\tau}, \quad \tau+1$$

sopra τ. Avremo quindi sugli indici ν dei rami di j' rispettivamente le sostituzioni:

$$\alpha)\ \nu'\equiv\frac{1}{1-\nu}, \quad \beta)\ \nu'\equiv-\frac{1}{\nu}, \quad \gamma)\ \nu'\equiv\nu+1 \pmod p.$$

La α) è a periodo 3 e quindi i rami si permutano attorno a $j=0$ tre a tre, e potranno restare eventualmente isolati due rami corrispondenti alle radici della congruenza

$$\nu^2-\nu+1\equiv 0 \pmod p.$$

ossia

$$(2\nu-1)^2\equiv-3 \pmod p.$$

Dunque quando $\left(\frac{-3}{p}\right)=+1$, cioè quando p è della forma $6r+1$, due rami restano isolati e i rimanenti $p-1=6r$ si permutano 3 a 3; che se invece p è della forma $6r+5$, allora tutti i $p+1$ rami si permutano 3 a 3. Nel caso particolare $p=3$ il solo ramo

$$j_2=j\left(\frac{\tau+2}{3}\right)$$

resta isolato, permutandosi ciclicamente i tre restanti.

Similmente dalla β) si vede che in $j = 12^3$ tutti i rami si scambiano 2 a 2, se p è della forma $4n+3$; e invece due dei rami corrono isolati, se p è della forma $4n+1$.

In fine per $j = \infty$ abbiamo in ogni caso un ramo isolato, mentre i p rimanenti si scambiano ciclicamente.

Volendo rappresentare la superficie Riemanniana, corrispondente all'equazione algebrica modulare (III), basterà costruire, secondo il § 177, il poligono fondamentale di una delle sue radici, per es. di

$$j\left(\frac{\tau}{p}\right),$$

ed esaminare la distribuzione dei suoi lati in coppie di lati coniugati. Ora dalla (5) risulta subito che le sostituzioni $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ del gruppo modulare Γ, che lasciano invariata la funzione modulare $j\left(\frac{\tau}{p}\right)$, sono tutte e sole quelle per le quali $\beta \equiv 0 \pmod p$. Queste formano in Γ un sottogruppo congruenziale G d'indice finito $= p+1$, che è il sottogruppo riproduttivo di $j\left(\frac{\tau}{p}\right)$. I $p+1$ valori distinti che assume $j_0 = j\left(\frac{\tau}{p}\right)$ per le sostituzioni di Γ sono, come sappiamo

$$j(p\tau) = j\left(-\frac{1}{p\tau}\right), \quad j\left(\frac{\tau+\nu}{p}\right),$$

percorrendo ν un sistema completo di resti (mod p), onde si rileva che un sistema completo di $p+1$ sostituzioni di Γ, non equivalenti rispetto a G, è dato da

$$T = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}, \quad S^\nu = \begin{pmatrix}1, & \nu\\ 0, & 1\end{pmatrix},$$

ove ν percorra un sistema completo di resti (mod p). Ogni altra sostituzione $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ di Γ sarà equivalente, rispetto a G, ad una di queste, cioè sarà

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}a, & b\\ c, & d\end{pmatrix} = \begin{pmatrix}-b, & a\\ -d, & c\end{pmatrix},$$

ovvero

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}1, & r\\ 0, & 1\end{pmatrix}\begin{pmatrix}a, & b\\ c, & d\end{pmatrix} = \begin{pmatrix}a, & ra+b\\ c, & rc+d\end{pmatrix},$$

essendo $\begin{pmatrix}a, & b\\ c, & d\end{pmatrix}$ una sostituzione di G, che ha cioè $b \equiv 0 \pmod p$. Si vede di qui che sono equivalenti a T tutte quelle sostituzioni che hanno $a \equiv 0 \pmod p$, che se invece $a \not\equiv 0 \pmod p$ sarà $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ equivalente a quella S^r per la quale

$$r\alpha \equiv \beta \pmod p.$$

Ciò premesso, ed escludendo il caso di $p = 2$, che si tratta subito direttamente, supponiamo p dispari e prendiamo per i $p+1$ rappresentanti le $p+1$ sostituzioni

$$\left(S^{-\frac{p-1}{2}} \ldots S^{-2},\ S^{-1},\ 1,\ S,\ S^2 \ldots S^{\frac{p-1}{2}}\right),\ T.$$

Il poligono fondamentale di $j\left(\frac{\tau}{p}\right)$, cioè del sottogruppo $\beta \equiv 0 \pmod p$, potrà costituirsi coi $p+1$ (doppi) triangoli omonimi della rete modulare, come è rappresentato nella fig. 17 per $p = 5$. Per ricercare poi come sono coniugati due a due i lati e quali sono le sostituzioni (generatrici del sottogruppo G) che li congiungono, basta applicare la regola generale del § 177 ed osservare che al triangolo $S^r (r \not\equiv 0)$ del poligono è aderente pel lato (circolare) esterno il triangolo

$$T S^r = \begin{pmatrix}r, & -1\\ 1, & 0\end{pmatrix},$$

il quale, secondo la regola sopra notata, è relativamente equivalente a quel triangolo $S^{r'}$ del poligono pel quale si ha

$$r r' \equiv -1 \pmod p,$$

e per la corrispondente sostituzione che ne congiunge i lati si trova subito

$$\tau' = \frac{r'\tau - kp}{\tau - r}, \tag{6}$$

supposto

$$r r' + 1 = kp.$$

Al triangolo $S\,T$ aderente a T per un lato esterno, essendo

$$S\,T = \begin{pmatrix} 0, & -1 \\ 1, & 1 \end{pmatrix},$$

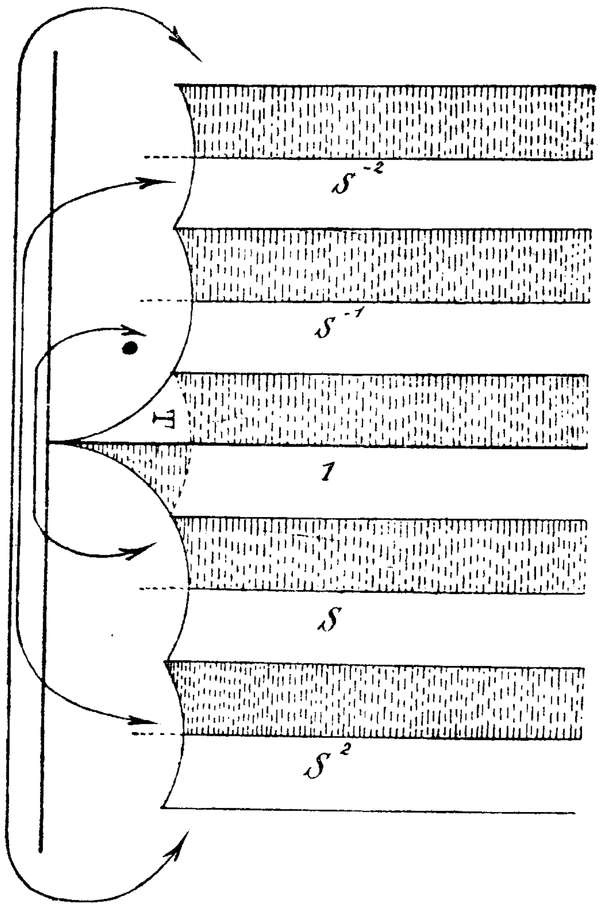

Fig. 17.

è equivalente T stesso, i cui due lati esterni sono dunque coniugati e la sostituzione che li congiunge è

$$\tau' = \frac{\tau}{\tau + 1},$$

che del resto si ottiene come caso particolare dalla (6) ove si faccia $r' = 1$, $r = -1$. Restano soltanto i due lati rettilinei del poligono, che sono congiunti dalla sostituzione

$$S^p = \begin{pmatrix} 1, & p \\ 0, & 1 \end{pmatrix}.$$

Così adunque: L'intero sottogruppo G, definito dalla congruenza $\beta \equiv 0 \pmod{p}$, è generato dalle sostituzioni

$$\begin{pmatrix} 1, & p \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} r', & -p\dfrac{r\,r'+1}{p} \\ 1, & -r \end{pmatrix}, \quad r\,r' \equiv -1 \pmod{p},$$

percorrendo r, r' le coppie incongrue che dànno $r\,r' \equiv -1 \pmod{p}$. La superficie Riemanniana chiusa, che si ottiene saldando i lati coniugati, offre naturalmente la diramazione già studiata al principio del presente paragrafo. Si potrà facilmente, colla nota formola della teoria della connessione, calcolare il *genere* della superficie Riemanniana e si vedrà che esso è zero solo nei casi

$$p = 3,\ 5,\ 7,\ 13\ ^{1)}.$$

[1]) Per calcolare il genere P della superficie Riemanniana si ha la formola già citata al § 92

$$P = \sum \frac{r-1}{2} - m + 1,$$

ove m è il numero dei fogli (qui $= p+1$), r è il numero dei fogli congiunti ciclicamente in ogni punto di diramazione. Basta ora distinguere i quattro casi che può offrire p rispetto al modulo 12, cioè i quattro câsi:

$$p = 12n+1, \quad 12\,n+5, \quad 12\,n+7, \quad 12\,n+11$$

ed, applicando la formola (α), si trova ordinatamente

$$P = n-1, \quad n, \quad n, \quad n+1.$$

ciò che dà immediatamente i risultati enunciati nel testo. Ulteriormente si ha $P = 1$ per

$$p = 11,\ 17,\ 19 \text{ ecc.}$$

§ 187. — Proprietà dei coefficienti dell'equazione modulare.

Andiamo ora a studiare più da vicino i polinomii a_1, a_2 .... a_{p+1} razionali interi in j, che sono i coefficienti dell'equazione modulare (III) § 184. In primo luogo, tenendo conto degli sviluppi (I), (II) in serie di potenze di q^2, facilmente valutiamo il loro grado. Intanto, avendosi

$$-a_1 = j_\infty + j_0 + j_1 + \dots + j_{p-1}\,,$$

nello sviluppo di a_1 per potenze di q^2 la più alta potenza negativa, che vi comparisce, è q^{-2p} che vi ha il coefficiente -1; onde per la (I) a_1 è un polinomio di grado p in j e la potenza j^p vi comparisce col coefficiente -1.

Con considerazioni analoghe si vede che i gradi di a_2, a_3, ..., a_n rispetto a j non superano p. Quanto all'ultimo

$$a_{p+1} = j_\infty\, j_0\, j_1 \dots j_{p-1}\ ^{1)},$$

esso contiene nello sviluppo in potenze di q^2 come più alta potenza negativa $q^{-2(p+1)}$ col coefficiente $+1$ e si ha per ciò

$$a_{p+1} = j^{p+1} + b_1 j^p + b_2 j^{p-1} \dots,$$

essendo le b coefficienti numerici. Da tuttociò si raccoglie che l'equazione modulare (III) può scriversi sotto la forma

$$\text{(V)} \qquad (j'^p - j)\,(j' - j^p) = \sum_{r,s}^{0\dots p} c_{rs}\, j'^r j^s,$$

dove $c_{r,s}$ è un coefficiente numerico, e per quanto sopra è detto

$$c_{p,p} = 0.$$

Dimostriamo ora l'importante proprietà: *Tutti i coefficienti* c_{rs} *dell'equazione modulare* (V) *sono numeri interi divisibili per* p.

In primo luogo dimostriamo che l'*equazione modulare* (V)

$$f(j', j) = (j'^p - j)\,(j' - j^p) - \sum_{r,s}^{0\dots p} c_{r,s}\, j'^r j^r = 0$$

[1]) Si suppone p impari.

è simmetrica in j', j. Si ha infatti, qualunque sia τ

$$f(j(p\tau), j(\tau)) = 0,$$

e cangiando τ in $\dfrac{\tau}{p}$

$$f\left(j(\tau), j\left(\frac{\tau}{p}\right)\right) = 0,$$

cioè

$$f(j, j') = 0,$$

ossia

$$j^{p+1} + j'^{p+1} - j'^p j^p - j j' - \sum c_{rs}\, j^r j'^s = 0.$$

Se questa non coincidesse colla precedente, sottraendole si avrebbe per j' un'equazione di grado inferiore a $p+1$, ciò che è contrario alla dimostrata irriducibilità dell'equazione modulare; dunque si ha

$$c_{rs} = c_{sr}$$

e la (V) può scriversi

$$\text{(V*)} \quad (j^p - j)\,(j' - j^p) = \sum_{r=0}^{r=p} \sum_{s=0}^{s=r-1} c_{rs}\,(j'^r j^s + j^r j'^s) + \sum_{s=n}^{s=p-1} c_{ss}\, j'^s j^s.$$

Per determinare i coefficienti c_{rs} osserviamo che questa equazione diventa un' identità se vi si fa

$$j = j(\tau) = q^{-2} \sum_{s=0}^{s=\infty} a_s q^{2s}$$

$$j' = j(p\tau) = q^{-2p} \sum_{s=0}^{s=\infty} a_s q^{2ps}.$$

Ora, per la legge di formazione della potenza p^{ma} di una serie, risulta di qui

$$j^p = q^{-2p} \sum_s a_s^p q^{2ps} + p\, q^{-2(p-1)} \sum_s a'_s q^{2s},$$

dove le a' sono, come le a, numeri interi.

Ma si ha, pel teorema di Fermat

$$a_s^p \equiv a_s \pmod{p}, \ a_0 = 1$$

e la precedente può scriversi

$$j^p = q^{-2p} \sum_s a_s q^{2ps} + p q^{-2(p-1)} \sum_s b_s q^{2s},$$

essendo le b altri numeri interi, onde risulta

$$(j'^p - j)\ (j' - j^p) = p q^{-2(p^2-p-1)} \sum_s d_s q^{2s},$$

ove le d sono nuovamente numeri interi.

Sostituiamo questo sviluppo nel primo membro della (V), ponendo nel secondo membro per

$$j'^r j^s + j^r j'^s, \quad j'^s j^s$$

i loro sviluppi per potenze di q^2, che cominciano rispettivamente coi termini

$$q^{-2(pr+s)}, \quad q^{-2s(p+1)},$$

aventi per coefficienti $+1$. Nel secondo membro della (V*) non possono comparire due termini colla stessa più alta potenza di q; poichè da

$$pr + s = pr' + s'$$

segue $s = s'$, $r = r'$. Paragonando adunque dalle due parti i coefficienti delle potenze negative di q, cominciando dalla più alta, avremo ogni volta delle equazioni lineari nelle c, delle quali ciascuna conterrà una sola nuova incognita c_{rs} col coefficiente $= 1$ [1]). Dunque tutti i coefficienti c sono numeri interi divisibili per p c. d. d.

[1]) Se si scrivono i coefficienti c_{rs} nel quadro

$$\begin{array}{lllll}
c_{p-1,\,p-1} & & & & \\
c_{p-1,\,p-2} & c_{p-2,\,p-2} & & & \\
c_{p-1,\,p-3} & c_{p-2,\,p-3} & c_{p-3,\,p-3} & & \\
\cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \\
c_{p-1,\,1} & c_{p-2,\,1} & c_{p-3,\,1} \ldots & c_{11} & \\
c_{p-1,\,0} & c_{p-2,\,0} & c_{p-3,\,0} \ldots & c_{10} & c_{00},
\end{array}$$

è chiaro che verranno così successivamente determinati i coefficienti della prima colonna (dall'alto in basso) poi quelli della seconda, della terza ecc.

§ 188. — Gruppo algebrico dell'equazione modulare.

Ora che conosciamo la natura dei coefficienti dell'equazione modulare (V) possiamo completare la ricerca del § 185, ove abbiamo dimostrato che il gruppo di monodromia di questa equazione contiene le $\frac{p(p^2-1)}{2}$ sostituzioni sugli indici

$$\text{(IV)} \qquad \nu' \equiv \frac{a\nu + b}{c\nu + d}, \quad ad - bc \equiv 1 \pmod{p},$$

e determinare anche il suo gruppo algebrico o di Galois *nel campo dei numeri razionali*. Il gruppo algebrico deve contenere quello di monodromia come sottogruppo invariante e si sa dalla teoria dei gruppi di sostituzioni che il più ampio gruppo, contenente come sottogruppo invariante il gruppo (IV), è quello formato da tutte le possibili sostituzioni lineari sugli indici

$$\nu' \equiv \frac{a\nu + b}{c\nu + d} \pmod{p}, \quad ad - bc \not\equiv 0.$$

In questo gruppo $H_{p(p^2-1)}$ di $p(p^2-1)$ sostituzioni il gruppo di monodromia (IV), che indichiamo con $H'_{\frac{p(p^2-1)}{2}}$, è contenuto come sottogruppo invariante d'indice 2; e si noti che H' contiene tutte le sostituzioni pari di H. Pertanto il gruppo algebrico dell'equazione modulare coinciderà o con H', o con H. Per decidere quale dei due casi abbia luogo, consideriamo la radice quadrata del discriminante D dell'equazione modulare

$$(7) \qquad \sqrt{D} = \prod_{\nu=0}^{\nu=p-1} (j_\infty - j_\nu) \prod_{\nu,\,\nu'} (j_\nu - j'_\nu),$$

il secondo prodotto essendo esteso a tutte le $\frac{p(p-1}{2}$ combinazioni degli indici ν, ν' presi nella serie 0, 1, 2, ..., $p-1$ colla condizione $\nu < \nu'$. Questa è una funzione razionale (intera) delle radici dell'equazione modulare, invariabile per le sostituzioni di H', non per quelle di H, ed è quindi un polinomio razionale intero in j con coefficienti numerici. Se il gruppo algebrico coincide con H', questi coefficienti saranno numeri razionali e nel caso opposto invece dovranno contenere un' irrazionalità quadratica $\sqrt{A}$, con A numero razionale, la cui aggiunta abbasserà il gruppo algebrico al gruppo di monodromia. Poniamo

$$\sqrt{D} = \Theta(j),$$

essendo Θ un polinomio razionale intero in j e calcoliamo il coefficiente a della più alta potenza di j in Θ. Sostituiamo per ciò nel secondo membro della (7) per j_∞, j_ν i loro sviluppi (II) in serie:

$$j_\infty = q^{-2p}(1 + a_1 q^{2p} + \ldots), \quad j_\nu = \varepsilon^{-\nu} q^{-\frac{2}{p}}\left(1 + a_1 \varepsilon^\nu q^{\frac{2}{p}} + \ldots\right)$$
$$\left(\varepsilon = e^{\frac{2\pi i}{p}}\right)$$

e vedremo subito che la più alta potenza di q^{-1} nel secondo membro è data da

$$q^{-(2p^2+p-1)}$$

ed il suo coefficiente sarà

$$a = \prod_{\nu,\nu'} (\varepsilon^\nu - \varepsilon^{\nu'}). \tag{8}$$

Dunque $\Theta(j)$ è di grado $p^2 + \frac{p-1}{2}$ in j e si ha

$$\Theta(j) = a j^{p^2 + \frac{p-1}{2}} + \ldots,$$

i termini seguenti essendo di grado inferiore a $p^2 + \frac{p-1}{2}$ e il coefficiente a avendo il valore (8). Si osservi ora che

$$a^2 = \prod_{\nu,\nu'} (\varepsilon^\nu - \varepsilon^{\nu'})^2$$

non è altro che il discriminante dell'equazione

$$x^p - 1 = 0,$$

e per ciò, indicando con s_r la somma delle potenze r^{me} delle sue radici, si ha

$$a^2 = \begin{vmatrix} s_0 & s_1 & \ldots & s_{p-1} \\ s_1 & s_2 & \ldots & s_p \\ \ldots & \ldots & \ldots & \ldots \\ s_{p-1} & s_p & \ldots & s_{2(p-1)} \end{vmatrix}$$

e poichè $s_r = 1 + \varepsilon^r + \varepsilon^{2r} \ldots, + \varepsilon^{(p-1)r}$ è eguale a p se $r \equiv 0 \pmod{p}$, e invece

$$s_r = \frac{\varepsilon^{pr} - 1}{\varepsilon^r - 1} = 0 \quad \text{per } r \not\equiv 0 \pmod{p},$$

avremo

$$a^2 = \begin{vmatrix} p & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & p \\ 0 & 0 & 0 & \ldots & p & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & p & 0 & \ldots & 0 & 0 \end{vmatrix} = (-1)^{\frac{p-1}{2}} p^p$$

e quindi

$$a = p^{\frac{p-1}{2}} \sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Se ne conclude adunque: *Il gruppo algebrico dell'equazione modulare è il gruppo lineare totale*

$$\nu' = \frac{a\nu + b}{c\nu + d} \pmod{p}, \quad ad - bc \not\equiv 0.$$

L'irrazionalità numerica, la cui aggiunta lo abbassa al gruppo di monodromia, è data da $\sqrt{(-1)^{\frac{p-1}{2}} p}$.

§ 189. — Equazione modulare per $\varphi(\tau) = \sqrt[4]{k}$ e sue radici.

Il processo indicato al § 187 pel calcolo dei coefficienti $c_{r,s}$ potrebbe servire a dare le effettive equazioni modulari per $j(\tau)$. Ma i valori effettivi dei coefficienti c_{rs} sono numeri tanto grandi, anche per piccoli valori di p, che i calcoli indicati riuscirebbero laboriosissimi. Soltanto per $p = 2$ è calcolata la forma *esplicita* dell'equazione modulare (da Stephen Smith) e pei casi $p = 3, 5, 7, 13$, in cui il genere della superficie Riemanniana riesce zero, il Klein, utilizzando il modo di diramazione della superficie di Riemann, ha dato delle formole che implicitamente determinano le corrispondenti equazioni modulari [1]).

[1]) *Math. Annalen*, Bd. XIV.

Assai più semplici riescono le equazioni modulari per le altre funzioni (modulari) teoricamente più complicate di $j(\tau)$ [1]). Così è per le equazioni modulari della funzione

$$\varphi(\tau) = \sqrt[4]{k},$$

che furono le prime calcolate (da Jacobi e Sohncke). Vogliamo ora trattare di queste particolari equazioni modulari e costruirle effettivamente pei valori più bassi di p.

Partiamo dalla seguente osservazione generale. Se $\Phi(\tau)$ è una qualsiasi funzione modulare, legata a $J(\tau)$ dell'equazione algebrica

$$F(\Phi(\tau),\ J(\tau)) = 0,$$

cangiando in questa τ in $\frac{\tau}{n}$ avremo

$$F\left(\Phi\left(\frac{\tau}{n}\right),\ J\left(\frac{\tau}{n}\right)\right) = 0.$$

Ora se prendiamo l'equazione modulare

$$f\left(J(\tau),\ J\left(\frac{\tau}{n}\right)\right) = 0$$

e fra le tre equazioni scritte eliminiamo $J(\tau)$, $J\left(\frac{\tau}{n}\right)$, avremo evidentemente una relazione della forma

$$\psi\left(\Phi(\tau),\ \Phi\left(\frac{\tau}{n}\right)\right) = 0,$$

1) Per es. nel caso $p = 2$ noi abbiamo potuto stabilire, studiando la trasformazione di Landen (§ 170), la semplice formola

$$k(\tau) = \frac{1 - \sqrt{1 - k^2\left(\frac{\tau}{2}\right)}}{1 + \sqrt{1 - k^2\left(\frac{\tau}{2}\right)}},$$

che è una forma dell'equazione modulare per $p = 2$. È manifesto che la relazione fra

$$J(\tau) = \frac{4}{27}\,\frac{(1 - k^2 + k^4)^3}{k^4(1 - k^2)^2} \text{ e } J\left(\frac{\tau}{2}\right)$$

è molto più complicata.

essendo ψ una funzione razionale intera (irriducibile) dei suoi due argomenti. Questa si dirà l'equazione modulare per $\Phi(\tau)$.

Consideriamo dunque in particolare la funzione modulare

$$\varphi(\tau) = \sqrt[4]{k}$$

e, supponendo senz'altro p numero primo dispari, ricerchiamo le proprietà dell'equazione modulare

$$\text{(VI)} \qquad f\left(\varphi(\tau),\ \varphi\left(\frac{\tau}{p}\right)\right) = 0,$$

che, ponendo

$$u = \varphi(\tau), \quad v = \varphi\left(\frac{\tau}{p}\right),$$

scriveremo anche

$$\text{(VI*)} \qquad f(u, v) = 0,$$

ndicando con $f(u, v)$ una funzione razionale, intera ed irriducibile dei due argomenti u, v.

Cerchiamo in primo luogo il grado della (VI) in $\varphi\left(\frac{\tau}{p}\right)$, e le sue radici. Per ciò bisogna far descrivere a $\varphi(\tau)$ nel suo piano complesso tutti i possibili cammini chiusi ed osservare quanti e quali valori diversi assume $\varphi\left(\frac{\tau}{p}\right)$. Per far descrivere a $\varphi(\tau)$ un cammino chiuso, bisogna cangiare τ secondo una sostituzione $\frac{\alpha\tau + \beta}{\gamma\tau + \delta}$ del sottogruppo Λ di $\varphi(\tau)$ § 182, e deve essere quindi

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \pmod 2, \quad \alpha\beta + \alpha^2 \equiv 1 \pmod{16}.$$

Il valore nel quale $\varphi\left(\frac{\tau}{p}\right)$ si cangerà con continuità sarà

$$\varphi\left(\frac{1}{p}\,\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right),$$

sicchè è da vedersi quanti valori distinti assume questa espressione percorrendo $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ le sostituzioni del detto sottogruppo Λ. Ora si avrà

$$\varphi\left(\frac{\alpha\tau + \beta}{p\gamma\tau + p\delta}\right) = \varphi\left(\frac{a\tau + b}{c\tau + d}\right),$$

con a, b, c, d numeri interi ed $ad - bc = p$, tutte le volte che si abbia

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ p\gamma, & p\delta \end{pmatrix} \begin{pmatrix} \alpha_1, & \beta_1 \\ \gamma_1, & \delta_1 \end{pmatrix} = \begin{pmatrix} \alpha\alpha_1 + p\gamma\beta_1, & \beta\alpha_1 + p\delta\beta_1 \\ \alpha\gamma_1 + p\gamma\delta_1, & \beta\gamma_1 + p\delta\delta_1 \end{pmatrix},$$

essendo

$$\begin{pmatrix} \alpha_1, & \beta_1 \\ \gamma_1, & \delta_1 \end{pmatrix}$$

un'altra sostituzione di Λ, cioè

$$\begin{pmatrix} \alpha_1, & \beta_1 \\ \gamma_1, & \delta_1 \end{pmatrix} \equiv \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \pmod 2, \quad \alpha_1^2 + \alpha_1\beta_1 \equiv 1 \pmod{16}.$$

Approfittando dell'indeterminazione di $\begin{pmatrix} \alpha_1, & \beta_1 \\ \gamma_1, & \delta_1 \end{pmatrix}$, possiamo ridurre $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ ad una forma normale nel modo seguente:

1º caso. — Supponiamo dapprima che sia

$$\alpha \not\equiv 0 \pmod p;$$

prendasi

$$\gamma_1 = -p\gamma \equiv 0 \pmod 2, \quad \delta_1 = \alpha \equiv 1 \pmod 2,$$

onde risulterà

$$c = \alpha\gamma_1 + p\gamma\delta_1 = 0,$$

indi si determini α_1, β_1 in guisa che sia

$$\alpha_1\delta_1 - \beta_1\gamma_1 = \alpha\alpha_1 + p\gamma\beta_1 = 1$$

e inoltre sia soddisfatta la congruenza

$$\alpha_1^2 + \alpha_1\beta_1 \equiv 1 \pmod{16},$$

ciò che con considerazioni elementari si vede esser sempre possibile [1]). Allora la sostituzione $\begin{pmatrix} \alpha_1, & \beta_1 \\ \gamma_1, & \delta_1 \end{pmatrix}$ appartiene al sottogruppo Λ e si ha

$$\begin{cases} a = \alpha\alpha_1 + p\gamma\beta_1 = 1, & b = \alpha_1\beta + p\delta\beta_1 \\ c = 0, & d = \beta\gamma_1 + p\delta\delta_1 = p, \end{cases}$$

1) Si prenda $\alpha_1 \equiv \alpha \pmod 8$, $\beta_1 \equiv \beta \pmod{16}$.

onde, essendo

$$a^2 + ab \equiv 1 \pmod{16},$$

risulta

$$b \equiv 0 \pmod{16}.$$

Ponendo

$$b = 16\nu,$$

avremo dunque

$$\varphi\left(\frac{1}{p}\,\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \varphi\left(\frac{\tau+16\nu}{p}\right). \tag{9}$$

Osserviamo poi che b, e quindi ν, è perfettamente determinato (mod p), poichè si ha per le precedenti

$$b \equiv \alpha_1\beta \pmod p, \quad \alpha_1\alpha \equiv 1 \pmod p,$$

onde

$$\alpha b \equiv \beta \pmod p,$$

cioè

$$16\alpha\nu \equiv \beta \pmod p.$$

I valori distinti dell'espressione (9) corrispondono ai valori incongrui di ν (mod p) e si ottengono così le p radici dell'equazione modulare (VI)

$$\varphi\left(\frac{\tau}{p}\right), \ \varphi\left(\frac{\tau+16}{p}\right), \ \varphi\left(\frac{\tau+2\cdot 16}{p}\right) \dots \varphi\left(\frac{\tau+16\,(p-1)}{p}\right),$$

corrispondenti all'ipotesi $\alpha \not\equiv 0 \pmod p$.

2º caso. — Sia ora $\alpha \equiv 0 \pmod p$. Allora si può scrivere

$$\varphi\left(\frac{1}{p}\,\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = \varphi\left(\frac{\frac{\alpha}{p}\cdot p\tau+\beta}{\gamma\cdot p\tau+p\delta}\right)$$

e siccome $\begin{pmatrix} \frac{\alpha}{p}, & \beta \\ \gamma, & p\delta \end{pmatrix}$ è una sostituzione $\equiv \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ (mod 2), per le formole (A) § 182, avremo

$$\varphi\left(\frac{1}{p}\,\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = e^{\frac{\pi i}{8}\left(\frac{\alpha^2}{p^2}+\frac{\alpha\beta}{p}-1\right)}\varphi(p\tau).$$

Ma, essendo p impari, si ha

$$p^2 \equiv 1 \pmod 8, \quad p^4 \equiv 1 \pmod{16}$$

e però

$$\frac{\alpha^2}{p^2} + \frac{\alpha\beta}{p} - 1 \equiv p^2(\alpha^2 + p\alpha\beta) - 1 \pmod{16},$$

e siccome, essendo $\beta \equiv 0 \pmod 8$ (§ 182), si ha

$$\alpha^2 + p\alpha\beta = \alpha^2 + \alpha\beta + (p-1)\,\alpha\beta \equiv 1 \pmod{16}$$

ne segue

$$e^{\frac{\pi i}{8}\left(\frac{\alpha^2}{p^2}+\frac{\alpha\beta}{p}-1\right)} = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right).$$

Si conclude quindi che, quando $\alpha \equiv 0 \pmod p$, si ha

$$\varphi\left(\frac{1}{p}\,\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right) = (-1)^{\frac{p^2-1}{8}}\varphi(p\tau),$$

che è una nuova ed ultima radice dell'equazione modulare (VI). Abbiamo così dimostrato il teorema:

L'equazione modulare (VI) *è del grado $p+1$ in $v = \varphi\left(\frac{\tau}{p}\right)$ e le sue $p+1$ radici, per un valore dato di $u = \varphi(\tau)$, sono date dalle espressioni*

$$v_\infty = (-1)^{\frac{p^2-1}{8}}\varphi(p\tau), \quad v_0 = \varphi\left(\frac{\tau}{p}\right), \quad v_1 = \varphi\left(\frac{\tau+16}{p}\right)$$

$$\ldots\ v_r = \varphi\left(\frac{\tau+16r}{p}\right) \ \ldots\ v_{p-1} = \varphi\left(\frac{\tau+16(p-1)}{p}\right).$$

§ 190. — Gruppo di monodromia ed algebrico dell'equazione modulare (VI*) $f(u, v) = 0$.

Dimostriamo ora che *il gruppo di monodromia dell'equazione modulare* (VI*) *è precisamente lo stesso che quello dell'equazione modulare per l' invariante assoluto* (§ 185).

Per fare descrivere ad $u = \varphi(\tau)$, nel suo piano complesso, un cammino chiuso dobbiamo cangiare τ in

$$\frac{\alpha\tau+\beta}{\gamma\tau+\delta},$$

essendo $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ una sostituzione del sottogruppo Λ di $\varphi(\tau)$, cioè

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \equiv \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \pmod 2$$

$$\alpha^2 + \alpha\beta \equiv 1 \pmod{16}.$$

Ora i $p+1$ rami di v

$$v_\infty = (-1)^{\frac{p^2-1}{8}}\varphi(p\tau), \quad v_\nu = \varphi\left(\frac{\tau+16\nu}{p}\right)$$

si permutano fra loro nello stesso modo di

$$j(p\tau), \quad j\left(\frac{\tau+16\nu}{p}\right)$$

e, supposto quindi che v_ν si cangi in $v_{\nu'}$, si avrà per la (5) § 185

$$16\nu' \equiv \frac{\delta \cdot 16\nu + \beta}{\gamma \cdot 16\nu + \alpha} \pmod p \tag{10}$$

che, determinando b dalla congruenza

$$16\,b \equiv \beta \pmod p$$

e ponendo

$$a = \delta, \quad c = 16\gamma, \quad d = \alpha,$$

ha la forma

$$(11) \qquad \nu' \equiv \frac{a\nu + b}{c\nu + d}, \quad ad - bc \equiv 1 \pmod p$$

del gruppo di monodromia per l'invariante assoluto. È poi facile vedere che qualunque sostituzione (11) si trova nel gruppo di monodromia di $f(u, v)$, per il che basta dimostrare che vi si trovano le due elementari

$$\nu' \equiv \nu + 1, \quad \nu' \equiv -\frac{1}{\nu} \pmod p.$$

Ora la prima si ottiene subito, facendo

$$\alpha = 1, \quad \beta = 16, \quad \gamma = 0, \quad \delta = 1,$$

e per la seconda basterà prendere $\alpha, \beta, \gamma, \delta$ per es. in guisa che soddisfino le congruenze

$$\begin{cases} \alpha \equiv 0 \pmod p, \ \beta \equiv 16 \pmod p, \ 16\gamma \equiv -1 \pmod p, \ \delta \equiv 0 \pmod p \\ \alpha \equiv 1 \pmod 8, \ \beta \equiv \ 0 \pmod{16}, \quad \gamma \equiv \ 0 \pmod 2 \end{cases}$$

e l'eguaglianza $\alpha\delta - \beta\gamma = 1$.

A tale scopo prendiamo

$$\alpha = p\alpha', \quad \beta = 16\beta', \quad \gamma = 2\gamma', \quad \delta = p\delta'$$

e dovremo determinare $\alpha', \beta', \gamma', \delta'$, in guisa che soddisfino le congruenze

$$p\alpha' \equiv 1 \pmod 8, \quad \beta' \equiv 1 \pmod p, \quad 32\gamma' \equiv -1 \pmod p$$

e l'eguaglianza

$$(12) \qquad p^2 \alpha' \delta' - 32 \beta' \gamma' = 1$$

che include, a causa di $32\gamma' \equiv -1 \pmod p$, la congruenza $\beta' \equiv 1 \pmod p$. Possiamo scegliere α', γ' in guisa che soddisfino le congruenze superiori

$$p\alpha' \equiv 1 \pmod 8, \quad 32\gamma' \equiv -1 \pmod p$$

e *siano inoltre primi fra loro*, e allora la (12) è risolubile in numeri interi δ', β' c. d. d.

Apparirà dalle ricerche seguenti (§ 191) che anche nell'equazione modulare $f(u, v) = 0$ i coefficienti numerici sono tutti interi, onde si pone la questione quale sia il gruppo algebrico di questa equazione modulare *nel campo dei numeri razionali*. Con considerazioni perfettamente analoghe a quelle del § 188 si dimostra che il gruppo algebrico è ancora il gruppo lineare totale

$$\nu' \equiv \frac{a\nu + b}{c\nu + d} \quad (ad - bc \not\equiv 0 \pmod p)$$

e l'irrazionalità numerica, la cui aggiunta lo abbassa al gruppo di monodromia, è data da $\sqrt{(-1)^{\frac{p-1}{2}} p}$.

§ 191. — **Proprietà della equazione modulare** $f(u, v) = 0$.

Dimostriamo ora alcune proprietà dell'equazione modulare (VI*), che ne faciliteranno la costruzione effettiva.

Scriviamo l'equazione modulare, ordinata per le potenze di v, nel modo seguente:

$$(\text{VII}) \qquad v^{p+1} + B_1 v^p + B_2 v^{p-1} + \dots + B_p v + B_{p+1} = 0,$$

ove le B sono funzioni razionali in u e stabiliamo le successive proprietà:

1ª proprietà. — *I coefficienti B sono polinomi razionali interi in u.*

Per dimostrarlo basta osservare che nessuna delle $p+1$ radici della (VII)

$$v_\infty = (-1)^{\frac{p^2-1}{8}} \varphi(p\tau), \quad v_\nu = \varphi\left(\frac{\tau + 16\nu}{p}\right)$$

può diventare infinita, se tale non diventa anche u. E infatti, per quanto si è visto al § 180, affinchè v_∞ o v_ν diventino infinite bisogna che l'argomento $p\tau$ o $\dfrac{\tau + 16\nu}{p}$ acquisti un valore razionale $\dfrac{a}{b}$

con a, b impari; ma allora anche τ acquista un tale valore, e $u=\varphi(\tau)$ diventa pure infinita.

2ª proprietà. — *L'ultimo coefficiente B_{p+1} dell'equazione modulare è dato da*

$$B_{p+1}=(-1)^{\frac{p^2-1}{8}}u^{p+1}.$$

Si osservi per ciò che le radici della equazione modulare si annullano soltanto quando l'argomento

$$p\tau \quad \text{o} \quad \frac{\tau+16\nu}{p}$$

è un numero razionale della forma $\frac{a}{b}$ con $(a,b)\equiv(1,0) \pmod 2$ (§ 180); ma allora avendo τ la medesima forma, anche u si annulla. Ne segue che $B_{p+1}=A\,u^r$.

Ora si ha

$$B_{p+1}=v_\infty\, v_0\, v_1 \,\ldots\, v_{p-1}=A\,u^r, \tag{13}$$

e per determinare l'esponente r ed il coefficiente A basta sviluppare dall'una parte e dall'altra per potenze di q secondo la formola

$$u=\sqrt{2}\,q^{\frac{1}{8}}(1-q+2q^2-3q^3+\ldots),$$

che ponendo

$$q^{\frac{1}{8}}=Q,$$

si scrive

$$u=\sqrt{2}\,Q\,\{1-Q^8+2Q^{16}-3Q^{24}+\ldots\}. \tag{14}$$

Per gli sviluppi di v_∞, v_ν ne deduciamo quindi

$$\left\{\begin{aligned} v_\infty&=(-1)^{\frac{p^2-1}{8}}\varphi(p\tau)=(-1)^{\frac{p^2-1}{8}}\sqrt{2}\,Q^p(1-Q^{8p}+2Q^{16p}+\ldots)\\ v_\nu&=\varphi\left(\frac{\tau+16\nu}{p}\right)=\varepsilon^\nu\sqrt{2}\,Q^{\frac{1}{p}}\left(1-\varepsilon^{8\nu}Q^{\frac{8}{p}}+2\varepsilon^{16\nu}Q^{\frac{16}{p}}+\ldots\right).\end{aligned}\right. \tag{15}$$

Sostituendo nella (13) e paragonando le potenze più basse di Q ne risulta appunto

$$r=p+1,\quad A=(-1)^{\frac{p^2-1}{8}}.$$

3ª proprietà. — *Ciascun polinomio B_s può porsi sotto la forma*

$$B_s=u^{r_s}A_s(u^8)$$

dove r_s è il minimo resto positivo del prodotto $ps \pmod 8$ e A_s è razionale intero in u^8.

Suppongasi che nel polinomio B_s figuri il termine

$$a\,u^r;$$

questo, sviluppato per potenze di Q, dà per termine colla minima potenza di Q

$$a\,2^{\frac{r}{2}}Q^r$$

e tutte le altre potenze di Q provenienti da quel termine hanno esponenti $\equiv r \pmod 8$.

Ora si ha

$$B_s=(-1)^s\sum v_\infty\, v_0\, v_1\,\ldots\, v_{s-2},$$

la somma essendo estesa alle combinazioni s ad s delle radici $v_\infty, v_0, \ldots, v_{p-1}$. Sostituendo nel secondo membro gli sviluppi (15), tutte le potenze di Q hanno esponenti dell'una o dell'altra delle due forme

$$p+\frac{s-1}{p}+8kp+\frac{8k'}{p},\quad \frac{s+8k}{p}\quad (\text{con } k,\,k' \text{ interi}),$$

e dovendo queste potenze trovare le loro equivalenti negli sviluppi dei vari termini $a\,u^r$ di B_s, nè potendo darsi che per gli sviluppi di due o più di tali termini si elidano completamente le potenze di Q, si avrà necessariamente una delle due congruenze:

$$pr\equiv p^2+s-1,\ \text{ovvero}\ pr\equiv s \pmod 8,$$

cioè in ogni caso, poichè $p^2 \equiv 1 \pmod 8$

$$r \equiv p\,s \pmod 8,$$

e però

$$r = r_s + 8m \quad (m \text{ intero}).$$

4ª proprietà. — *L'equazione modulare non muta, cangiando rispettivamente* u, v *in* $v, (-1)^{\frac{p^2-1}{8}} u$.

Si ha invero identicamente

$$f\left(\varphi(\tau),\ (-1)^{\frac{p^2-1}{8}} \varphi(p\tau)\right) = 0$$

e quindi anche

$$f\left(\varphi\left(\frac{\tau}{p}\right),\ (-1)^{\frac{p^2-1}{8}} \varphi(\tau)\right) = 0;$$

dunque l'equazione

$$f\left(v,\ (-1)^{\frac{p^2-1}{8}} u\right) = 0$$

ha a comune colla $f(u,v)=0$, che è irriducibile, la radice v_0 e però le due equazioni, salvo il segno $(-1)^{\frac{p^2-1}{8}}$, coincidono. Si rileva di qui in particolare che l'equazione (VII) è del grado $p+1$ in u, come in v, e i coefficienti B salgono *al massimo* al grado p in u.

5ª proprietà. — *L'equazione modulare non muta, cangiando* u, v *rispettivamente in* $\frac{1}{u}, \frac{1}{v}$, e *moltiplicando l'equazione per*

$$(-1)^{\frac{p^2-1}{8}} u^{p+1} v^{p+1}.$$

Dall' identità

$$f\left(\varphi(\tau),\ \varphi\left(\frac{\tau}{p}\right)\right) = 0,$$

cangiando τ in $\frac{\tau}{\tau+1}$, coll'osservare che si ha (pag. 253, (A))

$$\varphi\left(\frac{\tau}{\tau+1}\right) = \frac{1}{\varphi(\tau)},\quad \varphi\left(\frac{\tau}{p(\tau+1)}\right) = \varphi\left(\frac{\frac{\tau}{p}}{p\cdot\frac{\tau}{p}+1}\right) = \frac{1}{\varphi\left(\frac{\tau}{p}\right)},$$

risulta

$$f\left(\frac{1}{\varphi(\tau)},\ \frac{1}{\varphi\left(\frac{\tau}{p}\right)}\right) = 0,$$

onde

$$(-1)^{\frac{p^2-1}{8}} u^{p+1} v^{p+1} \cdot f\left(\frac{1}{u}, \frac{1}{v}\right)$$

deve coincidere con $f(u,v)$.

6ª proprietà. — *Se nell'equazione modulare si pone* $u = 1$, *una delle radici diventa eguale a* $+1$ *e le rimanenti* p *a* $(-1)^{\frac{p^2-1}{8}}$.

Pongasi $\tau = -\frac{1}{\tau_1}$ e si avrà

$$u = \varphi(\tau) = \psi(\tau_1);$$

facendo crescere τ_1, per valori puramente immaginari, all'infinito la u convergerà appunto verso $+1$. Ora abbiamo

$$v_\infty = (-1)^{\frac{p^2-1}{8}} \varphi\left(-\frac{p}{\tau_1}\right) = (-1)^{\frac{p^2-1}{8}} \psi\left(\frac{\tau_1}{p}\right)$$

$$v_0 = \varphi\left(-\frac{1}{p\tau_1}\right) = \psi(p\tau_1),$$

onde v_∞, v_0 convergono rispettivamente verso

$$(-1)^{\frac{p^2-1}{8}},\ +1.$$

Per ogni altra radice v_ν si ha

$$v_\nu = \varphi\left(\frac{16\nu\tau_1 - 1}{p\tau_1}\right);$$

e se prendiamo due numeri interi a, c tali che sia

$$16\nu a - pc = 1,$$

avremo

$$\frac{16\nu\tau_1 - 1}{p\tau_1} = \frac{c + 16\nu\frac{\tau_1 - a}{p}}{a + p\frac{\tau_1 - a}{p}}.$$

Facendo inoltre $a \equiv 0 \pmod{16}$

$$a = 16\nu_1,$$

avremo secondo la tabella (A), pag. 253:

$$v_\nu = \varphi\left(\frac{16\nu\tau_1 - 1}{p\tau_1}\right) = e^{\frac{\pi i}{8}(c^2-1)}\psi\left(\frac{\tau_1 - a}{p}\right),$$

il che dimostra che v_ν converge verso $(-1)^{\frac{c^2-1}{8}}$ ovvero, essendo $pc \equiv -1 \pmod{16}$, verso $(-1)^{\frac{p^2-1}{8}}$, c. d. d.

7ª proprietà. — *Nell'equazione modulare figura il termine $a\,u\,v$, col coefficiente* $a = -2^{\frac{p-1}{2}}$.

Se nel primo membro della equazione modulare (VIII)

$$v^{p+1} + B_1 v^p + \dots B_p v + (-1)^{\frac{p^2-1}{8}} u^{p+1} = 0$$

sostituiamo per u, v gli sviluppi (14), (15)

$$u = \sqrt{2}\,Q(1 - 2Q^8 + \dots),$$
$$v = (-1)^{\frac{p^2-1}{8}}\sqrt{2}\,Q^p(1 - 2Q^{8p} + \dots),$$

debbono annullarsi i varî coefficienti delle potenze di Q. Ma l'ultimo termine porta la potenza

$$(-1)^{\frac{p^2-1}{8}}(\sqrt{2})^{p+1}Q^{p+1}$$

e questa potenza minima Q^{p+1} non è portata da alcun altro termine salvo da

$$a\,u\,v = (-1)^{\frac{p^2-1}{8}} a(\sqrt{2})^2 Q^{p+1} + \dots,$$

onde si trae appunto

$$a = -2^{\frac{p-1}{2}}.$$

Per la quinta proprietà, segue che nell'equazione modulare il termine $u^p v^p$ vi figura col coefficiente

$$-(-1)^{\frac{p^2-1}{8}}2^{\frac{p-1}{2}}.$$

§ 192. — Le equazioni modulari per $p = 3, 5, 7, 11$.

Le proprietà ora stabilite per l'equazione modulare bastano già a costruire effettivamente queste equazioni nei casi

$$p = 3, 5, 7, 11.$$

a) Per $p = 3$ l'equazione modulare, in forza della terza proprietà e della prima, sarà

$$v^4 + a u^3 v^3 + b u v - u^4 = 0$$

e per la settima $a = 2, b = -2$, onde si ha

$$v^4 + 2u^3v^3 - 2uv - u^4 = 0. \qquad (a)$$

Si può dare a questa equazione modulare una notevole forma irrazionale (Legendre). Se la scriviamo sotto le due forme

$$(1 - u^4)(1 + v^4) = 1 - u^4v^4 + 2uv(1 - u^2v^2)$$
$$(1 + u^4)(1 - v^4) = 1 - u^4v^4 - 2uv(1 - u^2v^2),$$

moltiplicando otteniamo

$$(1 - u^8)(1 - v^8) = (1 - u^2v^2)^4$$

e ponendo

$$u^4 = k, \quad v^4 = \lambda, \quad 1 - u^8 = k'^2, \quad 1 - v^8 = \lambda'^2,$$

si può scrivere quindi

$$\sqrt{k\lambda} + \sqrt{k'\lambda'} = 1, \tag{a^*}$$

che è la forma di Legendre.

b) Sia $p = 5$. — L'equazione modulare, per la terza e quinta proprietà, sarà:

$$v^6 + a u^5 v^5 + b u^2 v^4 - b u^4 v^2 - a u v - u^6 = 0$$

e dalla settima avremo $a = 4$, indi dalla sesta

$$v^6 + 4 v^5 + b v^4 - b v^2 - 4 v - 1 = (v - 1)\ (v + 1)^5,$$

onde $b = 5$ e però

$$v^6 - u^6 - 4 u v (1 - u^4 v^4) + 5 u^2 v^2 (v^2 - u^2) = 0. \tag{b}$$

c) Sia $p = 7$. — L'equazione modulare sarà

$$\begin{aligned} v^8 + u^8 + a (u^7 v^7 + u v) + b (u^6 v^6 + u^2 v^2) + \\ + c (u^5 v^5 + u^3 v^3) + d u^4 v^4 = 0, \end{aligned}$$

e per la sesta proprietà avremo

$$v^8 + a v^7 + b v^6 + c v^5 + d v^4 + c v^3 + b v^2 + a v + 1 = (v - 1)^8,$$

da cui

$$a = -8, \quad b = 28, \quad c = -56, \quad d = 70$$

e però

$$\begin{aligned} v^8 - 8 u^7 v^7 + 28 u^6 v^6 - 56 u^5 v^5 + 70 u^4 v^4 - 56 u^3 v^3 + \\ + 28 u^2 v^2 - 8 u v + u^8 = 0. \end{aligned} \tag{c}$$

Questa si può scrivere anche

$$(1 - u^8)\ (1 - v^8) = (1 - u v)^8$$

e dà luogo alla forma irrazionale di Gutzlaff

$$\sqrt[4]{k\lambda} + \sqrt[4]{k'\lambda'} = 1. \tag{c^*}$$

d) Sia in fine $p = 11$. — Per le proprietà 3ª, 4ª e 5ª, l'equazione modulare ha la forma seguente:

$$\begin{aligned} v^{12} + u^3 (a + 2^5 u^8) v^{11} + b u^6 v^{10} + u (-a + d u^8) v^9 + e u^4 v^8 + \\ + f u^7 v^7 + b u^2 (1 - u^8) v^6 - f u^5 v^5 - e u^8 v^4 + \\ + u^3 (-d + a u^8) v^3 - b u^6 v^2 - u (2^5 + a u^8) v - u^{12} = 0. \end{aligned}$$

I coefficienti costanti a, b, d, e, f si determinano subito dalla sesta proprietà, secondo la quale, per $u = 1$, deve il primo membro ridursi a $(v - 1)\ (v + 1)^{11}$. Si trova così

$$a = -22, \quad b = 44, \quad d = 88, \quad e = 165, \quad f = 132.$$

Osservazioni circa il caso generale. — Nei casi superiori non bastano più le proprietà dell'equazione modulare, descritte al § 191, per determinare completamente i valori numerici dei coefficienti. In tutti i casi però ci potremo servire del metodo seguente. Scriviamo l'equazione modulare sotto la forma

$$\begin{aligned} v^{p+1} + (-1)^{\frac{p^2-1}{8}} u^{p+1} - (-1)^{\frac{p^2-1}{8}} . \, 2^{\frac{p-1}{2}} u^p v^p - 2^{\frac{p-1}{2}} u v = \\ = \sum_{r,s}^{0 \ldots p} c_{rs} u^r v^s \quad (c_{11} = 0, \ c_{pp} = 0). \end{aligned} \tag{VII*}$$

Essa dovrà risultare identicamente soddisfatta, quando per u, v si pongano rispettivamente gli sviluppi

$$\left\{ \begin{aligned} u &= \sqrt{2}\,Q\,(1 - Q^8 + 2 Q^{16} + \ldots) \\ v &= (-1)^{\frac{p^2-1}{8}} \sqrt{2}\,Q^p\,(1 - Q^{8p} + 2 Q^{16p} + \ldots), \end{aligned} \right.$$

talchè i coefficienti delle varie potenze di Q dovranno eguagliarsi dall'una parte e dall'altra. Ora il termine del secondo membro

$$c_{rs} u^r v^s$$

porta come minima potenza di Q

$$Q^{ps+r},$$

col coefficiente

$$(-1)^{\frac{p^2-1}{8}} (\sqrt{2})^{r+s},$$

e queste minime potenze sono tutte differenti pei vari termini. Inoltre per la quinta proprietà si ha, salvo il segno,

$$c_{rs} = c_{p+1-r,\ p+1-s},$$

onde basta limitarsi a quei valori degli indici r, s pei quali $r + s \leq p + 1$. Ma allora, poichè nel primo membro tutti i coefficienti sono interi e contengono $2^{\frac{p+1}{2}}$, mentre $r + s \leq p + 1$ è in ogni caso pari [1]), si conclude: *Tutti i coefficienti* c_{rs} *nell'equazione modulare* (VII*) *sono numeri interi*. In modo analogo a quello tenuto al § 187, si potrebbe dimostrare ulteriormente che tutti questi coefficienti interi c_{rs} sono divisibili per p.

§ 193. — Abbassamento della equazione di sesto grado (Notizie storiche).

Galois scoperse e lasciò enunciata una celebre proposizione relativa all'abbassamento delle equazioni modulari per $p = 5, 7, 11$. Queste equazioni, dei rispettivi gradi 6, 8, 12, posseggono risolventi di un grado inferiore $= p$. L'esistenza di queste risolventi è dovuta al fatto che il gruppo di monodromia:

$$(\alpha) \qquad \nu' \equiv \frac{a\nu + b}{c\nu + d}, \quad ad - bc \equiv 1 \pmod{p}$$

di $\frac{p(p^2-1)}{2}$ sostituzioni contiene, nei detti casi $p = 5, 7, 11$, sottogruppi d'indice p, ciò che non ha più luogo nei casi superiori. La prima dimostrazione del teorema fu data dal Betti [2]). Sol-

1) Ciò segue dalla terza proprietà, secondo la quale si ha $r \equiv (p + 1 - s)p \pmod{8}$, indi

$$r + s \equiv 0 \pmod{2}.$$

2) *Annali* di TORTOLINI, vol. III (1853).

tanto in epoca molto più recente (1881) fu trattata e completamente risoluta dal Gierster [1]) la questione di determinare *tutti* i sottogruppi del gruppo (α) e fu così spiegata l'intima ragione per la quale differiscono i casi $p = 5, 7, 11$ dai superiori.

Riconosciuta la possibilità d'abbassamento delle equazioni modulari nei casi indicati, restava da calcolare effettivamente le risolventi che la teoria indicava.

Hermite per il primo, in una celebre memoria del 1858 [2]), costruì effettivamente una particolare risolvente di quinto grado dell'equazione modulare di sesto e riconobbe che a questa particolare forma poteva ridursi, risolvendo soltanto equazioni ausiliarie di secondo e terzo grado, *la più generale equazione di quinto grado*. Con ciò fu ottenuta la risoluzione per funzioni ellittiche (modulari) della equazione generale di quinto grado. Il metodo di Hermite venne perfezionato e trasformato nel seguito specialmente per le ricerche di Kronecker e Brioschi; e in particolare si vide che la risoluzione dell'equazione ausiliaria di terzo grado si poteva evitare, costruendo altre più convenienti risolventi di quinto grado dell'equazione modulare.

Noi ci contenteremo qui di esporre il primo metodo di Hermite e rimanderemo per la teoria generale della risoluzione dell'equazione di quinto grado ai lavori originali di Hermite stesso, Kronecker, Brioschi e in particolare al libro del Klein: *Vorlesungen über das Ikosaeder*, ove la intera teoria è esposta sistematicamente in modo nuovo ed originale.

Per noi si tratta qui in primo luogo, ricorrendo a note proposizioni della teoria dei gruppi, di riconoscere che il gruppo di monodromia dell'equazione modulare di sesto grado, rappresentato dalla formola

$$\nu' \equiv \frac{a\nu + b}{c\nu + d} \quad ad - bc \equiv 1 \pmod{5},$$

possiede in effetto sottogruppi d'indice 5 e però esistono risolventi di quinto grado dell'equazione modulare. Il detto gruppo è infatti semplice e di ordine 60, e per ciò oloedricamente isomorfo col gruppo delle 60 rotazioni dell'icosaedro, ovvero col gruppo

1) *Math. Annalen*, Bd. 18.

2) *Comptes Rendus*, tomo 46: *Sur la résolution de l'équation du cinquième degré.*

alterno su 5 lettere. Ora il gruppo dell'icosaedro contiene cinque sottogruppi tetraedrali d'ordine 12, e quindi d'indice $= 5$, ai quali nel gruppo alterno su 5 lettere corrispondono i gruppi alterni su quattro sole delle lettere. Definiamo uno dei cinque detti sottogruppi Γ_{12} del gruppo di monodromia, dando le due sostituzioni elementari di un Γ_{12}

$$\nu' \equiv \frac{1}{\nu}\,, \quad \nu' \equiv \frac{\nu+2}{\nu+3} \pmod 5, \tag{16}$$

che composte fra loro e colle loro potenze dànno appunto luogo a 12 sole sostituzioni distinte, come subito si verifica.

Prendiamo ora una funzione razionale delle 6 radici

$$v_\infty\,,\ v_0\,,\ v_1\,,\ v_2\,,\ v_3\,,\ v_4$$

dell'equazione modulare, che rimanga invariata per le due sostituzioni elementari (16), cioè per le due

$$(v_0\, v_\infty)\ (v_1\, v_4),\ (v_0\, v_4\, v_3)\ (v_\infty\, v_1\, v_2).$$

Una tale funzione è semplicemente la seguente

$$z_0 = (v_\infty - v_0)\ (v_1 - v_4)\ (v_2 - v_3)\ ;$$

essa per tutte le sostituzioni del gruppo modulare assume i 5 valori distinti

$$\left\{\begin{array}{l} z_0 = (v_\infty - v_0)\ (v_1 - v_4)\ (v_2 - v_3),\ \ z_1 = (v_\infty - v_1)\ (v_2 - v_0)\ (v_3 - v_4) \\ z_2 = (v_\infty - v_2)\ (v_3 - v_1)\ (v_4 - v_3),\ \ z_3 = (v_\infty - v_3)\ (v_4 - v_2)\ (v_0 - v_1) \\ \qquad\qquad z_4 = (v_\infty - v_4)\ (v_0 - v_3)\ (v_1 - v_2), \end{array}\right. \tag{17}$$

che possono compendiarsi nell'unica formola

$$z_\lambda = (v_\infty - v_\lambda)\ (v_{1+\lambda} - v_{4+\lambda})\ (v_{2+\lambda} - v_{3+\lambda})$$
$$\lambda = 0,\ 1,\ 2,\ 3,\ 4.$$

Le sostituzioni elementari

$$\nu' \equiv \nu + 1,\ \ \nu' \equiv -\frac{1}{\nu} \pmod 5$$

del gruppo modulare permutano fra loro questi cinque valori, e precisamente la prima produce la sostituzione ciclica del quinto ordine $(z_0\, z_1\, z_2\, z_3\, z_4)$ e la seconda il prodotto di due trasposizioni

$$(z_1\, z_2)\ \ (z_3\, z_4),$$

colle quali sostituzioni elementari si genera tutto il gruppo alterno sulle cinque z.

Se ne conclude: *I cinque valori* (17) *sono radici di una risolvente di quinto grado dell'equazione modulare; il gruppo di questa risolvente è il gruppo alterno sulle cinque radici.*

§ 194. — Costruzione effettiva della risolvente di Hermite.

Per costruire effettivamente la risolvente di Hermite, cominciamo dall'osservare che se nell'equazione modulare

$$v^6 + 4\,u^5 v^5 + 5\,u^2 v^4 - 5\,u^4 v^2 - 4\,u\,v - u^6 = 0$$

si pone

$$w = \frac{v}{u^5}\,,$$

la nuova equazione in w ha coefficienti razionali (non interi) in u^8; e posto quindi

$$W_\lambda = (w_\infty - w_\lambda)\ (w_{1+\lambda} - w_{4+\lambda})\ (w_{2+\lambda} - w_{3+\lambda})$$
$$\lambda = 0,\ 1,\ 2,\ 3,\ 4,$$

le 5 quantità W_λ sono radici di una risolvente di quinto grado

$$W^5 + a_1\ W^4 + a_2\ W^3 + a_3\ W^2 + a_4\ W + a_5 = 0,$$

con coefficienti razionali in u^8, e poichè si ha

$$z_\lambda = u^{15}\, W_\lambda\,,$$

la risolvente di quinto grado in z avrà la forma

$$z^5 + B_1 u^7 z^4 + B_2 u^6 z^3 + B_3 u^5 z^2 + B_4 u^4 z + B_5 u^3 = 0, \tag{18}$$

dove i coefficienti B sono funzioni razionali di u^8. Ora, siccome per valori finiti di u le sei v_ν, e quindi anche le cinque z_λ, sono finite, vediamo che *le B sono polinomii razionali interi in u^8.*

Per la quinta proprietà dell'equazione modulare (§ 191), se si cangia τ in $\frac{\tau}{\tau+1}$, u si cangia in $\frac{1}{u}$ e le radici v_ν nelle loro inverse $\frac{1}{v_{\nu'}}$, salvo l'ordine. Ma vediamo subito come dipende ν' da ν, osservando che per la medesima sostituzione $\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ eseguita su τ deve J_ν cangiarsi in $J_{\nu'}$ [1]) e si ha quindi

$$\nu' \equiv \frac{\nu}{\nu+1} \pmod 5,$$

onde

$$v_\infty,\ v_0,\ v_1,\ v_2,\ v_3,\ v_4$$

si muteranno rispettivamente in

$$\frac{1}{v_1},\ \frac{1}{v_0},\ \frac{1}{v_3},\ \frac{1}{v_4},\ \frac{1}{v_2},\ \frac{1}{v_\infty}$$

e quindi z_0 in

$$\frac{-z_3}{v_\infty v_0 v_1 v_2 v_3 v_4} = \frac{z_3}{u^6}.$$

Dunque la risolvente (18), che è irriducibile, deve rimanere invariata quando vi si cangi u, z rispettivamente in $\frac{1}{u}$, $\frac{z}{u^6}$ e si moltiplichi tutta l'equazione per u^{30}, il che dà:

$$z^5 + u^{-1} B_1\left(\frac{1}{u}\right) z^4 + u^6 B_2\left(\frac{1}{u}\right) z^3 + u^{13} B_3\left(\frac{1}{u}\right) z^2 + u^{20} B^4\left(\frac{1}{u}\right) z + $$
$$+ u^{27} B_5\left(\frac{1}{u}\right) = 0,$$

[1]) Si osservi che $J\left(\frac{\tau+16\nu}{5}\right) = J\left(\frac{\tau+\nu}{5}\right) = J_\nu$.

e paragonando colla (18), si ottiene

$$B_1\left(\frac{1}{u}\right) = u^8 B_1(u),\quad B_2\left(\frac{1}{u}\right) = B_2(u),\quad u^8 B_3\left(\frac{1}{u}\right) = B_3(u)$$
$$u^{16} B_4\left(\frac{1}{u}\right) = B_4(u),\ u^{24} B_5\left(\frac{1}{u}\right) = B_5(u).$$

Queste dimostrano che si ha $B_1 = 0$, B_2 costante, mentre B_3, B_4, B_5 sono polinomî reciproci dei rispettivi gradi 1, 2, 3 in u^8. Dunque la (18) avrà la forma

$$z^5 + a u^6 z^3 + b u^5 (1 + u^8) z^2 + c u^4 (1 + d u^8 + u^{16}) z +$$
$$+ e u^3 (1 + f u^8 + f u^{16} + u^{24}) = 0,$$

essendo a, b, c, d, e, f costanti numeriche.

Ora per $u = 1$ tutte cinque le radici z si annullano (§ 191, 2ª) e quindi anche tutti i coefficienti, dopo il primo, della (18).

Se ne trae subito

$$a = 0,\quad b = 0,\quad d = -2,\quad f = -1$$

onde l'equazione diventa

$$z^5 + c u^4 (1 - u^8)^2 \cdot z + e u^3 (1 - u^8)^2 (1 + u^8) = 0 \tag{18*}$$

e resteranno solo da determinarsi le due costanti c, e. Per ciò serviamoci degli sviluppi (14), (15), § 192:

$$\begin{aligned}
u &= \sqrt{2}\, Q\ (1 - Q^8 + 2Q^{16} + \ldots.)\\
v_\infty &= -\sqrt{2}\, Q^5\ (1 - Q^{40} + 2Q^{80} + \ldots.)\\
v_0 &= \sqrt{2}\, Q^{\frac{1}{5}}\ (1 - Q^{\frac{8}{5}} + \ldots.)\\
v_1 &= \varepsilon \sqrt{2}\, Q^{\frac{1}{5}}\ (1 - \varepsilon^3 Q^{\frac{8}{5}} + \ldots.)\\
v_2 &= \varepsilon^2 \sqrt{2}\, Q^{\frac{1}{5}}\ (1 - \varepsilon\, Q^{\frac{8}{5}} + \ldots.)\\
v_3 &= \varepsilon^3 \sqrt{2}\, Q^{\frac{1}{5}}\ (1 - \varepsilon^4 Q^{\frac{8}{5}} + \ldots.)\\
v_4 &= \varepsilon^4 \sqrt{2}\, Q^{\frac{1}{5}}\ (1 - \varepsilon^2 Q^{\frac{8}{5}} + \ldots.),
\end{aligned}$$

avendo posto

$$\varepsilon = e^{\frac{2\pi i}{5}}.$$

Se si osserva che si ha

$$(\varepsilon - \varepsilon^4)\ (\varepsilon^2 - \varepsilon^3) = -\sqrt{5},$$

ne risulta per z_0 lo sviluppo

$$z_0 = 2^{\frac{3}{2}} \sqrt{5}\, Q^{\frac{3}{5}} (1 - Q^{\frac{8}{5}} + \ldots.)\ (2 + Q^{\frac{8}{5}} + \ldots.)\ (1 + Q^{\frac{8}{5}} + \ldots.),$$

ossia

$$z_0 = 2^{\frac{3}{2}} \sqrt{5}\, Q^{\frac{3}{5}} (1 + Q^{\frac{8}{5}} + \ldots.),$$

le potenze di $Q^{\frac{1}{5}}$ trascurate entro parentesi essendo la 16ª, 24ª ecc.

Sostituendo nella (18*), col tener conto soltanto delle due più basse potenze di Q che vi compariscono, che sono

$$Q^3,\ Q^{\frac{23}{5}},$$

avremo l'identità

$$2^{\frac{15}{2}} 5^2 \sqrt{5}\, Q^3 (1 + 5\, Q^{\frac{8}{5}} + \ldots.) + 2^{\frac{7}{2}} \sqrt{5}\, c\, .\, Q^{\frac{23}{5}} + \ldots. + 2^{\frac{3}{2}} e\, Q^3 + \ldots. = 0,$$

onde si trae

$$c = -2^4\, 5^3,\quad e = -2^6\, 5^2 \sqrt{5}.$$

Abbiamo dunque per la forma definitiva della risolvente di Hermite:

$$\text{(VIII)}\qquad z^5 - 2^4\, 5^3\, u^4 (1 - u^8)^2 z - 2^6\, 5^2 \sqrt{5}\, u^3 (1 - u^8)^2 (1 + u^8) = 0.$$

Colla trasformazione

$$z = \sqrt[4]{2^4\, .\, 5^3\, .\, u^4 (1 - u^8)^2}\, .\, y,$$

cioè

$$z = 2 \sqrt[4]{5^3}\, u \sqrt{1 - u^8}\, .\, y,$$

essa diventa:

$$\text{(VIII*)}\qquad y^5 - y - A = 0,$$

dove si è posto

$$A = \frac{2}{\sqrt[4]{5^5}} \frac{1 + u^8}{u^2 \sqrt{1 - u^8}} = \frac{2}{\sqrt[4]{5^5}} \frac{1 + k^2}{\sqrt{k(1 - k^2)}}.$$

Ora Bring, e successivamente Jerrard, hanno dimostrato che ogni equazione di quinto grado può ridursi, con trasformazioni di Tschirnhaus, risolvendo soltanto equazioni di secondo e terzo grado, alla forma (VIII*). Dopo di ciò, se determiniamo il modulo k dalla equazione di quarto grado

$$\frac{(1 + k^2)^2}{k\,(1 - k^2)} = \frac{5^2 \sqrt{5}}{4} A^2,$$

cioè

$$k^4 + \frac{5^2 \sqrt{5}}{4} A^2 k^3 + 2\, k^2 - \frac{5^2 \sqrt{5}}{4} A^2 k + 1 = 0,$$

che ponendo

$$\mu = k - \frac{1}{k},$$

si riduce alle due successive di secondo grado

$$\begin{cases} \mu^2 + \dfrac{5^2 \sqrt{5}}{4} A^2 \mu + 4 = 0 \\ k^2 - \mu\, k - 1 = 0, \end{cases}$$

avremo ridotto l'equazione generale di quinto grado alla forma di una risolvente di Hermite e le sue radici si esprimeranno per funzioni ellittiche (modulari). La risoluzione dell'equazione di quinto grado è così ridotta alla divisione (o moltiplicazione) per 5 dell'argomento della funzione modulare $\varphi(\tau)$, in modo analogo come si ottiene la risoluzione trigonometrica dell'equazione di terzo grado, riducendola alla trisezione dell'argomento nelle funzioni circolari.

CAPITOLO XVIII.

Principî della teoria delle funzioni ellittiche a moltiplicazione complessa.

§ 195. — Definizione delle funzioni ellittiche a moltiplicazione complessa e formole fondamentali.

Nei capitoli precedenti abbiamo studiato quelle proprietà generali delle funzioni ellittiche, e in particolare della $\wp(u \mid \omega, \omega')$ che convengono a tutte le funzioni ellittiche, comunque siano assegnati i valori particolari 2ω, $2\omega'$ dei periodi. Ma vi ha un'importante classe di funzioni ellittiche che, per la natura speciale dei loro periodi (o meglio del loro rapporto $\tau = \dfrac{\omega'}{\omega}$), vengono inoltre a godere di singolari proprietà speciali. È questa la classe delle funzioni ellittiche *a moltiplicazione complessa*, che per primo Abel considerò, lasciando enunciate alcune loro proprietà fondamentali.

Per opera specialmente di Kronecker, e per le ricerche successive di altri matematici (Hermite, Stuart, Pick, Weber, Greenhill ecc.), fu costruita la teoria di questa speciale classe di funzioni ellittiche. Le singolari proprietà aritmetiche di queste particolari funzioni ellittiche, e specialmente la loro intima relazione colla teoria delle forme binarie quadratiche secondo Gauss, dànno un particolare interesse allo studio di questo ramo nella moderna teoria delle funzioni ellittiche.

Qui noi ci proponiamo soltanto di far conoscere i principî fondamentali della indicata teoria e nella esposizione ci atterrèmo particolarmente alle memorie di Halphen [1]) e Sylow [2]) e all'opera di Weber [3]).

[1]) *Sur la multiplication complèxe des fonctions elliptiques*, in « Journal de Mathèm. », 1889, tomo V.

[2]) Id., in « Journal de Mathèm. », 1887, tomo III.

[3]) *Elliptische Funtionen und algebraische Zahlen*, Braunschweig, Wieweg., 1891.

Perveniamo direttamente alla speciale classe di funzioni ellittiche, che deve ora formare l'oggetto del nostro studio, proponendoci il problema seguente: *Per quali funzioni ellittiche $\wp(u \mid \omega, \omega')$ accade che $\wp(\varepsilon u)$, essendo ε un conveniente fattore costante (moltiplicatore), si esprima razionalmente per $\wp u$?*

Sappiamo che ciò accade per qualunque funzione ellittica $\wp u$, se il moltiplicatore ε è un numero reale intero; ed ora si tratta appunto di vedere se può accadere in altri casi. Siccome, per la formola di omogeneità, si ha

$$\wp(\varepsilon u \mid \omega, \omega') = \frac{1}{\varepsilon^2}\, \wp\left(u \,\Big|\, \frac{\omega}{\varepsilon}, \frac{\omega'}{\varepsilon}\right),$$

dai principî della teoria della trasformazione (§ 161) risulta che, supposto $\wp(\varepsilon u)$ funzione razionale di $\wp u$, dovranno sussistere relazioni della forma

$$\text{(I)} \qquad \left\{\begin{aligned} \omega &= a\frac{\omega}{\varepsilon} + b\frac{\omega'}{\varepsilon} \\ \omega' &= c\frac{\omega}{\varepsilon} + d\frac{\omega'}{\varepsilon}, \end{aligned}\right.$$

dove a, b, c, d sono numeri interi e

$$ad - bc = N > 0.$$

Inversamente, se sono soddisfatte relazioni fondamentali della forma (I), sarà $\wp(\varepsilon u)$ una funzione razionale di grado N della $\wp u$. Possiamo scrivere le (I) anche così:

$$\text{(I*)} \qquad \begin{aligned} (a-\varepsilon)\,\omega + \quad b\,\omega' &= 0 \\ c\,\omega \quad + (d-\varepsilon)\,\omega' &= 0, \end{aligned}$$

dalle quali risulta che due casi soli possono presentarsi e cioè:

1° Le (I*) sono identità e però

$$a = d = \varepsilon, \quad b = c = 0,$$

e si hanno allora le formole di ordinaria moltiplicazione, che valgono qualunque siano i periodi.

2° Se le (I) o (I*) non sono identiche, eliminando ε si ha

$$(a\,\omega + b\,\omega')\,\omega' = (c\,\omega + d\,\omega')\,\omega,$$

ossia, ponendo come al solito

$$\tau = \frac{\omega'}{\omega},$$

$$\text{(II)} \qquad b\,\tau^2 + (a - d)\,\tau - c = 0.$$

Eliminando invece $\dfrac{\omega'}{\omega}$ dalle (I*), abbiamo per ε l'equazione di secondo grado

$$\begin{vmatrix} a - \varepsilon & b \\ c & d - \varepsilon \end{vmatrix} = 0,$$

cioè

$$\text{(II*)} \qquad \varepsilon^2 - (a + d)\,\varepsilon + (a\,d - b\,c) = 0.$$

Il discriminante comune

$$\Delta = (a + d)^2 - 4\,(a\,d - b\,c) = (a + d)^2 - 4\,N$$

delle (II), (II*) deve essere negativo, poichè τ è complesso (col coefficiente dell' immaginario positivo), e per ciò il moltiplicatore ε è un numero complesso della forma

$$\varepsilon = \frac{1}{2}\,(a + d + i\sqrt{-\Delta}).$$

Inversamente, se il rapporto τ dei periodi di una funzione ellittica $\wp\,u$ è radice di un'equazione di secondo grado a coefficienti interi e a determinante negativo

$$\text{(1)} \qquad P\,\tau^2 + Q\,\tau + R = 0,$$

ponendo per es. nelle (I)

$$b = P, \quad a - d = Q, \quad c = -R$$

$$\text{(2)} \qquad \varepsilon = \frac{1}{2}\left\{a + d + i\sqrt{-\Delta}\right\},$$

vediamo che $\wp\,(\varepsilon\,u)$ si esprimerà per una funzione razionale di $\wp\,u$ di grado

$$N = a\,d - b\,c.$$

Dunque: *Condizione necessaria e sufficiente perchè $\wp\,(\varepsilon\,u)$ sia funzione razionale di $\wp\,u$, senza che ε sia un intero reale, è che il rapporto τ dei periodi sia radice di un'equazione* (I) *a coefficienti interi e a determinante negativo. Allora il moltiplicatore ε è un numero complesso della forma* (2).

Di qui appunto l'origine del nome di *moltiplicazione complessa*.

Ora notiamo che ci potremo restringere al caso in cui i quattro interi a, b, c, d nelle (I) non hanno alcun divisore comune (eccetto la unità); poichè, se σ è il loro massimo comun divisore e si pone $\varepsilon = \sigma\,\varepsilon_1$, si vede dalle (I) che già

$$\wp\,(\varepsilon_1\,u)$$

si esprimerà razionalmente per $\wp\,u$, e successivamente si avrà

$$\wp\,(\varepsilon\,u) = \wp\,(\sigma\,.\,\varepsilon_1\,u)$$

colle ordinarie formole di moltiplicazione pel numero σ. Potremo dunque limitarci al caso in cui a, b, c, d sono primi fra loro, cioè al caso delle moltiplicazioni complesse *primitive* (Cfr. § 164).

§ 196. — Corrispondenza fra le funzioni $\wp\,u$ a moltiplicazione complessa e le classi delle forme binarie quadratiche. Moltiplicazioni elementari.

Se $\wp\,(u \mid \omega, \omega')$ è una funzione ellittica a moltiplicazione complessa, fra ω, ω' avremo una relazione quadratica della forma

$$A\,\omega'^2 + 2\,B\,\omega\,\omega' + C\,\omega^2 = 0,$$

dove A, B, C sono numeri interi *senza divisore comune*. Il primo membro è una forma binaria quadratica (Cfr. § 23)

$$(A,\ B,\ C)$$

primitiva, che si dice *di prima specie* se anche $A, 2\,B, C$ sono primi fra loro, se cioè A, C non sono ambedue pari, e *di seconda* *specie* nel caso opposto. Il *determinante* della forma (che qui prenderemo col segno opposto a quello considerato da Gauss) è dato da

$$D = A\,C - B^2$$

ed è essenzialmente positivo. Siccome i coefficienti estremi A, C hanno necessariamente il medesimo segno, li supporremo, come è lecito, positivi.

Si noti che per le forme di seconda specie, essendo A, C pari, quindi B impari, sarà sempre

$$D \equiv -1 \pmod 4.$$

Una forma primitiva di prima o seconda specie

$$(A,\ B,\ C)$$

definisce completamente, a meno di un fattore, i periodi e quindi una funzione ellittica $\wp(u \mid \omega, \omega')$ a moltiplicazione complessa. Ma siccome, senza cangiare la $\wp u$, possiamo eseguire sui periodi una sostituzione lineare, omogenea a coefficienti interi e a determinante 1, così vediamo che le infinite forme

$$(A',\ B',\ C)$$

equivalenti alla (A, B, C) (§ 23), e queste soltanto, dànno luogo alla medesima $\wp u$. Dunque: *Ogni classe di forme binarie quadratiche a determinante positivo dà una funzione $\wp u$ a moltiplicazione complessa ed inversamente.*

Si tratta ora di stabilire per una tale funzione $\wp u$, corrispondente ad una data forma quadratica

$$(A,\ B,\ C),$$

le più generali formole di moltiplicazione complessa. Dovendo essere τ radice della equazione

$$A\,\tau^2 + 2\,B\,\tau + C = 0,$$

paragonando colla (II), risulta intanto che dovremo porre

$$b = x\,A, \quad a - d = x \cdot 2\,B, \quad c = -x\,C,$$

essendo x un fattore di proporzionalità che, per la condizione che a, b, c, d siano interi, mentre A, B, C sono primi fra loro, dovrà essere un numero *intero* se (A, B, C) è di prima specie, laddove se (A, B, C) è di seconda specie potrà anche essere la metà di un numero intero. Possiamo dunque porre

$$\text{(III)} \qquad b = x\,A, \quad a = x\,B + y, \quad d = -x\,B + y, \quad c = -x\,C,$$

dove i numeri x, y saranno certamente interi se (A, B, C) è di prima specie e potranno invece essere ambedue la metà di numeri interi dispari se (A, B, C) è di seconda specie; in ogni caso però saranno x, y, ovvero $2\,x$, $2\,y$, primi fra loro, poichè supponiamo la trasformazione $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ primitiva (§ 164).

Dai valori precedenti di a, b, c, d risultano le formole

$$\text{(IV)} \qquad N = a\,d = b\,c - D\,x^2 + y^2, \quad \Delta = (a + d)^2 - 4\,N = -4\,D\,x^2$$

$$\text{(V)} \qquad \varepsilon = y + i\,x\sqrt{D}$$

In queste formole (III), (IV), (V) possiamo dare a x, y valori qualunque, soddisfacenti alle dette condizioni, e rimanendo sempre la stessa la funzione $\wp u$, varierà il moltiplicatore ε ed il grado

$$N = D\,x^2 + y^2$$

della trasformazione. Il valore minimo di questo grado si otterrà evidentemente pei valori seguenti di x, y

$x = \pm 1$, $y = 0$ per una forma di prima specie,

$x = \pm \frac{1}{2}$, $y = \pm \frac{1}{2}$ per una forma di seconda specie,

e si avrà rispettivamente nei due casi

$$N = D, \quad N = \frac{D + 1}{4},$$

e corrispondentemente pel moltiplicatore

$$\varepsilon = i\sqrt{D}, \quad \varepsilon = \frac{1}{2}(1 + i\sqrt{D}).$$

Le formole corrispondenti, che esprimono

$$\wp\,(i\sqrt{D}\,.\,u),$$

ovvero

$$\wp\left(\frac{1+i\sqrt{D}}{2}\,.\,u\right)$$

razionalmente per $\wp\,u$, si diranno le *formole elementari di moltiplicazione complessa*, perchè tutte le altre formole di moltiplicazione complessa si otterranno da queste elementari e dalle formole ordinarie di addizione e moltiplicazione dell'argomento. E invero ogni altro valore $\bar{\varepsilon}$ del moltiplicatore sarà, per la (V), della forma

$$\bar{\varepsilon}=r+s\,\varepsilon$$

avendo ε il valore elementare $i\sqrt{D}$ o $\dfrac{1+i\sqrt{D}}{2}$, con r, s interi ordinari, sarà cioè un intero complesso nel campo quadratico $(1, \varepsilon)$.

Ma la formola elementare di moltiplicazione complessa ci dà

$$\wp\,(\varepsilon\,u)=F\,(\wp\,u)$$

e le formole ordinarie di moltiplicazione

$$\wp\,(r\,u)=\Phi\,(\wp\,u),\quad \wp\,(s\,\varepsilon\,u)=F\,(\wp\,(s\,u))=\Phi_1\,(\wp\,u),$$

essendo F, Φ, Φ_1 razionali nel loro argomento. Derivando le precedenti, abbiamo

$$\left\{\begin{aligned}\wp'\,(r\,u)&=\frac{1}{r}\,\Phi'\,(\wp\,u)\,.\,\wp'\,u\\ \wp'\,(s\,\varepsilon\,u)&=\frac{1}{s\,\varepsilon}\,\Phi'_1\,(\wp\,u)\,.\,\wp'\,u\,;\end{aligned}\right.$$

ed ora dalla formola d'addizione

$$\wp\,(r\,u+r\,\varepsilon\,u)=$$
$$=\frac{(2\wp\,(ru)\,\wp\,(s\varepsilon u)-\frac{1}{2}\,g_2)\,\,(\wp\,(ru)+\wp\,(s\varepsilon u))-g_3-\wp'\,(ru)\,\wp'\,(s\varepsilon u)}{2\,(\wp\,(ru)-\wp\,(s\varepsilon u))^2}$$

avremo subito

$$\wp\,(r+s\,\varepsilon)\,u$$

espressa razionalmente per $\wp\,u$. Ne concludiamo:

Le formole elementari di moltiplicazione complessa per la funzione $\wp\,u$, corrispondente ad una forma (A, B, C) primitiva, si ottengono dando ai coefficienti $\begin{pmatrix}a, b\\ c, d\end{pmatrix}$ della trasformazione ed al moltiplicatore ε i valori seguenti

$$a=B,\ \ b=A,\ \ c=-C,\ \ d=-B,\ \ N=D,\ \ \varepsilon=i\sqrt{D}$$

per le forme di prima specie; e invece

$$a=\frac{1}{2}(B+1),\ \ b=\frac{1}{2}\,A,\ \ c=-\frac{1}{2}\,C,\ \ d=\frac{1}{2}\,(-B+1),\ \ N=\frac{D+1}{4}$$
$$\varepsilon=\frac{1+i\sqrt{D}}{2}$$

per le forme di seconda specie.

§ 197. — **Formole effettive di moltiplicazione complessa.**

Le formole effettive di moltiplicazione complessa, corrispondenti alle formole (I)

$$\text{(I)}\qquad\left\{\begin{aligned}\omega\ &=a\,\frac{\omega}{\varepsilon}+b\,\frac{\omega'}{\varepsilon}\\ \omega'&=c\,\frac{\omega}{\varepsilon}+d\,\frac{\omega'}{\varepsilon},\end{aligned}\right.$$

dove a, b, c, d sono interi primi fra loro, non sono altro in sostanza che le formole della trasformazione primitiva:

$$\begin{pmatrix}a, b\\ c, d\end{pmatrix}$$

d'ordine $N=a\,d-b\,c$. Siccome però, al Cap. XIV, noi abbiamo stabilito queste formole nel solo caso di N primo, converrà ora che le deduciamo in modo diretto, e nello stesso tempo avremo anche così le formole generali (primitive) di trasformazione per un ordine N qualunque. A tale oggetto cominciamo dallo scrivere le (I) risolute rispetto a $\frac{\omega}{\varepsilon}$, $\frac{\omega'}{\varepsilon}$:

$$(3)\qquad \begin{cases} \dfrac{\omega}{\varepsilon} = \dfrac{d\,\omega - b\,\omega'}{N} \\ \dfrac{\omega'}{\varepsilon} = \dfrac{-c\,\omega + a\,\omega'}{N} \end{cases} \quad N = a\,d - b\,c.$$

Gli infiniti della funzione

$$\wp\left(u \,\middle|\, \frac{\omega}{\varepsilon}, \frac{\omega'}{\varepsilon}\right) = \varepsilon^2 \wp(\varepsilon u)$$

sono nei punti

$$u_\infty = \frac{2r\omega + 2s\omega'}{\varepsilon} \quad (r, s \text{ interi qualunque}),$$

coi termini d'infinito

$$\frac{1}{(u - u_\infty)^2}.$$

Ora ci conviene in primo luogo dimostrare che i valori u_∞ coincidono con tutti i multipli della parte aliquota

$$\frac{2\tilde{\omega}}{N}$$

di un conveniente periodo $2\tilde{\omega}$. Se consideriamo le (I), (3) come formole della trasformazione $\begin{pmatrix} a, b \\ c, d \end{pmatrix}$, corrispondente alle relazioni

$$\begin{cases} \omega = a\,\Omega + b\,\Omega' \\ \omega' = c\,\Omega + d\,\Omega, \end{cases}$$

sostituendo ad Ω, Ω' un sistema di semiperiodi equivalenti Ω_1, Ω'_1, potremo dare alla trasformazione la forma normale (§ 163)

$$\begin{cases} \omega = \sigma\,\Omega_1 \\ \omega' = \xi\,\Omega_1 + \dfrac{N}{\sigma}\,\Omega'_1, \end{cases}$$

dove σ è un divisore di N, e il numero ξ è determinato $\left(\text{mod}\ \frac{N}{\sigma}\right)$ e non ha divisore comune con σ e $\frac{N}{\sigma}$. Di qui si trae

$$\Omega_1 = \frac{\frac{N}{\sigma}\cdot\omega}{N}, \quad \Omega'_1 = \frac{\sigma\,\omega' - \xi\,\omega}{N}.$$

Sia μ il massimo comun divisore di σ, ξ che sarà primo con $\frac{N}{\sigma}$, e pongasi

$$\sigma = \mu\,\sigma_1, \quad \xi = \mu\,\xi_1,$$

onde

$$(4)\qquad \Omega_1 = \frac{\frac{N}{\sigma}\cdot\omega}{N}, \quad \Omega'_1 = \mu\,\frac{\sigma_1\,\omega' - \xi_1\,\omega}{N}.$$

Eseguiamo ora sui periodi 2ω, $2\omega'$ la sostituzione lineare

$$\begin{cases} \omega = \omega_1 \\ \omega' = \gamma\,\omega_1 + \omega'_1, \end{cases}$$

dove γ indica un intero qualunque, e i nuovi periodi $2\omega_1$, $2\omega'_1$ saranno ancora fondamentali. Le (4) diventano

$$\Omega_1 = \frac{\frac{N}{\sigma}\,\omega_1}{N}, \quad \omega'_1 = \mu\,\frac{(\sigma_1\gamma - \xi_1)\,\omega_1 + \sigma_1\,\omega'_1}{N}.$$

Poniamo $\sigma_1\gamma - \xi_1 = h$ e scegliamo γ in guisa che h, il quale è primo con σ_1, lo sia anche con $\frac{N}{\sigma}$, ciò che è possibile essendo σ_1, ξ_1 primi fra loro; avremo

$$\Omega_1 = \frac{\frac{N}{\sigma}\,\omega_1}{N}, \quad \Omega'_1 = \mu\,\frac{h\,\omega_1 + \sigma_1\,\omega'_1}{N}.$$

Trascurando multipli di semiperiodi ω_1, ω'_1, possiamo scrivere

$$\Omega'_1 \equiv \mu\,\frac{h\,\omega_1 + \sigma_1\left(1 + \varrho\,\frac{N}{\sigma}\right)\omega'_1}{N},$$

essendo ϱ un intero arbitrario. Ora prendiamo ϱ in guisa che sia $1+\frac{N}{\sigma}\varrho$ multiplo di $h\mu$, ciò che è possibile perchè $\frac{N}{\sigma}$ è primo con $h\mu$, e ponendo

$$1+\varrho\frac{N}{\sigma}=h\mu\,.\,\varrho' \quad (\varrho' \text{ intero}),$$

$$\tilde{\omega}=\omega_1+\sigma\varrho'\omega'_1$$

avremo

$$\left\{\begin{aligned} \Omega_1 &= \frac{\frac{N}{\sigma}\omega_1}{N}=\frac{\frac{N}{\sigma}(\tilde{\omega}-\sigma\varrho'\omega'_1)}{N}\equiv\frac{\frac{N}{\sigma}\tilde{\omega}}{N} \\ \Omega'_1 &\equiv \frac{h\mu\tilde{\omega}}{N}. \end{aligned}\right.$$

Le espressioni

$$u_\infty = 2r\Omega_1+2s\Omega'_1$$

avranno quindi la forma

$$u_\infty \equiv \left(\frac{N}{\sigma}r+h\mu\,.\,s\right)\frac{2\tilde{\omega}}{N}$$

e il numero $\frac{N}{\sigma}r+h\mu\,.\,s$, essendo $\frac{N}{\sigma}$, $h\mu$ primi fra loro, percorrerà tutti gli interi possibili, cioè u_∞ tutti i multipli di

$$\frac{2\tilde{\omega}}{N} \quad \text{c. d. d.}$$

Risulta di qui che gli infiniti della funzione

$$\varepsilon^2\wp(\varepsilon u),$$

che ammette i periodi della $\wp u$, sono di secondo ordine nei punti incongrui

$$r\frac{2\tilde{\omega}}{N} \quad (r=0,\ 1,\ 2,\ \ldots,\ N-1),$$

coi termini d'infinito

$$\frac{1}{\left(u-r\frac{2\tilde{\omega}}{N}\right)^2},$$

e si ha quindi

$$\varepsilon^2\wp(\varepsilon u)=\wp u+\sum_{r=1}^{r=N-1}\wp\left(u-r\frac{2\tilde{\omega}}{N}\right)+C.$$

Per determinare la costante C basta sviluppare dalle due parti per potenze di u, nell'intorno di $u=0$, e paragonando i termini costanti il che dà

$$C=-\sum_1^{N-1}\wp\left(r\frac{2\tilde{\omega}}{N}\right),$$

ne risulta la formola domandata:

$$\text{(VI)}\quad \varepsilon^2\wp(\varepsilon u)=\wp u+\sum_{r=1}^{r=N-1}\left\{\wp\left(u-r\frac{2\tilde{\omega}}{N}\right)-\wp\left(r\,.\,\frac{2\tilde{\omega}}{N}\right)\right\}.$$

§ 198. — Natura dei coefficienti nelle formole di moltiplicazione complessa.

Si tratta ora di convertire il secondo membro della (VI) in una funzione razionale di $\wp u$. Per ciò distinguiamo due casi, secondo che N è dispari o pari.

1° caso: *N dispari.* — Associando i valori r, $N-r$ di r, la (VI) può scriversi

$$\varepsilon^2\wp(\varepsilon u)=\wp u-2\sum_{r=1}^{s=\frac{N-1}{2}}\wp\left(s\frac{2\tilde{\omega}}{N}\right)+$$

$$+\sum_{s=1}^{s=\frac{N-1}{2}}\left\{\wp\left(u-s\frac{2\tilde{\omega}}{N}\right)+\wp\left(u+s\,.\,\frac{2\tilde{\omega}}{N}\right)\right\},$$

da cui per le formole d'addizione

$$\text{(VII)}\qquad \varepsilon^2 \wp(\varepsilon u) = \wp u - 2 \sum_{s=1}^{s=\frac{N-1}{2}} \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right) +$$

$$+ \sum_{s=1}^{s=\frac{N-1}{2}} \frac{\left(2 \wp u \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right) - \frac{1}{2} g_2\right)\left(\wp u + \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right)\right) - g_3}{\left[\wp u - \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right)\right]^2},$$

formola che esprime effettivamente $\wp(\varepsilon u)$ razionalmente per $\wp u$.

2° caso: N *pari*. — Associando ancora i valori r, $N-r$, resta questa volta isolato il valore $r = \frac{N}{2}$, onde si ha

$$\varepsilon^2 \wp(\varepsilon u) = \wp u - 2 \sum_{s=1}^{s=\frac{N}{2}-1} \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right) + \wp(u - \tilde{\omega}) - \wp \tilde{\omega} +$$

$$+ \sum_{s=1}^{s=\frac{N}{2}-1} \left[\wp\left(u - s \cdot \frac{2\tilde{\omega}}{N}\right) + \wp\left(u + s \cdot \frac{2\tilde{\omega}}{N}\right)\right].$$

Siccome $\tilde{\omega}$ è un semiperiodo, sarà $\wp \tilde{\omega}$ uno dei tre valori e_1, e_2, e_3, sia e_α, e diciamo e_β, e_γ gli altri due; avremo

$$\wp(u - \tilde{\omega}) - \wp \tilde{\omega} = \frac{(e_\alpha - e_\beta)(e_\alpha - e_\gamma)}{\wp u - e_\alpha},$$

sicchè la formola (VI) diventa in questo caso:

$$\text{(VII*)}\quad \varepsilon^2 \wp(\varepsilon u) = \wp n - 2 \sum_{s-1}^{s=\frac{N}{2}-1} \wp\left(s \frac{2\tilde{\omega}}{N}\right) + \frac{(e_\alpha - e_\beta)(e_\alpha - e_\gamma)}{\wp u - e^\alpha} +$$

$$+ \sum_{s=1}^{s=\frac{N}{2}-1} \frac{\left(2 \wp u \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right) - \frac{1}{2} g_2\right)\left(\wp u + \wp\left(s \frac{2\tilde{\omega}}{N}\right)\right) - g_3}{\left[\wp u - \wp\left(s \cdot \frac{2\tilde{\omega}}{N}\right)\right]^2}.$$

In ambedue i casi risulta

$$\text{(VIII)}\qquad \varepsilon^2 \wp(\varepsilon u) = \frac{U(\wp u)}{V(\wp u)},$$

dove U, V sono polinomî razionali interi in $\wp u$, primi fra loro, di grado N il primo, $N-1$ il secondo.

Importa ora che ricerchiamo di quale natura sono i coefficienti di questi polinomî, che già dalle formole stesse risultano razionalmente formati con g_2, g_3 e col valore $\wp\left(\frac{2\tilde{\omega}}{N}\right)$. Dimostriamo che sussiste l'importante proprietà:

I coefficienti dei polinomî U, V nella formula di moltiplicazione complessa (VIII) *sono funzioni razionali intere di g_2, g_3 con coefficienti numerici razionali se la forma* (A, B, C) *è di prima specie, ovvero contenenti l'unica irrazionalità i $\sqrt{D}$ se la forma è di seconda specie.*

Pongasi

$$\wp u = y,\ U(y) = y^N + a_1 y^{N-1} + a_2 y^{N-2} + \dots + a_{N-1} y + a_N,$$

$$V(y) = y^{N-1} + b_1 y^{N-2} + b_2 y^{N-3} + \dots + b_{N-2} y + b_{N-1},$$

e si scriva la (VIII) nel modo seguente:

$$\text{(5)}\qquad \varepsilon^2 \wp(\varepsilon u)\left[y^{N-1} + b_1 y^{N-2} + b_2 y^{N-3} + \dots + b_{N-1}\right] - $$

$$- \left[y^N + a_1 y^{N-1} + \dots, a_N\right] = 0.$$

Se svolgiamo in serie di potenze di u, servendoci degli sviluppi

$$\begin{cases} x = \wp u = \dfrac{1}{u^2} + \dfrac{g_2}{20} u^2 + \dfrac{g_3}{28} u^4 + \dfrac{g_2^2}{2^4 \cdot 3 \cdot 5^2} u^6 + \dots \\ \varepsilon^2 \wp(\varepsilon u) = \dfrac{1}{u^2} + \dfrac{g_2}{20} \varepsilon^4 u^2 + \dfrac{g_3}{28} \varepsilon^6 u^4 + \dfrac{g_2^2}{2^4 \cdot 3 \cdot 5^2} \varepsilon^8 u^6 + \dots, \end{cases}$$

ed eguagliamo a zero i coefficienti delle varie potenze di u, otteniamo una serie di equazioni lineari nei coefficienti a, b e i coefficienti di queste equazioni sono appunto della natura indicata nell'enunciato del teorema. Ora queste equazioni lineari, qualunque numero se ne prenda, sono sempre fra loro compatibili quando g_2, g_3 abbiano i valori speciali convenienti alla nostra $\wp u$ a moltiplicazione complessa, perchè le a, b sono certamente determinabili in guisa che la (5) risulti identicamente soddisfatta. Ma se lasciamo le a, b indeterminate, il primo membro della (5)

$$\text{(5*)}\qquad \varepsilon^2 \wp(\varepsilon u)\left[(\wp u)^{N-1} + b_1 (\wp u)^{N-2} + \dots + b^{N-1}\right] -$$

$$- \left[(\wp u)^N + a_1 (\wp u)^{N-1} + \dots + a_N\right]$$

è una funzione ellittica coi periodi 2ω, $2\omega'$ che ha nell'origine $u = 0$ un infinito d'ordine $2N - 2$ ed al massimo altri $N - 1$ infiniti del secondo ordine nei punti

$$r\frac{2\bar{\omega}}{N}\ (r = 1, 2, 3, \ldots, n - 1).$$

Se nello sviluppo (5*) eguagliamo a zero i coefficienti delle potenze

$$\frac{1}{u^{2(N-1)}},\ \frac{1}{u^{2(N-2)}},\ \ldots,\ \frac{1}{u^2},\ u^0,\ u^2,\ u^4,\ \ldots,\ u^{2(N-1)}$$

avremo $2N - 1$ relazioni lineari fra le $2N - 1$ costanti a, b, che saranno certo compatibili, per quanto precede, se g_2, g_3 hanno i valori che appartengono alla nostra $\wp u$.

Prendendo le a, b in guisa che tali relazioni siano soddisfatte, la funzione ellittica del primo membro della (5*) avrà al massimo $2(N - 1)$ poli, mentre in $u = 0$ avrà un infinitesimo d'ordine $2N$, e però la funzione stessa sarà identicamente nulla, cioè sarà indenticamente:

$$\text{(VIII*)}\qquad \varepsilon^2\wp(\varepsilon u) = \frac{(\wp u)^N + a_1(\wp u)^{N-1} + \ldots. + a_N}{(\wp u)^{N-1} + b_1(\wp u)^{N-2} + \ldots. + b_{N-1}}.$$

E siccome non può in questa formola restare arbitraria qualcuna delle a, b, segue che le $2N - 1$ relazioni lineari ricordate fra le a, b servono a determinarle completamente; cioè il determinante formato coi coefficienti delle a, b, in quelle $2N - 1$ equazioni lineari, è diverso da zero per quei particolari valori di g_2, g_3. Esso è quindi *a fortiori* diverso da zero se lasciamo in quelle $2N - 1$ equazioni g_2, g_3 arbitrari; queste servono adunque ad esprimere nella (VIII*) i coefficienti a, b razionalmente per g_2, g_3.

Un fatto molto importante segue anche da ciò che, oltre g_2, g_3, nelle equazioni lineari che servono a determinare le costanti a, b, figurano unicamente il numero N ed il moltiplicatore ε, mentre non vi è alcuna traccia dei coefficienti (A, B, C) della forma cui la nostra funzione ellittica $\wp u$ a moltiplicazione complessa corrisponde. Ne risulta: *La formola* (VIII) *o* (VIII*) *di moltiplicazione complessa dipende solo dal determinante D e dalla specie della forma.*

Osserviamo di più che quando $D \equiv -1 \pmod 4$, ed esistono quindi forme di prima e seconda specie, converrà sempre cominciare la ricerca dalle forme di seconda specie, per la quale il grado N ha il minimo valore $\frac{D+1}{4}$, e si passerà poi alle formole relative alle forme di prima specie, operando una trasformazione di secondo grado. E infatti, se si considerano le due forme *principali* di prima e seconda specie

$$(1, 0, D),\quad \left(2, 1, \frac{D+1}{2}\right),$$

e si indicano rispettivamente con τ, τ_1 i rapporti dei periodi, si ha

$$\tau = i\sqrt{D},\quad \tau_1 = \frac{-1 + i\sqrt{D}}{2},$$

e quindi τ è legato a τ_1 dalla trasformazione di secondo grado $\begin{pmatrix}2, 1\\0, 1\end{pmatrix}$

$$\tau = 2\tau_1 + 1.$$

§ 199. — **Risolubilità per radicali dell'equazione per la divisione dei periodi.**

Al § 116, occupandoci delle funzioni $\wp$ lemniscatiche, che sono appunto le più semplici funzioni ellittiche a moltiplicazione complessa e corrispondono a $D = 1$, abbiamo dimostrato che l'equazione per la divisione dei periodi è, in questo caso, risolubile per radicali. Questa proprietà compete, come ora dimostreremo, a tutte le funzioni ellittiche a moltiplicazione complessa, quando dapprima si riguardino come noti (o si aggiungano al campo di razionalità) gli invarianti g_2, g_3.

Sia $\wp$ una funzione ellittica a moltiplicazione complessa, ed ε il moltiplicatore elementare; avremo

$$(6)\qquad \wp((m + n\varepsilon)u) = F(\wp u),$$

essendo m, n due interi qualunque ed F una funzione razionale con coefficienti razionali in g_2, g_3, $i\sqrt{D}$.

Consideriamo ora l'equazione per la divisione dei periodi in un numero qualunque q di parti, che supporremo senz'altro, come è lecito, un numero primo dispari [1]). Se con Ω indichiamo un semiperiodo qualsiasi

(7) $$\Omega = \lambda\,\omega - \mu\,\omega',$$

dove λ, μ sono interi non pari insieme, i valori

(8) $$\wp\left(\frac{2(r+s\,\varepsilon)\,\Omega}{q}\right) \quad (r,\ s \text{ interi})$$

saranno altrettante radici della equazione $\psi_q(y) = 0$ per la divisione dei periodi (§ 114) di grado $\frac{q^2-1}{2}$. Facciamo ora percorrere nella (8) a (r, s) $\frac{q^2-1}{2}$ coppie incongrue fra loro e colle opposte $(-r, -s)$ (mod q), per es. le seguenti:

$$r = 1,\ 2,\ 3,\ \ldots,\ \frac{q-1}{2}\,, \quad \text{con } s = 0$$

$$r = 0,\ 1,\ 2,\ \ldots,\ q-1\,, \quad \text{con } s = 1,\ 2,\ 3\ \ldots.\ \frac{q-1}{2},$$

e dimostriamo che, scegliendo convenientemente λ, μ nella (7), i $\frac{q^2-1}{2}$ corrispondenti valori (8) saranno tutti diseguali, e per ciò saranno tutte le radici di $\psi_q(y) = 0$. Se supponiamo infatti

$$\wp\left(\frac{2(r+s\,\varepsilon)\,\Omega}{q}\right) = \wp\left(\frac{2(r_1+s_1\,\varepsilon)\,\Omega}{q}\right),$$

avremo necessariamente

$$\frac{[(r \pm r_1) + (s \pm s_1)\,\varepsilon]\,\Omega}{q} = m\,\omega + n\,\omega' \quad (m,\ n \text{ interi}),$$

cioè

$$(r \pm r_1)\ (\lambda\,\omega - \mu\,\omega') + (s \pm s_1)\ (\lambda\,\varepsilon\,\omega - \mu\,\varepsilon\,\omega') = q\,(m\,\omega + n\,\omega'),$$

e sostituendo per $\varepsilon\,\omega$, $\varepsilon\,\omega'$ i valori

$$\begin{cases} \varepsilon\,\omega = a\,\omega + b\,\omega' \\ \varepsilon\,\omega' = c\,\omega + d\,\omega', \end{cases}$$

[1]) Del resto le considerazioni che seguono valgono anche per q dispari qualunque.

dovranno risultare eguali dall'una e dall'altra parte i coefficienti di ω, ω'. Ne seguono le congruenze

$$\left.\begin{aligned} (r \pm r_1)\,\lambda + (s \pm s_1)\ (\lambda\,a - \mu\,c) \equiv 0 \\ (r \pm r_1)\,\lambda + (s \pm s_1)\ (\lambda\,b - \mu\,d) \equiv 0 \end{aligned}\right\} \ (\text{mod } q),$$

le quali, *non essendo simultaneamente*

$$r \pm r_1 \equiv 0, \quad s \pm s_1 \equiv 0 \ (\text{mod } q),$$

richiedono che si abbia

$$\begin{vmatrix} \lambda & \mu\,c - \lambda\,a \\ \mu & \lambda\,b - \mu\,d \end{vmatrix} \equiv 0 \ (\text{mod } q),$$

cioè (§ 197)

$$A\,\lambda^2 + 2\,B\,\lambda\,\mu + C\,\mu^2 \equiv 0 \ (\text{mod } q).$$

Ma poichè (A, B, C) è una forma primitiva, risulta da considerazioni elementari che si possono scegliere λ, μ, non simultaneamente pari, in guisa che la precedente congruenza *non* risulti soddisfatta [1]). Scelti λ, μ in questa guisa, facendo percorrere nell'espressione (8) ad r, s le indicate $\frac{q^2-1}{2}$ coppie di valori, si avranno tutte le radici di $\psi_q(y) = 0$. Ora prendiamo le formole di moltiplicazione complessa

$$\wp\,((r + s\ \varepsilon)\,u) = F\ (\wp\,u)$$
$$\wp\,((r_1 + s_1\,\varepsilon)\,u) = F_1\,(\wp\,u),$$

essendo F, F_1 funzioni razionali della specie descritta. Mutando nella prima formola u in $(r_1 + s_1\,\varepsilon)\,u$, e nella seconda u in $(r + s\,\varepsilon)\,u$, deduciamo

$$F\,(F_1\,(\wp\,u)) = F_1\,(F\,(\wp\,u)).$$

[1]) Se q divide A e C si diano a λ, μ valori non divisibili per q; se poi q non divide per es. A, si dia a μ un valore divisibile per q, a λ un valore non divisibile (Cfr. Dirichlet, *Teoria dei numeri*, pag. 227, edizione italiana).

Facendo in particolare $u = \frac{2\Omega}{q}$, abbiamo

$$\wp\left(\frac{(r+s\varepsilon)\,2\Omega}{q}\right) = F\left(\wp\left(\frac{2\Omega}{q}\right)\right)$$

$$\wp\left(\frac{(r_1+s_1\varepsilon)\,2\Omega}{q}\right) = F_1\left(\wp\left(\frac{2\Omega}{q}\right)\right)$$

$$F\left(F_1\left(\wp\left(\frac{2\Omega}{q}\right)\right)\right) = F_1\left(F\left(\wp\left(\frac{2\Omega}{q}\right)\right)\right),$$

vediamo adunque che l'equazione $\psi_q(y) = 0$ è in questo caso un'equazione Abeliana (con un gruppo di Galois di sostituzioni permutabili) ed è per ciò risolubile per radicali, come si era asserito.

§ 200. — Equazione algebrica fra g_2, g_3 per le funzioni $\wp$ a moltiplicazione complessa.

Nei paragrafi precedenti abbiamo riguardato le funzioni ellittiche a moltiplicazione complessa come definite dal rapporto τ dei periodi, radice di una forma quadratica (A, B, C), e in particolare, nella risoluzione per radicali dell'equazione per la divisione dei periodi, abbiamo considerati come *noti* gli invarianti g_2, g_3. Ora vogliamo occuparci del problema di determinare gli invarianti g_2, g_3, appena sia data la forma (A, B, C) cui la nostra funzione ellittica

$$\wp(u \mid \omega, \omega')$$

appartiene. Ricordiamo che, assegnato il rapporto τ dei periodi, gli invarianti g_2, g_3 sono determinati soltanto a meno delle potenze λ^4, λ^6 di un fattore di omogeneità λ, e però il problema proposto si riduce essenzialmente a ricercare il valore corrispondente dell'invariante assoluto

$$J = \frac{g_2^3}{g_2^3 - 27\,g_3^2}.$$

Riprendendo le considerazioni alla fine del § 198, facilmente vediamo che:

Gli invarianti g_2, g_3 di una funzione ellittica a moltiplicazione complessa sono legati fra loro da un'equazione algebrica

$$\text{(A)} \qquad \Phi(g_2, g_3) = 0$$

a coefficienti interi, dipendente unicamente dal determinante D e dalla specie della forma (A, B, C), cui $\wp u$ appartiene.

Nel determinare infatti i valori delle $2N-1$ costanti a, b nella (5) noi abbiamo proceduto algebricamente, come se g_2, g_3 fossero arbitrari. Ora prendendo quante si vogliano delle seguenti equazioni lineari fra le a, b, dopo le prime $2N-1$, che ci hanno servito a determinare le a, b in funzione di g_2, g_3, è certo che esse sono compatibili colle precedenti *per quei particolari valori di* g_2, g_3 che appartengono alla nostra $\wp u$; ma è impossibile che ciò accada *lasciando* g_2, g_3 *arbitrari*, altrimenti la formola

$$\varepsilon^2 \wp(\varepsilon u) = \frac{(\wp u)^N + a_1 (\wp u)^{N-1} + \ldots + a^N}{(\wp u)^{N-1} + b_1 (\wp u)^{N-2} + \ldots + b_{N-1}},$$

con $\varepsilon = i\sqrt{D}$ o $\varepsilon = \frac{1+i\sqrt{D}}{2}$, varrebbe per una $\wp u$ arbitraria, ciò che è assurdo.

Dunque nella serie delle dette equazioni lineari ne incontreremo certamente una $(2N)^{ma}$ che non sarà più indipendente dalle prime $2N-1$ per g_2, g_3 arbitrari, ed eliminando quindi le $2N-1$ costanti a, b fra queste equazioni lineari, si avrà appunto, sotto forma di determinante, l'asserita relazione (A), che potremo liberare dall'irrazionalità $i\sqrt{D}$, se pur la contiene. È manifesto poi che la (A) dipende unicamente dal determinante D e dalla specie della forma (A, B, C), come porta l'enunciato del teorema.

Ora osserviamo che la relazione (A) fra g_2, g_3, a causa delle mentovate formole d'omogeneità, si può trasformare in un'equazione

$$\text{(B)} \qquad F(J) = 0$$

per l'invariante assoluto $J(\tau)$, *con coefficienti interi*, e di questa equazione saranno radici tutti gli invarianti assoluti delle funzioni ellittiche $\wp u$ a moltiplicazione complessa, corrispondenti a forme quadratiche (A, B, C) della medesima specie e dello stesso determinante D.

Alla dimostrazione della esistenza della equazione algebrica (A), e conseguentemente della (B), possiamo pervenire anche nel modo seguente (Halphen, loc. cit.). Sviluppiamo direttamente i due membri della (VI), § 197, per potenze di u e paragoniamo dalle due parti i coefficienti di u^2, u^4; abbiamo così le formole:

$$(9)\qquad \left\{\begin{aligned} \frac{1}{20}(\varepsilon^4-1)\,g_2 &= \frac{1}{2}\sum_{r=1}^{r=N-1}\wp''\left(\frac{2r\bar\omega}{N}\right)\\ \frac{1}{28}(\varepsilon^6-1)\,g_3 &= \frac{1}{24}\sum_{r=1}^{r=N-1}\wp^{\mathrm{IV}}\left(\frac{2r\bar\omega}{N}\right).\end{aligned}\right.$$

Sostituendo per $\wp''\left(\frac{2r\bar\omega}{N}\right)$, $\wp^{\mathrm{IV}}\left(\frac{2r\bar\omega}{N}\right)$ i loro valori

$$\wp''\left(\frac{2r\bar\omega}{N}\right) = 6\,\wp^2\left(\frac{2r\bar\omega}{N}\right)-\frac{1}{2}g_2$$

$$\wp^{\mathrm{IV}}\left(\frac{2r\bar\omega}{N}\right) = 12\left\{10\,\wp^3\left(\frac{2r\bar\omega}{N}\right)-\frac{3}{2}g_2\,\wp\left(\frac{2r\bar\omega}{N}\right)-g_3\right\},$$

ed esprimendo quindi i secondi membri delle (9) razionalmente per $\wp\left(\frac{2\bar\omega}{N}\right)$, colle formole ordinarie di moltiplicazione dell'argomento, l'eliminazione di $\wp\left(\frac{2\bar\omega}{N}\right)$ fra le (9) porterà ad una relazione (A) fra g_2, g_3, o alla (B) per $J(\tau)$.

§ 201. — **Esempi numerici** $D=3$, $D=2$, $D=7$.

Prima di procedere allo studio delle proprietà della equazione (B), cui soddisfano gli invarianti assoluti delle funzioni ellittiche a moltiplicazione complessa, applichiamo i processi generali esposti ad alcuni casi particolari più semplici.

In due soli casi il grado N della trasformazione per la moltiplicazione complessa è semplicemente $=1$, e cioè nei casi

$$D=1,\quad D=3,$$

corrispondentemente alla unica classe e determinante $D=1$

$$(1,\ 0,\ 1)$$

e all'unica classe di seconda specie per $D=3$

$$(2,\ 1,\ 2).$$

Le funzioni $\wp$ corrispondenti sono la lemniscatica e la equianarmonica, colle formole rispettive di moltiplicazione complessa

$$\wp(iu) = -\wp u$$
$$\wp(\varepsilon u) = \varepsilon\wp u.$$

I valori caratteristici degli invarianti sono $g_3=0$ nel primo caso, e $g_2=0$ nel secondo. Esaminiamo ora i casi successivi in cui si ha $N=2$, che corrispondono unicamente ai valori

$$D=2,\quad D=7,$$

quando, nel caso $D=7$, si considerino forme di seconda specie.

1º caso: *Sia* $D=2$. — Qui abbiamo una sola classe di forme, rappresentata dalla forma ridotta $(1, 0, 2)$. Le formole (I), § 195, diventano

$$\left.\begin{aligned}\varepsilon\omega &= \omega',\ \frac{\omega}{\varepsilon} = -\frac{\omega'}{2}\\ \varepsilon\omega' &= -2\omega,\ \frac{\omega'}{\varepsilon} = \omega\end{aligned}\right\}\quad \varepsilon = i\sqrt{2},\ N=2.$$

Per semiperiodo $\bar\omega$ si può prendere semplicemente $\bar\omega=\omega'$ e la formola (VII*), pag. 311, ci darà subito

$$(10)\qquad \varepsilon^2\wp(\varepsilon u) = \wp u + \frac{(e_3-e_1)\,(e_3-e_2)}{\wp u - e_3};$$

che scriviamo sotto la forma

$$\varepsilon^2\wp(\varepsilon u) = \frac{\wp^2 u - a\,\wp u + \beta}{\wp u - a}.$$

Per determinare le costanti α, β, seguiamo il processo indicato al § 198, sostituendo nella (10) gli sviluppi in serie

$$\wp u = \frac{1}{u^2} + \frac{g_2}{20} u^2 + \frac{g_3}{28} u^4 + \frac{g_2^2}{2^4 . 3 . 5^2} u^6 + \dots$$

$$\wp^2 u = \frac{1}{u^4} + \frac{g_2}{10} + \frac{g_3}{14} u^2 + \frac{g_2^2}{2^4 . 3 . 5} u^4 + \dots$$

$$\varepsilon^2 \wp(\varepsilon u) = \frac{1}{u^2} + \frac{4 g_2}{20} u^2 - \frac{8 g_3}{28} u^4 + \frac{16 g_2^2}{2^4 . 3 . 5^2} u^6 + \dots,$$

e paragonando i termini costanti e i coefficienti di u^2 dalle due parti dell' identità

$$\varepsilon^2 \wp(\varepsilon u)\ (\wp u - \alpha) = \wp^2 u - \alpha \wp u + \beta,$$

troveremo subito

$$\alpha = -\frac{15 g_3}{7 g_2},\ \beta = \frac{3 g_2}{20}.$$

Il paragone poi dei coefficienti di u^4 darà

$$3^2 . 5^2 \alpha g_3 + 14 g_2^2 = 0,$$

da cui la relazione algebrica fra g_2, g_3

$$g_2^3 = \frac{3^3 . 5^3}{2 . 7^2} . g_3^2 .$$

Ne deduciamo quindi

$$J(i\sqrt{2}) = \left(\frac{5}{3}\right)^3.$$

Si assuma per es. disponendo del fattore di omogeneità in g_2, g_3,

$$g_2 = 2 . 3 . 5 . = 30$$
$$g_3 = 2^2 . 7 = 28$$

e si troverà

$$e_1 = 1 + \frac{3}{\sqrt{2}},\ e_2 = 1 - \frac{3}{\sqrt{2}},\ e_3 = -2,$$

onde la formola di moltiplicazione complessa (10) diventa

$$(12) \qquad -2 \wp(i\sqrt{2} . u) = \wp u + \frac{9}{2 \wp u + 4}.$$

2° caso: *Sia* $D = 7$. — Qui si ha una sola classe di prima specie ed una sola di seconda specie, rappresentate rispettivamente dalle forme ridotte

$$(1,\ 0,\ 7),\quad (2,\ 1,\ 4).$$

Cerchiamo la formola di moltiplicazione complessa della $\wp u$ corrispondente alla seconda forma, dalla quale potremmo poi dedurre quella relativa alla $\wp u$ di prima specie con una trasformazione di secondo grado (§ 198).

Le formole fondamentali (I) diventano nel caso attuale:

$$\left\{\begin{array}{l} \varepsilon\omega = \omega + \omega' \\ \varepsilon\omega' = -2\omega \end{array}\right. \quad \left\{\begin{array}{l} \dfrac{\omega}{\varepsilon} = -\dfrac{\omega'}{2} \\ \dfrac{\omega'}{\varepsilon} = \omega + \dfrac{\omega'}{2} \end{array}\right., \quad \text{con } \varepsilon = \frac{1 + i\sqrt{7}}{2}$$

$$N = \frac{7+1}{4} = 2.$$

Potremo quindi fare $\tilde{\omega} = \omega'$ e la (VII*) pag. 311 ci darà nuovamente

$$(10) \qquad \varepsilon^2 \wp(\varepsilon u) = \wp u + \frac{(e_3 - e_2)\ (e_3 - e_1)}{\wp u - e_3}.$$

Per determinare i coefficienti e la relazione fra g_2, g_3 potremmo procedere come nel caso precedente; qui preferiamo il calcolo seguente. Facciamo nella (11) $u = \omega$ e avremo

$$\varepsilon^2 e_2 = e_1 + e_2 - e_3,$$

che combinata coll' identità

$$0 = e_1 + e_2 + e_3$$

e avendo riguardo all'equazione

$$\varepsilon^2 - \varepsilon + 2 = 0$$

cui soddisfa il moltiplicatore, ci dà

$$e_3=\left(1-\frac{\varepsilon}{2}\right)e_2\,,\ e_1=\left(\frac{\varepsilon}{2}-2\right)e_2$$

e quindi

$$g_2=2\,(e_1^2+e_2^2+e_3^2)=5\,(2-\varepsilon)\,e_2^2$$
$$g_3=4\,e_1\,e_2\,e_3 \qquad =(2-\varepsilon)\;(\varepsilon-4)\,e_2^3\,,$$

onde

$$\frac{g_2^3}{g_3^2}=\frac{5^3}{7}\,,$$

quindi

$$J\left(\frac{-1+i\sqrt{7}}{2}\right)=-\frac{5^3}{2^6}\,.$$

A meno di un fattore di omogeneità, possiamo porre

$$g_2=5\,.\,7=35,\ \ g_3=7^2=49\,;$$

e allora per le radici e_1, e_2, e_3 avremo:

$$e_1=\frac{7}{2}\,,\ e_2=-\frac{\varepsilon+3}{2}=-\frac{7+i\sqrt{7}}{4}\,,\ e_3=\frac{\varepsilon-4}{3}=\frac{-7+i\sqrt{7}}{4}$$

e per la formola di moltiplicazione complessa [1]):

$$(\varepsilon-2)\,\wp\,(\varepsilon\,u)=\wp\,u+\frac{7}{2}\,\frac{1-3\,\varepsilon}{2\,\wp\,u+4-\varepsilon}\,. \tag{13}$$

Conformemente ai teoremi generali, vediamo che nella (12) il secondo membro è libero dalla irrazionalità ε, laddove nella (13) vi comparisce.

[1]) Si osservi che si ha

$$(e_3-e_1)\,(e_3-e_2)=\frac{7}{4}\,(1-3\,\varepsilon).$$

§ 202. — Invarianti delle classi.

Abbiamo veduto, al § 200, che tutti gli invarianti assoluti J delle funzioni ellittiche a moltiplicazione complessa, corrispondenti alle classi delle forme quadratiche $(A,\ B,\ C)$ del medesimo determinante e della medesima specie, sono radici di una medesima equazione (B) a coefficienti interi. Siccome ad ogni classe di forme quadratiche corrisponde un tale invariante, chiameremo i valori $J\,(\tau_1)$, ove τ_1 sia radice di una forma quadratica (A, B, C), *invarianti delle classi* e potremo enunciare il teorema :

Gli invarianti delle classi sono numeri algebrici.

Vogliamo stabilire e precisare questo teorema, applicando la teoria delle equazioni modulari, nella qual cosa ci serviremo nuovamente dell' invariante modificato (§ 183)

$$j\,(\tau)=12^3\,J\,(\tau).$$

Per questo ci è necessario premettere alcune nozioni sulle equazioni modulari per $j\,(\tau)$, anche pel caso che il grado della trasformazione

$$\begin{pmatrix} d, & c \\ b, & a \end{pmatrix},$$

dato da $a\,d-b\,c=N$, non sia un numero primo. Se eseguiamo sull'argomento τ di $j\,(\tau)$ tutte le sostituzioni primitive [1])

$$\frac{d\,\tau+c}{b\,\tau+a}$$

a determinante

$$a\,d-b\,c=N,$$

i valori distinti che assume

$$j'=j\left(\frac{d\,\tau+c}{b\,\tau+a}\right)$$

[1]) In cui cioè $a,\ b,\ c,\ d$ sono primi fra loro.

sono tutti compresi nella formola

$$\text{(C)} \qquad j\left(\frac{\sigma\tau+\nu}{n}\right), \quad n\sigma = N,$$

essendo σ, ν, n tre numeri senza divisore comune, tali che $n\sigma = N$, e ν risultando determinato solo rispetto al modulo n. Il numero $\psi(N)$ di questi valori distinti (C), supposto che decomponendo N in fattori primi si abbia

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

sarà dato da

$$\psi(N) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_r^{\alpha_r-1} (p_1+1) \ (p_2+1) \dots (p_r+1)$$

(Cfr. § 164). Precisamente come si è fatto nel § 184, pel caso di N primo, si dimostra che questi $\psi(N)$ valori j' sono radici di un'equazione algebrica (modulare), che indicheremo con

$$\text{(D)} \qquad F_N(j', j) = 0,$$

dove F_N è una funzione razionale intera con coefficienti interi e di grado $\psi(N)$ in j'.

Sia ora τ_0 l'indice di una forma quadratica (A, B, C) a determinante D, di prima o di seconda specie. Poniamo, secondo le formole (III) del § 196:

$$b = xA, \quad a = xB + y, \quad d = -xB + y, \quad c = -xC$$
$$N = ad - bc = Dx^2 + y^2,$$

dove x, y saranno interi primi fra loro se (A, B, C) è di prima specie, o anche, nel caso che (A, B, C) sia di seconda specie, la metà di numeri *dispari* primi fra loro.

Avremo

$$\tau_0 = \frac{d\tau_0 + c}{b\tau_0 + a},$$

e perciò anche

$$j(\tau_0) = j\left(\frac{d\tau_0 + c}{b\tau_0 + a}\right),$$

onde segue che l'equazione modulare (D) è soddisfatta ponendo

$$j = j(\tau_0) \quad j' = j\left(\frac{d\tau_0 + c}{b\tau_0 + a}\right) = j(\tau_0);$$

dunque: l'invariante di classe $j(\tau_0)$ è radice della equazione

$$\text{(D*)} \qquad F_N(u, u) = 0,$$

e poichè questa equazione ha i coefficienti interi, segue nuovamente il risultato superiore che gli invarianti di classi sono numeri algebrici. Ma possiamo spingere più in là la ricerca e dimostrare che: *Gli invarianti $j(\tau)$ di classi sono numeri* **interi** *algebrici*[1]). Per ciò dimostreremo che, *escluso il caso in cui N sia un quadrato perfetto*, caso che possiamo sempre evitare scegliendo convenientemente nella (14) i numeri x, y:

Il coefficiente della più alta potenza di u nella (D*) *è l'unità.*

Per dimostrarlo osserviamo che si ha identicamente

$$F_N(j', j(\tau)) = \Pi\left(j' - j\left(\frac{\sigma\tau+\nu}{n}\right)\right),$$

il prodotto del secondo membro essendo esteso ad un sistema completo di rappresentanti $\begin{pmatrix}\sigma, & \nu \\ 0, & n\end{pmatrix}$; ne risulta:

$$\text{(15)} \qquad F_N(j(\tau), \ j(\tau)) = \Pi\left[j(\tau) - j\left(\frac{\sigma\tau+\nu}{n}\right)\right].$$

Ora sviluppando $u = j(\tau)$ in serie di potenze di $Q = q^2 = e^{2\pi i\tau}$, si ha

$$u = j(\tau) = Q^{-1}(1 + a_1 Q + a_2 Q^2 + \dots),$$

le a essendo numeri interi. Per ciò la più alta potenza di u nella (D*) avrà un esponente ed un coefficiente eguali rispettivamente all'esponente e coefficiente della più alta potenza di Q^{-1},

[1]) Numero *intero* algebrico è un numero che soddisfa ad un'equazione con coefficienti interi e il primo eguale all'unità (Cfr. DEDEKIND, Suppl. alla *Zahlentheorie* di DIRICHLET).

che figura nello sviluppo per potenze di Q nel secondo membro della (15). Lo sviluppo di ciascun fattore

$$j(\tau) - j\left(\frac{\sigma\tau + \nu}{n}\right)$$

è dato da

$$Q^{-1}(1 + a_1 Q + \ldots) - Q^{-\frac{\sigma}{n}} e^{-\frac{2\pi i \nu}{n}} \left(1 + a_1 Q^{\frac{\sigma}{n}} e^{\frac{2\pi i \nu}{n}} + \ldots\right),$$

e la più alta potenza di Q^{-1} che vi figura è la prima se $\sigma < n$ ed ha coefficiente $= 1$, mentre quando $\sigma > n$ [1]) questa più alta potenza negativa di Q è $Q^{-\frac{\sigma}{n}}$, con coefficiente $= -e^{-\frac{2\pi i \nu}{n}}$. Se riuniamo tutti i fattori che si ottengono tenendo fissi σ, n e facendo percorrere a ν tutti i suoi valori distinti, cioè un sistema completo di resti (mod n), che siano primi col massimo comun divisore δ di σ, n, il numero di questi fattori sarà dato da $\frac{n}{\delta}\varphi(\delta)$, avendo $\varphi(\delta)$ il solito significato aritmetico [2]), e il prodotto di questi fattori porterà la potenza $\frac{\sigma}{\delta}\varphi(\delta)$ di Q^{-1} col coefficiente

$$\pm e^{\frac{2\pi i}{n}\Sigma\nu}. \tag{16}$$

Ora si ha $\Sigma\nu \equiv 0$ (mod n), poichè se r indica un numero primo con n, mentre ν percorre i suoi valori, anche $r\nu$ percorre un sistema completo di resti (mod n) e primi con δ onde, $r\Sigma\nu \equiv \Sigma\nu$ (mod n) e quindi appunto $\Sigma\nu \equiv 0$ (mod n), se $n > 2$. Ma se $n = 2$, allora $\nu = 1$ e il valore (16) è $= \pm 1$.

In ogni caso dunque il valore assoluto del coefficiente (16) è l'unità. L'esponente della potenza di u portata dai fattori corrispondenti a valori fissi di σ, n è quindi $\frac{n}{\delta}\varphi(\delta)$ o $\frac{\sigma}{\delta}\varphi(\delta)$, secondo che $n > \sigma$ o $\sigma > n$, e per ciò l'esponente totale h è dato da:

$$h = \sum \frac{n}{\delta}\varphi(\delta) + \sum \frac{\sigma}{\delta}\varphi(\delta),$$

[1]) Non può essere $\sigma = n$, altrimenti sarebbe $N = n^2$ un quadrato contro la ipotesi.

[2]) Numero dei numeri inferiori a δ e primi con δ.

tanto la prima che la seconda somma essendo estese ai divisori n o σ di N che sono $> \sqrt{N}$. Si conclude quindi: *La più alta potenza di u, che figura nella* (D*), *ha un esponente h dato da*

$$h = 2\sum \frac{n}{\delta}\varphi(\delta),$$

dove n percorre i divisori di N che sono maggiori di $\sqrt{N}$ e δ è il massimo comun divisore di n, $\frac{N}{n}$; il coefficiente di questa più alta potenza è $= \pm 1$.

Così adunque è stabilito il teorema enunciato:

Gli invarianti $j(\tau)$ delle classi sono numeri interi algebrici.

In particolare quando vi ha una sola classe, come nei casi

$$D = 1, \quad D = 2$$
$$D = 3, \quad D = 7,$$

i valori corrispondenti di j saranno numeri interi ordinarii. Come conferma, ricordiamo che abbiamo trovato

$$j(i) \quad = 12^3, \; j\left(\frac{-1 + i\sqrt{3}}{2}\right) = 0$$

$$j(i\sqrt{2}) = 20^3, \; j\left(\frac{-1 + i\sqrt{7}}{2}\right) = -3^3 \cdot 5^3 \; (\S\, 201).$$

§ 203. — Proprietà delle equazioni irriducibili per gli invarianti delle classi.

Ogni invariante j_1 di una classe, essendo un numero intero algebrico, soddisfa ad un'equazione

$$\varphi(j) = 0 \tag{E}$$

irriducibile con coefficienti interi ed il primo eguale all'unità. Vogliamo ora dimostrare il teorema: *Tutte le radici della equazione irriducibile* (E), *cui soddisfa un invariante j_1 di classe, sono pure invarianti di classi, del medesimo determinante e della medesima specie.*

Per questo riprendiamo l'equazione (D*)

(D*) $$F_N(u, u) = 0$$

per meglio caratterizzare tutte le sue radici. Se u è una radice di (D*) e si pone

$$u = j(\tau_1),$$

l'equazione

$$F_N(j', j(\tau_1)) = 0$$

avrà una radice $j' = j(\tau_1)$ e per ciò sarà, per convenienti valori dei numeri σ, n, ν (senza divisore comune):

$$j(\tau_1) = j\left(\frac{\sigma\tau_1 + \nu}{n}\right), \quad n\sigma = N,$$

e quindi

$$\tau_1 = \frac{d\tau_1 + c}{b\tau_1 + a}, \quad ad - bc = N,$$

essendo a, b, c, d quattro interi senza divisore comune, cioè τ_1 sarà indice di una forma quadratica (A, B, C) primitiva.

Ora di qui seguono (§ 196) le relazioni (14) del paragrafo precedente, essendo x, y interi primi fra loro, ovvero la metà di numeri dispari primi fra loro. Se ne deduce il teorema fondamentale:

Le radici della equazione (D*)

(D*) $$F_N(u, u) = 0$$

sono tutti e soli quegli invarianti di classi (A, B, C) *di prima specie con determinanti* D *pei quali è risolubile, in modo proprio, l'equazione*

$$N = Dx^2 + y^2$$

e quegli invarianti di classi di seconda specie con tali determinanti D *che sia solubile l'equazione precedente, ovvero l'altra*

$$4N = Dx^2 + y^2$$

in numeri x, y *impari primi fra loro.*

In altre parole le radici di $F_N(u, u) = 0$ sono tutti e soli quegli invarianti di classi tali che o il grado N sia rappresentabile in modo proprio dalla forma principale $(1, 0, D)$, ovvero $4N$ dalla forma stessa con soluzioni impari.

Sia dunque la (E) l'equazione irriducibile, cui soddisfa un invariante di classe j_1 a determinante D. Allora j_1 è anche radice della equazione

$$F_D(u, u) = 0,$$

la quale avrà pure tutte le altre radici della equazione irriducibile (E), onde si vede intanto che: *tutte le radici della* (E) *sono invarianti di classi.* Ma ora dobbiamo di più dimostrare che tutte queste radici sono invarianti, appartenenti al medesimo determinante ed alla medesima specie.

Siano j_1, j_2 due invarianti di classi, radici della (E), ed appartengano, se è possibile, a determinanti diversi D, D_1; sia per es. $D > D_1$.

Allora j_2 non potrà essere di prima specie; perchè l'equazione

$$F_D(u, u) = 0,$$

avendo la radice j_1 dell'equazione irriducibile (E), ammetterebbe pure la j_2 e, pel teorema fondamentale, dovrebbe quindi essere solubile in modo proprio l'equazione

$$D = D_1 x^2 + y^2,$$

ciò che è assurdo essendo $D < D_1$ [1]). La radice j_2 di maggior determinante sarà quindi di *seconda specie.* Quella j_1 di minor determinante sarà invece di prima specie; perchè se fosse anche j_1 di seconda specie, sarebbe $D \equiv -1 \pmod 4$ e j_1 sarebbe radice di

$$F_{\frac{D+1}{4}}(u, u) = 0,$$

e però anche j_2, onde dovrebbe aversi pel teorema fondamentale, in numeri x, y primi fra loro:

$$\frac{D+1}{4} = D_1 x^2 + y^2,$$

1) Il caso $D = 1$ naturalmente si esclude perchè allora j_1 è razionale $= 12^3$.

ovvero

$$D + 1 = D_1 x^2 + y^2,$$

in quest'ultimo caso con x, y impari e ciò è assurdo, perchè $D > D_1$ e si suppone $D \neq 3$ [1]).

Dunque nelle nostre ipotesi sarà j_1 di prima, j_2 di seconda specie; e poichè ambedue sono radici di $F_D(u, u) = 0$; e non è solubile propriamente l'equazione

$$D = D_1 x^2 + y^2,$$

lo sarà, in numeri impari, l'altra

$$4\,D = D_1 x^2 + y^2,$$

onde deduciamo

$$a) \qquad D \geq \frac{D_1 + 1}{4}.$$

D'altronde j_2, quindi j_1, è radice di

$$F_{\frac{D_1+1}{4}}(u, u) = 0$$

e però è solubile propriamente l'equazione

$$\frac{D_1 + 1}{4} = D x^2 + y^2,$$

onde si trae (perchè $D_1 \neq 3$)

$$\frac{D_1 + 1}{4} \geq D,$$

e, confrontando con a), risulterebbe

$$D = \frac{D_1 + 1}{4}.$$

[1]) Per $D = 3$ sarebbe $j_1 = 0$.

Ma l'equazione

$$F_{D_1}(u, u) = 0$$

ammette la radice j_2, quindi j_1, e però è solubile propriamente l'equazione

$$D_1 = D x^2 + y^2$$

o

$$4\,D - 1 = D x^2 + y^2,$$

onde seguirebbe $x = \pm 1$ indi $y^2 \equiv -1 \pmod 3$, ciò che è assurdo.

Così è dimostrato che tutte le radici della (E) appartengono al medesimo determinante. Ma anche la loro specie è la stessa; perchè se j_1 fosse di prima, j_2 di seconda specie, essendo ambedue radici di

$$F_{\frac{D+1}{4}}(u, u) = 0,$$

sarebbe solubile propriamente l'equazione

$$\frac{D + 1}{4} = D x^2 + y^2,$$

ciò che è assurdo, essendo $D \neq 3$.

Dal teorema dimostrato segue che se

$$f_1\,,\ f_2\,,\ f_3 \ldots f_h$$

sono un sistema completo di forme di egual determinante D e della medesima specie, i cui indici siano

$$\tau_1\,,\ \tau_2\,,\ \tau_3 \ldots \tau_h\,,$$

e i corrispondenti valori degli invarianti delle classi si indicano con

$$j_1\,,\ j_2\,,\ j_3 \ldots j_h\,,$$

il polinomio di grado h in j,

$$(j - j_1)\ (j - j_2) \ldots (j - j_h)$$

ha coefficienti interi e per primo coefficiente 1. Indicheremo questo polinomio con $H_D(j)$ per le forme di prima specie, e con $H'_D(j)$ per quelle di seconda specie. Così avremo per esempio

$$H_1(j) = j - 12^3, \quad H_2(j) = j - 20^3$$
$$H'_3(j) = j \quad , \quad H'_7(j) = j + 3^3 \cdot 5^3.$$

§ 204. — Modo di calcolare i fattori $H_m(j)$, $H'_m(j)$.

Nel paragrafo precedente abbiamo dimostrato che i polinomii $H_D(j)$, $H'_D(j)$ hanno coefficienti interi (il primo $= 1$); ma resta a dare un metodo che serva al calcolo effettivo di questi polinomii. Per questo procediamo, con Weber, nel modo seguente, che dà nel medesimo tempo una nuova dimostrazione, *per induzione completa*, dei risultati sopra ottenuti. Supponiamo adunque di conoscere tutti i polinomii [1]).

$$H_n(j), \quad H'_{4n-1}(j)$$

per $n < m$, e di aver verificato che essi hanno tutti coefficienti interi, e proponiamoci di calcolare

$$H_m(j), \quad H'_{4m-1}(j).$$

Per questo costruiamo l'equazione

$$(\beta) \qquad F_m(u, u) = 0,$$

le cui radici sono tutti invarianti di classi e precisamente alcune sono invarianti di prima specie, appartenenti a determinanti n pei quali è solubile propriamente l'equazione

$$m = x^2 + n y^2.$$

Il massimo valore che si può dare ad n è appunto m, talchè $F_m(u, u)$ contiene come fattore il polinomio di prima specie $H_m(j)$ ed altri $H_n(j)$ di prima specie con $n < m$, e per ciò già noti per

1) Si ricordi che i polinomii $H'_m(j)$ di seconda specie esistono solo per $m \equiv -1 \pmod 4$.

ipotesi. Le altre radici della (β) saranno invarianti di classi di seconda specie, appartenenti a determinanti $4n - 1$ pei quali è solubile l'equazione

$$4m = x^2 + (4n - 1) y^2,$$

e nuovamente il massimo valore di n è m, ove $x = \pm 1$, $y = \pm 1$. Si vede adunque che $F_m(u, u)$ contiene il fattore

$$H_m(j) \cdot H'_{4m-1}(j),$$

e tutte le rimanenti radici appartengono a polinomii

$$H_n(j), \quad H'_{4n-1}(j)$$

con $n < m$ e quindi già noti. Se adunque, coi noti processi razionali, si libera $F_m(u, u)$ dai fattori multipli e da quelli comuni coi polinomii $H_n(j)$, $H'_{4n-1}(j)$, già calcolati, si otterrà intanto il prodotto

$$H_m(j) \cdot H'_{4m-1}(j),$$

che avrà coefficienti razionali. Per separare poi questi due fattori H_m, H'_{4m-1}, si osservi che l'equazione

$$F_{4m-1}(u, u) = 0$$

ammette il fattore $H'_{4m-1}(j)$, ma non l'altro $H_m(j)$, giacchè l'equazione

$$4m - 1 = x^2 + m y^2$$

è insolubile [1]). Il massimo comun divisore di $F_{4m-1}(u, u)$ e del prodotto $H_m(j) \cdot H'_{4m-1}(j)$ è adunque $H'_{4m-1}(j)$, che si può quindi separare razionalmente. Così, se ammettiamo dimostrato che i polinomii

$$H_n(j), \quad H'_{4n-1}(j),$$

1) Altrimenti seguirebbe $y^2 = 1$, $x^2 \equiv -1 \pmod 3$.

finchè $n < m$, hanno coefficienti razionali, lo stesso vale di $H_m(j)$, $H'_{4m-1}(j)$; e poichè i polinomii

$$H_1(j), \quad H'_3(j); \quad H_2(j), \quad H'_7(j)$$

hanno coefficienti razionali (§ 203), lo stesso vale in generale. Che poi questi coefficienti siano inoltre **interi** segue da ciò che le loro radici sono numeri interi algebrici.

Il metodo descritto pel calcolo dei polinomii $H_m(j)$, $H'_{4m-1}(j)$ ha un valore soltanto teorico, poichè, anche per valori relativamente piccoli di m, la funzione $F_m(j, j)$ è complicatissima e i calcoli da eseguirsi sarebbero immensamente laboriosi. Altri metodi si hanno per la costruzione dei detti polinomii, che sono principalmente fondati sulle proprietà di funzioni modulari più elevate e delle corrispondenti equazioni modulari; ma noi qui non possiamo occuparcene e rimandiamo alla citata opera del Weber ed alle memorie di Greenhill.

§ 205. — Gli invarianti di classi di seconda specie espressi razionalmente per quelli di prima.

A fine di poter limitare le ulteriori considerazioni ai polinomii $H_m(j)$ di prima specie e alle corrispondenti equazioni

$$H_m(j) = 0,$$

dimostreremo il teorema [1]).

Gli invarianti di seconda specie, appartenenti ad un dato determinante m, sono razionalmente esprimibili per quelli di prima specie col medesimo determinante m.

Consideriamo una radice qualsiasi

$$j = j(\omega)$$

della equazione $H_m(j) = 0$, e sia (A, B, C) una corrispondente forma di prima specie, dove quindi uno almeno dei due numeri A, C è dispari, poniamo per es. sia $A \equiv 1 \pmod 2$. Possiamo supporre anche B dispari; altrimenti colla sostituzione $\begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}$ trasformeremmo (A, B, C) nell'equivalente $(A, B + A, A + 2B + C)$, ove il coefficiente medio $B + A$ sarebbe impari.

1) WEBER, loc. cit., § 89, pag. 338.

Allora essendo

$$m = AC - B^2 \equiv -1 \pmod 4,$$

sarà necessariamente

$$C \equiv 0 \pmod 4.$$

Si consideri ora l'equazione modulare di terzo grado

$$F_2(j', j(\omega)) = 0, \tag{17}$$

le cui tre radici in j' sono

$$j'_\infty = j(2\omega), \quad j'_0 = j\left(\frac{\omega}{2}\right), \quad j'_1 = j\left(\frac{\omega + 1}{2}\right).$$

Posto ordinatamente

$$\omega' = 2\omega, \quad \omega' = \frac{\omega}{2}, \quad \omega' = \frac{\omega + 1}{2},$$

l'equazione cui soddisfa ω' sarà rispettivamente:

$$A\omega'^2 + 4B\omega' + 4C = 0 \quad \text{per } \omega' = 2\omega$$

$$2A\omega'^2 + 2B\omega' + \frac{C}{2} = 0 \quad \text{»} \quad \omega' = \frac{\omega}{2}$$

$$4A\omega'^2 + 4(B - A)\omega' + A - 2B + C = 0 \quad \text{»} \quad \omega' = \frac{\omega + 1}{2}.$$

Tutte tre le corrispondenti forme

$$(A, 2B, 4C), \quad \left(2A, B, \frac{C}{2}\right)$$

$$(4A, 2(B - A), \quad A - 2B + C)$$

sono primitive; ma le due estreme sono di prima specie, col determinante $4m$, la media invece è di seconda specie col determinante m. Dunque, delle tre radici della (17), soltanto la media $j'_0 = j\left(\frac{\omega}{2}\right)$ soddisfa anche la equazione

$$H'_m(j) = 0,$$

e perciò i due polinomii

$$H'_m(j') \quad F_2(j',\ j(\omega))$$

hanno a comune soltanto il fattore lineare

$$j' - j\left(\frac{\omega}{2}\right),$$

che si calcolerà quindi razionalmente per $j(\omega)$. Si avrà così:

$$j\left(\frac{\omega}{2}\right) = \Theta(j(\omega)), \tag{18}$$

essendo Θ il simbolo di una funzione razionale a coefficienti razionali, che sarà affatto indipendente dalla particolare radice scelta $j(\omega)$ della $H_m(u) = 0$. Ogni radice $j(\omega)$ di $H_m(j) = 0$, sostituita nella (18), dà quindi una radice j' di $H'_m(j') = 0$, ed ora vogliamo dimostrare che così si ottengono *tutte* le radici di $H'_m(j') = 0$, dopo di che sarà dimostrato il teorema enunciato. Sia $j(\omega')$ una radice di $H'_m(j) = 0$ e

$$(2A,\ B,\ 2C)$$

una corrispondente forma primitiva di seconda specie, sicchè avremo:

$$A\,\omega'^2 + B\,\omega' + C = 0$$

e potremo supporre che sia A dispari [1]).

[1]) Se A fosse pari, C impari, basterebbe cangiare ω' in $-\frac{1}{\omega'}$ e se A, C fossero ambedue pari, in $\frac{\omega'}{\omega'+1}$.

Allora, posto $\omega = 2\,\omega'$, sarà ω radice della forma primitiva di prima specie a determinante m:

$$A\,\omega^2 + 2\,B\,\omega + 4\,C = 0,$$

e perciò la radice $j(\omega')$ di $H'_m(j) = 0$ si esprimerà colla (18) per la radice $j(\omega) = j(2\,\omega')$ della $H_m(j) = 0$, c. d. d.

Le varie radici $j(\omega)$ di $H_m(j) = 0$, sostituite in (18), dànno *tutte* e sole le radici di $H'_m(j) = 0$; ma vogliamo ora esaminare ulteriormente la questione se queste radici di $H'_m(j) = 0$ si troveranno o no ripetute. Per decidere la cosa osserviamo che, se due radici differenti $j(\omega)$, $j(\omega_1)$ di $H_m(j) = 0$ dànno, sostituite nella (18), la medesima radice $j(\omega')$ di $H'_m(j) = 0$, dovranno $j(\omega)$, $j(\omega_1)$ essere ambedue radici della equazione modulare

$$F_2(j',\ j(\omega')) = 0.$$

Ma queste radici sono

$$j(2\,\omega'),\quad j\left(\frac{\omega'}{2}\right),\quad j\left(\frac{\omega'+1}{2}\right), \tag{19}$$

e si tratta dunque di vedere in primo luogo quali di questi tre valori sono radici di $H_m(j) = 0$. Ora, posto successivamente

$$\omega = 2\,\omega',\quad \omega = \frac{\omega'}{2},\quad \omega = \frac{\omega'+1}{2},$$

dall'equazione

$$A\,\omega'^2 + B\,\omega' + C = 0$$

si deduce che ω sarà rispettivamente radice dell'equazione

$$\begin{aligned}
A\,\omega^2 + 2\,B\,\omega + 4\,C &= 0 \quad \text{per} \quad \omega = 2\,\omega' \\
4\,A\,\omega^2 + 2\,B\,\omega + C &= 0 \quad \text{»} \quad \omega = \frac{\omega'}{2} \\
4\,A\,\omega^2 + 2\,(B - 2\,A)\,\omega + A - B + C &= 0 \quad \text{»} \quad \omega = \frac{\omega'+1}{2}
\end{aligned}$$

e le tre forme corrispondenti hanno ancora il determinante m. Di esse però la prima è certamente primitiva (di prima specie), le altre due invece, come subito vediamo, saranno imprimitive se $m \equiv -1 \pmod 8$, primitive quando $m \equiv 3 \pmod 8$. E infatti siccome

$$4AC - B^2 = m,$$

e $B^2 \equiv +1 \pmod 8$, perchè B è dispari, sarà nel primo caso $AC \equiv 0 \pmod 2$ e nel secondo $AC \equiv 1 \pmod 2$ e quindi, essendo A impari, sarà C pari se $m \equiv -1 \pmod 8$, impari se $m \equiv 3 \pmod 8$.

Dunque se $m \equiv -1 \pmod 8$, dei tre valori (19) solo il primo è radice di $H_m(j) = 0$ ed ogni invariante di seconda specie ne dà uno solo di prima specie, cioè: *Se* $m \equiv -1 \pmod 8$ *gli invarianti di prima specie si esprimono razionalmente per quelli di seconda.*

Nel caso $m \equiv 3 \pmod 8$ tutti tre i valori (19) sono invarianti di prima specie, e rimane soltanto da vedere se sono differenti o no, se cioè fra i tre valori

$$2\omega', \quad \frac{\omega'}{2}, \quad \frac{\omega'+1}{2}$$

ve ne sono due equivalenti. Basterà esaminare se i due primi $2\omega'$, $\frac{\omega'}{2}$ possono essere equivalenti, gli altri casi riducendosi a questo col cangiare ω' in $\omega'+1$, ovvero in $-\frac{1}{\omega'}$. Supponiamo dunque che sia

$$2\omega' = \frac{\alpha\frac{\omega'}{2} + \beta}{\gamma\frac{\omega'}{2} + \delta}$$

con $\alpha, \beta, \gamma, \delta$ interi e $\alpha\delta - \beta\gamma = 1$; avremo

$$2\gamma\omega'^2 + (4\delta - \alpha)\omega' - 2\beta = 0,$$

che, paragonata con

$$A\omega'^2 + B\omega' + C = 0,$$

dà

$$2\gamma = xA, \quad 4\delta - \alpha = xB, \quad -2\beta = xC,$$

dove x sarà un intero (perchè A, B, C non hanno divisor comune) evidentemente pari; e se poniamo

$$4\delta + \alpha = y,$$

sarà pure y un intero pari, e dalle formole

$$2\alpha = y - Bx, \quad 2\beta = -Cx, \quad 2\gamma = Ax, \quad 8\delta = y + Bx$$

si trae

$$16(\alpha\delta - \beta\gamma) = 16 = y^2 + mx^2,$$

equazione solubile soltanto per $m = 3$. In questo caso i tre valori

$$2\omega', \quad \frac{\omega'}{2}, \quad \frac{\omega'+1}{2}$$

sono fra loro equivalenti.

Vediamo dunque che se $m \equiv 3 \pmod 8$, e non è $m = 3$, le radici $j(\omega)$ di $H_m(j) = 0$, sostituite nella (18), dànno tre a tre la medesima radice di $H'_m(j)$. Se si indica quindi con h il numero delle classi delle forme primitive di prima specie a determinante m, con h' quello delle classi di seconda specie, si avrà

$$h' = h \quad \text{per } m \equiv -1 \pmod 8$$
$$h' = \frac{h}{3} \quad \text{per } m \equiv 3 \pmod 8,$$

eccettuato $m = 3$ ove nuovamente $h' = h$ [1]).

[1]) DIRICHLET-DEDEKIND, *Zahlentheorie*, § 97 e Supplemento X.

CAPITOLO XIX.

Composizione delle forme quadratiche e gruppo di Galois per l'equazione degli invarianti delle classi.

§ 206. — Composizione delle forme quadratiche secondo Gauss.

Nella ricerca degli invarianti assoluti delle classi tutto si riduce, per quanto sopra si è visto, allo studio dell'equazione

$$H_D(j) = 0, \tag{1}$$

le cui radici sono gli invarianti appartenenti alle classi di prima specie a determinante D. Secondo un teorema enunciato da Abel[1]), l'equazione (1), che ha per radici gli invarianti delle classi, è un'equazione risolubile per radicali. Il gruppo di Galois per quest'equazione, quando al campo assoluto di razionalità si aggiunga il radicale quadratico $i\sqrt{D}$, è un gruppo Abeliano (di sostituzioni permutabili); esso coincide (è oloedricamente isomorfo) col gruppo *di composizione*, secondo Gauss, delle forme quadratiche di prima specie a determinante D. Così la teoria della composizione delle forme, data da Gauss nelle *Disquisitiones arithmeticae*, contiene già tutti gli elementi necessarii per la conoscenza delle equazioni per gli invarianti delle classi, dal punto di vista della teoria di Galois.

Noi ci proponiamo qui, come ultima ricerca, di stabilire le enunciate proprietà, il che ci obbliga a riassumere brevemente la teoria della composizione delle forme quadratiche, rimandando per maggiori notizie al X. Supplemento dell'opera di Dirichlet-Dedekind e alle lezioni litografate di Klein[2]), alle quali ci atteniamo nell'esposizione seguente. Consideriamo una forma quadratica

$$(a,\ b,\ c),$$

1) L'enunciato d'ABEL si riferisce naturalmente ai moduli k^2 di LEGENDRE.

2) Ausgewählte Kapitel der *Zahlentheorie*, Göttingen, 1896.

che supporremo senz'altro primitiva di prima specie. Essa determina una classe di funzioni ellittiche, nelle quali il rapporto τ dei periodi è dato da

$$\tau = \frac{\omega'}{\omega} = \frac{-b+i\sqrt{D}}{a},$$

e i periodi 2ω, $2\omega'$ sono determinati a meno di un fattor comune di proporzionalità. Consideriamo i vertici della rete parallelogrammica appartenente alla $\wp(u\,|\,\omega,\ \omega')$, che sono nei punti

$$u = 2\omega\,.\,x + 2\omega'\,.\,y, \tag{2}$$

percorrendo x, y tutti i valori interi.

L'insieme di tutti questi punti si dirà il *reticolo* appartenente alla forma $(a,\ b,\ c)$; esso sarà determinato solo a meno di una rotazione attorno all'origine e di un'omotetia rispetto all'origine stessa. Per fissare le idee prendiamo

$$2\omega = \sqrt{a},\quad 2\omega' = \frac{-b+i\sqrt{D}}{\sqrt{a}}$$

e il reticolo consterà allora dei punti

$$M = \sqrt{a}\,x + \frac{-b+i\sqrt{D}}{\sqrt{a}}\,y. \tag{3}$$

Da considerazioni già svolte in altra occasione (vedi Cap. II, § 23 e Cap. VIII, § 95) risulta il teorema: *Se due forme quadratiche primitive $(a,\ b,\ c)$, $(a',b',\ c')$ hanno il medesimo reticolo, ovvero reticoli che si cangiano l'uno nell'altro per rotazione ed omotetia rispetto all'origine, esse sono equivalenti.*

Veniamo ora all'oggetto proprio di questo paragrafo, cioè alla *composizione* dei reticoli e delle forme. Siano (a, b, c), (a', b', c') due forme quadratiche primitive di prima specie e di egual determinante D, e si considerino i rispettivi reticoli

$$M = \sqrt{a}\,x + \frac{-b+i\sqrt{D}}{\sqrt{a}}\,y$$

$$M' = \sqrt{a'}\,x' + \frac{-b'+i\sqrt{D}}{\sqrt{a'}}\,y'.$$

Facciamo tutti i possibili prodotti $M M'$ di un numero del primo reticolo per un numero del secondo e addizioniamo quanti si vogliano di questi prodotti, moltiplicati per numeri interi arbitrarii. Dimostreremo che *i numeri così ottenuti sono tutti e soli i vertici di un terzo reticolo, appartenente ad una terza forma quadratica a determinante D.* Il terzo reticolo si dirà il reticolo *composto* dei due e la terza forma si dirà composta delle due (a, b, c), (a', b', c'). Già prima di eseguire il nostro calcolo osserviamo che, siccome a forme equivalenti appartiene il medesimo reticolo e inversamente, si avrà senz'altro il teorema: *La classe della forma composta dipende unicamente dalle classi delle due forme componenti.*

Per dimostrare ora il teorema fondamentale cominciamo dal prendere due forme dalle rispettive classi delle due forme date, che abbiano i primi coefficienti a, a' primi fra loro ed eguale coefficiente medio $b' = b$, ciò che vediamo subito esser sempre possibile. E infatti possiamo intanto supporre che i due primi coefficienti a, a' siano primi fra loro, poichè ad ogni forma primitiva possiamo sostituirne una equivalente il cui primo coefficiente sia primo col numero che più ci piace [1]). Ed ora, mediante le sostituzioni rispettive

$$\begin{pmatrix}1, & m\\ 0, & 1\end{pmatrix}, \quad \begin{pmatrix}1, & n\\ 0, & 1\end{pmatrix},$$

si traducano le forme

$$(a,\ b,\ c),\quad (a',\ b',\ c')$$

nelle equivalenti

$$(a\ ,\ b + a\,m,\ c + 2\,b\,m + a\,m^2)$$

$$(a',\ b' + a'\,n,\ c' + 2\,b'\,n + a'\,n^2),$$

e si determinino i numeri interi m, n in guisa che risulti

$$b + a\,m = b' + a'\,n,$$

cioè

$$a\,m - a'\,n = b' - b,$$

1) Cf. DIRICHLET-DEDEKIND, § 93.

il che è sempre possibile, essendo a, a' primi fra loro. Otterremo così due forme equivalenti alle primitive

$$f_1 = (a,\ b,\ c),\quad f_2 = (a',\ b,\ c')$$

in cui a, a' saranno primi fra loro e il coefficiente medio b sarà il medesimo. Si osservi ora che, il determinante D essendo il medesimo, si ha

$$a\,c = a'\,c'$$

e poichè a, a' sono primi fra loro avremo

$$c = a'\,C,\quad c' = a\,C,$$

essendo C un conveniente terzo numero. Le due forme saranno quindi

$$f_1 = (a,\ b,\ a'\,C),\quad f_2 = (a',\ b,\ a\,C). \tag{4}$$

Come si è visto, in due classi qualunque possiamo scegliere due tali forme (4) in cui a, a' siano primi fra loro. Ma, per le applicazioni che dovremo farne fra breve, converrà che consideriamo il caso più generale in cui nelle forme (4) si supponga soltanto che i tre numeri

$$a,\ a',\ 2\,b$$

non abbiano alcun divisore comune. Se questa condizione è soddisfatta, le due forme (4) si diranno *concordanti.*

Ora si prendano due numeri dei corrispondenti reticoli

$$\begin{cases} M_1 = \sqrt{a}\ x + \dfrac{-b + i\sqrt{D}}{\sqrt{a}}\ y \\[2ex] M_2 = \sqrt{a'}\ x' + \dfrac{-b + i\sqrt{D}}{\sqrt{a'}}\ y'\ ; \end{cases}$$

moltiplicandoli fra loro troviamo, a causa della formola

$$a\,a'\,C - b^2 = D:$$

$$M_1\,M_2 = \sqrt{a\,a'}\,.\,(x\,x' - C\,y\,y') + \tag{5}$$

$$+ \frac{-b + i\sqrt{D}}{\sqrt{a\,a'}}\,(a\,x\,y' + a'\,x'\,y - 2\,b\,y\,y').$$

Questi prodotti $M_1 M_2$, e quindi anche la somma di quanti si vogliano di essi, sono numeri del terzo reticolo

$$M_3 = \sqrt{a a'}\, X + \frac{-b + i\sqrt{D}}{\sqrt{a a'}}\, Y, \tag{6}$$

appartenente alla forma

$$f_3 = (a a', b, C),$$

che è ancora a determinante D e primitiva di prima specie, come f_1, f_2. Ma vogliamo di più dimostrare che coi prodotti (5) e colle loro somme si ottengono tutti i numeri del terzo reticolo (6).

Basterà per ciò constatare che si possono ottenere nel detto modo i due numeri fondamentali del terzo reticolo

$$\sqrt{a a'}, \quad \frac{-b + i\sqrt{D}}{\sqrt{a a'}}.$$

Quanto al primo si ottiene subito come prodotto di $M_1 = \sqrt{a}$ per $M_2 = \sqrt{a'}$; se facciamo poi

$$M_1 = \sqrt{a}, \quad M'_1 = \frac{-b + i\sqrt{D}}{\sqrt{a}}$$

$$M_2 = \sqrt{a'}, \quad M'_2 = \frac{-b + i\sqrt{D}}{\sqrt{a'}},$$

abbiamo

$$M_1 M'_2 = \frac{-b + i\sqrt{D}}{\sqrt{a a'}} \cdot a, \quad M_2 M'_1 = \frac{-b + i\sqrt{D}}{\sqrt{a a'}}\, a'$$

$$M'_1 M'_2 + C M_1 M_2 = 2b\, \frac{b - i\sqrt{D}}{\sqrt{a a'}},$$

che sono numeri formati dai due reticoli nel modo prescritto, ed ora, indicando con

$$m, \; n, \; p$$

tre interi qualunque, sarà pure uno dei detti numeri:

$$m M_1 M'_2 + n M'_1 M_2 - p(M'_1 M'_2 + C M_1 M_2) =$$
$$= \frac{-b + i\sqrt{D}}{\sqrt{a a'}}(a m + a' n + 2 b p)$$

ed, essendo a, a', $2b$ primi fra loro, potremo rendere

$$a m + a' n + 2 b p = 1,$$

il che dimostra quanto volevamo. Così abbiamo stabilito il teorema fondamentale della composizione delle forme e ritrovata la regola seguente:

Per comporre due classi K, K' di forme (primitive di prima specie) di egual determinante, si scelgano dalle due classi due forme concordanti

$$(a, b, a' C), \quad (a', b, a C),$$

nelle quali a, a', $2b$ siano primi fra loro, e la forma composta sarà

$$(a a', b, C).$$

Denoteremo la classe composta K'' col simbolo

$$K'' = K K',$$

come prodotto delle due classi componenti, ove l'ordine dei fattori sarà naturalmente indifferente.

§ 207. — Gruppo di composizione delle forme.

Consideriamo tutte le classi di forme primitive di prima specie di un dato determinante D; se h è il loro numero, indichiamo queste h classi distinte con

$$K_1, \; K_2, \; K_3, \ldots, K_h. \tag{7}$$

Componiamo le h classi di questo sistema completo con una qualunque di esse, presa ad arbitrio, K_i. Le h classi composte

$$(8) \qquad K_1 K_i, \ K_2 K_i, \ldots, K_h K_i$$

si troveranno certamente fra le (7) e siccome, come ora dimostreremo, nessuna classe è ripetuta nel sistema (8), così le (8) saranno, in altro ordine, le (7) stesse, sicchè la composizione di tutte le classi con una determinata K_i dà luogo ad una *sostituzione* fra le h classi, che indicheremo con s_i.

Per dimostrare la nostra asserzione facciamo le due seguenti osservazioni:

1ª Sia K_1 la classe principale, contenente cioè la forma principale $(1, 0, D)$. Questa forma principale, composta con ogni altra forma (a, b, c), dà la forma (a, b, c) stessa. E infatti la forma $(1, 0, D)$ è equivalente alla forma $(1, b, ac)$, che è concordante con (a, b, c), e composta con essa, secondo la regola del § 206, dà appunto (a, b, c). Per ciò la classe principale K_1 si indicherà anche col simbolo 1.

2ª Sia (a, b, c) una forma qualunque e si consideri la sua *opposta* $(a, -b, c)$, che mediante la sostituzione $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$ si traduce nella equivalente (c, b, a). Possiamo sempre supporre che a, c siano primi fra loro, altrimenti ci ridurremo a questo caso trasportando (a, b, c), mediante una sostituzione $\begin{pmatrix} 1, & m \\ 0, & 1 \end{pmatrix}$, in una forma equivalente

$$(a, b + am, \quad c + 2bm + am^2),$$

e prendendo m primo col massimo comun divisore di a, c. Allora le due forme

$$(a, b, c), \quad (c, b, a)$$

sono concordanti e composte dànno la classe principale

$$(ac, b, 1) \equiv (1, -b, ac) \equiv (1, 0, D).$$

Dunque: *Ogni classe K composta colla sua opposta K' dà la classe principale* 1.

Ciò premesso, se si avessero due classi eguali nella serie (8), per es.

$$K_a K_i = K_b K_i,$$

componendo colla opposta K'_i di K_i risulterebbe $K_a = K_b$.

Ad ogni classe K_i, adoperata come classe moltiplicatrice di tutte le classi (7), corrisponde adunque una sostituzione s_i sulle classi stesse, ed è chiaro che ad una classe composta

$$K_i \ K_j$$

corrisponde la sostituzione prodotto

$$s_i \ s_j$$

e alla classe opposta K_i^{-1} di K_i la sostituzione inversa s_i^{-1}, sicchè se K_i è diversa da K_j anche s_i è diversa da s_j.

Così adunque: *Le h sostituzioni sulle classi*

$$s_1 = 1, \ s_2, \ s_3, \ldots, s_h$$

formano un gruppo d'ordine h di sostituzioni permutabili sulle h classi.

Questo è evidentemente un gruppo Abeliano semplicemente transitivo sulle h classi; esso dicesi *il gruppo di composizione delle forme*.

Diremo *periodo* di una classe K il minimo esponente positivo β, a cui bisogna elevare la classe per ottenere la classe principale 1. Evidentemente sarà allora $K^{\beta-1}$, o K^{-1}, la classe opposta di K.

Meritano particolare menzione quelle classi che coincidono colle proprie opposte, che sono cioè a periodo 2; esse diconsi, secondo Gauss, classi *ancipiti* o *ambigue*. Se (a, b, c) è una forma ancipite, equivalente cioè ad $(a, -b, c)$, i due indici equivalenti $\frac{-b + i\sqrt{D}}{a}$, $\frac{b + i\sqrt{D}}{a}$ sono simmetrici rispetto all'asse immaginario e per ciò, supposta la forma ridotta, il suo indice sarà sul contorno del triangolo fondamentale, onde si vede che sussiste il teorema: *Gli invarianti delle classi ancipiti e questi soltanto sono reali.*

Essendo il gruppo di composizione un gruppo Abeliano, potremo scegliere fra le h classi un certo numero r di classi fondamentali

$$k_1, \; k_2, \; \ldots, \; k_r$$

per formare una *base* del gruppo [1]) e se

$$\beta_1, \; \beta_2, \; \ldots, \; \beta_r$$

sono i rispettivi periodi di $k_1, k_2, \ldots, k_r$, tutte le h forme saranno date dalle espressioni

$$(a) \qquad k_1^{\alpha_1} k_2^{\alpha_2} \ldots k_r^{\alpha_r} \left\{ \begin{array}{l} \alpha_1 = 0, \; 1, \; 2, \; \ldots, \; \beta_1 - 1 \\ \alpha_2 = 0, \; 1, \; 2, \; \ldots, \; \beta_2 - 1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \alpha_r = 0, \; 1, \; 2, \; \ldots, \; \beta_r - 1, \end{array} \right.$$

nè alcuna forma si troverà così ripetuta, sicchè sarà

$$h = \beta_1 \cdot \beta_2 \ldots \beta_r .$$

Una forma (a) sarà ancipite se sussisteranno le congruenze

$$2\,\alpha_1 \equiv 0 \pmod{\beta_1}, \; 2\,\alpha_2 \equiv 0 \pmod{\beta_2} \; \ldots \; 2\,\alpha_r \equiv 0 \pmod{\beta_r};$$

e poichè se per es. β_1 è impari, ne risulta $\alpha_1 \equiv 0 \pmod{\beta_1}$, mentre se β_1 è pari vi è l'altra soluzione $\frac{\beta_1}{2}$, vediamo che *il numero delle classi ancipiti è dato da* 2^n [2]), essendo n il numero dei periodi fondamentali $\beta_1, \beta_2, \ldots, \beta_r$ che sono pari.

§ 208. — Teoremi vari sulla composizione delle forme.

Prima di applicare la teoria della composizione delle forme all'equazione degli invarianti delle classi, conviene che dimo-

[1]) Vedi *Teoria dei gruppi*.

[2]) Naturalmente è qui computata fra le classi ancipiti anche la principale (a periodo 1).

striamo ancora alcuni teoremi relativi alla composizione, in primo luogo il seguente:

Ogni forma (A, B, C) *si può ottenere come risultato di composizione di successive forme*

$$(p, b, c), \quad (p', b', c'), \quad (p'', b'', c''), \ldots,$$

i cui primi coefficienti $p, p', p'', \ldots,$ *sono numeri primi* [1]).

Prendiamo la forma (A, B, C) in guisa che il primo coefficiente sia dispari e primo con D e sia p un fattore primo di A, che, non dividendo D, non dividerà nemmeno B. Ora le due forme primitive di prima specie a determinante D

$$\left(p, B, \frac{A\,C}{p}\right), \quad \left(\frac{A}{p}, B, C\,p\right)$$

sono evidentemente concordanti, e composte fra loro, dànno appunto

$$(A, B, C) = \left(p, B, \frac{A\,C}{p}\right) \cdot \left(\frac{A}{p}, B, C\,p\right).$$

Similmente, se p' è un divisore primo di $\frac{A}{p}$, avremo

$$\left(\frac{A}{p}, B, C\,p\right) = \left(p', B, \frac{A\,C}{p'}\right) \left(\frac{A}{p\,p'}, B, C\,p\,p'\right).$$

Così continuando, vediamo che, se si scinde A nei suoi fattori primi $p, p', p'', \ldots,$ diversi od eguali

$$A = p\,p'\,p'' \ldots,$$

la forma (A, B, C) si otterrà componendo le successive

$$\left(p, B, \frac{A\,C}{p}\right), \quad \left(p', B, \frac{A\,C}{p'}\right), \quad \left(p'', B, \frac{A\,C}{p''}\right) \ldots,$$

ciò che dimostra il teorema.

[1]) Un teorema molto più generale, la cui dimostrazione è dovuta a WEBER, assicura che in ogni classe primitiva di prima specie vi sono infinite forme il cui primo coefficiente è un numero primo, che cioè fra i numeri rappresentabili da una tale forma ve ne sono infiniti primi. Ma la dimostrazione di questo teorema è assai riposta; per le applicazioni attuali basta la proposizione del testo.

Consideriamo ora in particolare una forma

$$P = (p, b, c),$$

il cui primo coefficiente p sia un numero primo dispari che non divida D, del quale quindi $-D$ sarà residuo quadratico, a causa di

$$pc - b^2 = D,$$

e sia β il periodo della classe P. Alla forma (p, b, c) possiamo sostituirne una equivalente (p, B, C), in cui sia

$$B \equiv b \pmod{p}, \quad B^2 \equiv -D \pmod{p^\beta}.$$

Come si sa [1]), essendo $\left(\frac{-D}{p}\right) = +1$, la seconda congruenza è sempre solubile ed ha due radici opposte incongrue (mod p), ed una di esse è appunto $\equiv b$ (mod p). Se poniamo

$$B^2 + D = C p^\beta,$$

avremo

$$P = (p, B, C p^{\beta - 1}).$$

Essendo p primo con $2B$, potremo comporre la classe P con sè stessa ed avremo

$$P^2 = (p^2, B, C p^{\beta - 2}).$$

Similmente

$$P^3 = (p^3, B, C p^{\beta - 3})$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$P^{\beta - 1} = (p^{\beta - 1}, B, C p)$$

$$P^\beta = (p^\beta, B, C);$$

e poichè per ipotesi P^β è la minima potenza di P che coincide colla classe principale $(1, 0, D)$, se ne conclude che la potenza p^β di p è rappresentabile dalla forma principale

$$x^2 + D y^2$$

ed è la minima per la quale ciò accade.

1) DIRICHLET, *Zahlentheorie*, § 35.

Dunque: *Se p è un numero primo non divisore di $2D$ e tale che $\left(\frac{-D}{p}\right) = +1$, esiste una minima potenza p^β di p per la quale è risolubile l'equazione*

$$p^\beta = x^2 + D y^2;$$

questo esponente β è anche il periodo delle due classi opposte rappresentate da forme P col primo coefficiente $= p$.

§ 209. — **Trasformazione degli invarianti delle classi.**

Dopo queste necessarie preparazioni, veniamo ad un'altra parte della ricerca che utilizza le proprietà delle equazioni modulari, esaminando l'effetto della trasformazione sugli invarianti di classi.

Introduciamo per ciò un'opportuna notazione abbreviata, che ci sarà molto utile. Essendo

$$K_1, K_2, \ldots, K_h$$

un sistema completo di classi, o di forme loro rappresentanti, a determinante D e primitive di prima specie, indichiamo i corrispondenti valori degli invarianti di classi con

$$j_{K_1}, j_{K_2}, j_{K_h}, \tag{9}$$

ciò che si potrà fare senza alcuna ambiguità, la classe determinando completamente il corrispondente valore dell'invariante e reciprocamente. Gli h valori (9) saranno allora tutte e sole le radici dell'equazione

$$H_D(j) = 0. \tag{10}$$

Prendiamo ad arbitrio una classe K e la corrispondente radice j_K della (10) e indichiamo con p *un numero primo che non divida D e di cui $-D$ sia residuo quadratico.* Come è ben noto, e dimostrabile elementarmente, vi sono infiniti numeri primi di questa specie [1]).

Scegliamo la forma (A, B, C), rappresentante della classe K, in guisa che i coefficienti estremi A, C siano ambedue divisibili per p, ciò che facilmente si vede esser sempre possibile [2]). Essendo ora ω l'indice della forma (A, B, C), cioè

$$A\,\omega^2 + 2\,B\,\omega + C = 0,$$

[1]) La proprietà enunciata nel testo equivale a dire che se nell'espressione $x^2 + D$ si fanno percorrere a x gli infiniti numeri interi primi con D, i numeri ottenuti offriranno una serie illimitata di divisori primi. Ciò si dimostra subito osservando che se $p_1, p_2, \ldots, p_r$ è una serie finita di numeri primi, non divisori di D, e si pone $x = p_1 . p_2 \ldots p_r\, y$ con y intero, il numero $x^2 + D$ ha i suoi divisori primi fuori di $p_1, p_2, \ldots, p_r$.

[2]) In primo luogo, se A non è già divisibile per p trasformando (A, B, C) colla sostituzione $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$, il nuovo coefficiente A è dato da

$$A\,\alpha^2 + 2\,B\,\alpha\,\gamma + C\,\gamma^2,$$

e possiamo sempre prendere α, γ primi fra loro in guisa che risulti

$$A\,\alpha^2 + 2\,B\,\alpha\,\gamma + C\gamma^2 \equiv 0 \pmod{p},$$

cioè

$$(A\,\alpha + B\,\gamma)^2 \equiv -D\,\gamma^2 \pmod{p}.$$

Essendo ν una radice di $\nu^2 \equiv -D \pmod{p}$, basta porre infatti $\alpha \equiv \mu\,\gamma$ e determinare μ da

$$A\,\mu + B \equiv \pm\,\nu \pmod{p}.$$

Supposto ora $A = p^r A'$ e A' non divisibile per p, alla forma

$$(A,\ B,\ C)$$

se ne può sostituire una equivalente

$$(A,\ B + \lambda\,A,\ C'),$$

determinando λ in guisa che sia

$$(B + \lambda\,A)^2 = (B + \lambda\,p^r A')^2 \equiv B^2 + 2\,B\,\lambda\,p^r\,A' \equiv -D \pmod{p^{r+1}},$$

per il che essendo

$$B^2 + D = A\,C = p^r\,A'\,C,$$

basterà prendere λ in guisa che si abbia

$$2\,B\,\lambda \equiv -C \pmod{p}.$$

Ma allora, poichè $A\,C' - (B + \lambda A)^2 = D$, sarà $A\,C'$ divisibile per p^{r+1} e perciò C' per p, come si voleva.

assoggettiamo l'invariante $j(\omega) = j_K$ alla trasformazione d'ordine p e, considerando la corrispondente equazione modulare

$$F_p(j',\ j(\omega)) = F_p(j',\ j_K) = 0, \tag{11}$$

esaminiamo se la (11) ha radici comuni colla (10), e quali. Per ciò ricordiamo che le radici della (11) sono

$$j'_\infty = j(p\,\omega),\quad j'_\nu = j\left(\frac{\omega + \nu}{p}\right),$$

percorrendo ν un sistema completo di resti (mod p). Ora, posto successivamente

$$\omega' = p\,\omega,\quad \omega' = \frac{\omega + \nu}{p},$$

vediamo che nel primo caso ω' soddisfa all'equazione

$$\frac{A}{p}\,\omega'^2 + 2\,B\,\omega' + C\,p = 0, \tag{12}$$

mentre nell'altro si ha:

$$A\,p^2 \cdot \omega'^2 + 2\,p\,(B - A\,\nu)\,\omega' + (A\,\nu^2 - 2\,B\,\nu + C) = 0.$$

Quando ν è differente da zero (mod p) i tre coefficienti

$$A\,p^2,\ \ 2\,p\,(B - A\,\nu),\ \ A\,\nu^2 - 2\,B\,\nu + C$$

sono primi fra loro e quindi le radici

$$j'_1,\ j'_2,\ \ldots,\ j'_{p-1}$$

sono bensì invarianti di classi, ma col determinante $D\,p^2$ e non soddisfano per ciò la (10). Quando invece $\nu = 0$, si ha

$$A\,p\,\omega'^2 + 2\,B\,\omega' + \frac{C}{p} = 0,$$

e tanto la forma

$$\left(\frac{A}{p},\ B,\ C\,p\right),$$

corrispondente alla (12), come la $\left(A\,p,\ B,\ \frac{C}{p}\right)$ corrispondente alla precedente, sono primitive di prima specie a determinante D. Dunque si conclude che: *La* (11) *ha a comune colla* (10) *soltanto le due radici*

$$j'_\infty = j(p\,\omega),\quad j'_0 = j\left(\frac{\omega}{p}\right).$$

Conviene ora vedere quali sono le classi K_i, K_r, indici di queste due radici. Per ciò si osservi che posto

$$P = \left(p,\ B,\ \frac{A\,C}{p}\right),$$

si ha (§ 208)

$$\left(A\,p,\ B,\ \frac{C}{p}\right) = \left(p,\ B,\ \frac{A\,C}{p}\right) \cdot (A,\ B,\ C),$$

cioè la classe di $\left(A\,p,\ B,\ \frac{C}{p}\right)$ è la classe composta $P\,K$, sicchè $j'_0 = j_{PK}$.

D'altronde l'altra forma $\left(\frac{A}{p},\ B,\ C\,p\right)$ è equivalente a

$$\left(C\,p,\ -B,\ \frac{A}{p}\right),$$

che si compone delle due

$$P^{-1} = \left(p, -B,\ \frac{A\,C}{p}\right),\quad K = (A,\ B,\ C)$$

e perciò $j'_\infty = j_{P^{-1}K}$.

Abbiamo dunque il teorema: *Se si trasforma un invariante* j_K *di una classe* K *(primitiva di prima specie) a determinante* D *mediante una trasformazione di grado primo* p *non divisore di* D, *e di cui* $-D$ *sia residuo quadratico, l'equazione modulare* (11)

$$F_p(j',\ j_K) = 0$$

ha due sole radici a comune colla (10)

$$H_D(j') = 0,$$

e queste sono gli invarianti di classi

$$j_{PK},\ j_{P^{-1}K},$$

essendo P, P^{-1} *le due classi opposte rappresentate da forme con primo coefficiente* p.

Ora si hanno due casi essenzialmente diversi, secondo che la classe P è ancipite o no, secondo che cioè il periodo di P è $= 2$ ovvero > 2.

1º caso. — Nel primo caso è $P = P^{-1}$ e le due radici j_{PK}, $j_{P^{-1}K}$ coincidono in un' unica radice doppia della (11), che è invece radice semplice della (10). Il massimo comun divisore dei primi membri delle (10), (11) è

$$j' - j_{PK},$$

e, calcolando coi processi di ordinaria divisione, si otterrà j_{PK} in funzione razionale $f(j_K)$ di j_K a coefficienti interi; questa funzione razionale f dipenderà unicamente dal numero primo p, cioè dalla classe P e nulla affatto dalla classe K, i calcoli indicati eseguendosi sulle (10), (11) riguardando in quest'ultima j_K come un parametro. Denoteremo per ciò la funzione razionale f con f_P sicchè avremo

$$j_{PK} = f_P(j_K), \tag{13}$$

e questa relazione varrà qualunque sia la classe K. Abbiamo dunque il teorema:

Se P *è una classe a periodo 2 (ancipite) (ed esiste un numero primo* p *rappresentabile dalla forma* P [1])*, preso l'invariante* j_K *di una qualunque classe* K, *l'invariante* j_{PK} *della classe composta* PK *è esprimibile razionalmente per* j_K *mediante la* (13), *la* f_P *avendo coefficienti interi e dipendendo unicamente dalla classe* P.

2º caso. — La P sia una classe non ancipite. Allora le due radici

$$j_{PK},\ j_{P^{-1}K},$$

[1]) Quest'ultima condizione non è veramente necessaria, trovandosi sempre soddisfatta pel teorema di Dirichlet (Cf. sopra).

che la (10) ha a comune colla (11), sono distinte e il massimo comun divisore dei due primi membri, che calcoliamo nuovamente in modo razionale per j_K, è il polinomio di secondo grado

$$j'^2 - (j_{PK} + j_{P^{-1}K})\, j' + j_{PK} \cdot j_{P^{-1}K},$$

onde vediamo che in questo caso potremo scrivere dapprima soltanto

$$(14) \qquad \begin{cases} j_{PK} + j_{P^{-1}K} = f_P(j_K) \\ j_{PK} \cdot j_{P^{-1}K} = F_P(j_K), \end{cases}$$

indicando nuovamente f_P, F_P funzioni razionali di j_K con coefficienti interi e dipendenti unicamente dalla classe P, non da K.

Si tratta ora di separare le due radici e ottenere per es. j_{PK} in funzione razionale di j_K. Ciò è sempre possibile, come dimostreremo; però la nuova funzione razionale di j_K che eguaglia j_{PK} non avrà più coefficienti razionali, ma conterrà invece nei coefficienti l'irrazionalità $i\sqrt{D}$, talchè potremo scrivere

$$(15) \qquad j_{PK} = \varphi_P(j_K, i\sqrt{D}),$$

la funzione razionale φ_p *dei due argomenti* j_K, $i\sqrt{D}$ *avendo coefficienti interi e dipendendo ancora unicamente dalla forma componente* P, *non dalla* K.

Nella dimostrazione di quest'importante risultato, cioè della formola (15), consiste l'ultimo passo che ci resta a fare per condurre a termine la nostra ricerca.

Un primo metodo per stabilire il teorema enunciato si fonda sulle proprietà delle così dette equazioni del *moltiplicatore* [1]; ma non avendo noi potuto trattare nel presente corso di queste speciali equazioni (risolventi dell'equazione per la divisione dei periodi), non possiamo seguire questa via.

Un secondo metodo, dato da Sylow [2]) pel caso del modulo k^2, e che utilizza le proprietà delle equazioni modulari e quelle proprie della moltiplicazione complessa, conduce pure, per via molto naturale, al risultato stesso ed è appunto il metodo che qui adotteremo.

[1]) Cf. WEBER, loc. cit.; PICK, *Math. Annalen*, 25; KLEIN, loc. cit.
[2]) *Journal de Mathém.*, 1887.

§ 210. — Ritorno all'equazione per la divisione dei periodi e determinazione del suo gruppo.

Ci conviene per ciò ritornare all'equazione per la divisione dei periodi della generale funzione ellittica $\wp u$ in p parti eguali (p numero primo) per determinarne il gruppo di monodromia rispetto ai parametri g_2, g_3 e il gruppo algebrico, quando al campo naturale di razionalità (dei numeri razionali) si aggiungano le indeterminate g_2, g_3 [1]).

Ricordiamo che le $\frac{p^2-1}{2}$ radici

$$(16) \qquad y_{r,s} = \wp\left(\frac{2r\omega + 2s\omega'}{p}\right)$$

dell'equazione

$$(17) \qquad \psi_p(y) = 0$$

per la divisione dei periodi si ottengono facendo percorrere agli indici (r, s) la metà di un sistema completo di $p^2 - 1$ coppie $(\bmod p)$, esclusa la coppia $(0, 0)$, sicchè queste coppie (r, s) insieme colle opposte $(-r, -s)$, che dànno la medesima radice $y_{r,s}$ percorrano il detto sistema completo, esclusa la coppia $(0, 0)$ (Cfr. §§ 114, 115). Per ciò gli indici r, s nella (16) si intendono presi $(\bmod p)$ e si riguardano come identiche le coppie opposte.

Per determinare il gruppo Γ di monodromia della (17) dobbiamo far descrivere ai parametri g_2, g_3, nei loro rispettivi piani complessi, cammini chiusi ed esaminare la sostituzione indotta sulle radici $y_{r,s}$. Ma, quando g_2, g_3 riprendono i medesimi valori, i periodi 2ω, $2\omega'$ subiscono una sostituzione

$$\begin{pmatrix} \alpha\omega + \beta\omega', & \gamma\omega + \delta\omega' \\ \omega & \omega' \end{pmatrix}$$

[1]) Alla dimostrazione del teorema enunciato nella formola (15) non sono propriamente indispensabili le ricerche di questo e del seguente paragrafo, ma soltanto le considerazioni alla fine del § 212; lo studio generale del detto gruppo e del suo abbassamento nel caso particolare della moltiplicazione complessa fa però meglio intendere la ragione del risultato espresso nella (15).

a coefficienti interi e a determinante 1, e per ciò

$$y_{r,s} = \wp\left(\frac{2r\omega + 2s\omega'}{p}\right)$$

si cangia in

$$y_{r',s'} = \wp\left(\frac{2r(\alpha\omega + \beta\omega') + 2s(\gamma\omega + \delta\omega')}{p}\right),$$

cioè gli indici r', s' subiscono (mod p) la sostituzione

$$(18) \qquad \left\{\begin{array}{l} r' \equiv \alpha r + \gamma s \\ s' \equiv \beta r + \delta s \end{array}\right. \pmod p, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod p,$$

e dando nella (18) ad $\alpha, \beta, \gamma, \delta$ tutti i possibili valori (mod p), che soddisfano alla condizione

$$\alpha\delta - \beta\gamma \equiv 1 \pmod p,$$

col prescindere inoltre da un cangiamento simultaneo di segno in $\alpha, \beta, \gamma, \delta$, si avrà il gruppo Γ di monodromia, che consta evidentemente di $\frac{p(p^2-1)}{2}$ sostituzioni.

Per determinare il gruppo algebrico G, ci fondiamo sulla nota proprietà che G deve contenere il gruppo di monodromia come sottogruppo invariante. Ogni sostituzione di G deve dunque trasformare Γ in sè stesso, e quindi ogni sottogruppo ciclico d'ordine p in Γ in un altro tale sottogruppo.

Ma poichè la più alta potenza di p che divide l'ordine $p\,\frac{p^2-1}{2}$ di Γ è appunto p, tutti questi sottogruppi ciclici d'ordine p, per un corollario del teorema di Sylow, sono fra loro affini, cioè nascono tutti da uno di essi trasformando questo con una sostituzione di Γ. Se g è una sostituzione qualunque di G che trasformi uno dei detti sottogruppi H_1 in un altro H_2, combinando g con una conveniente γ di Γ, avremo una nuova sostituzione $g' = g\gamma$ di G (equivalente a g rispetto a Γ) che trasformerà H_1 in sè medesimo. Per sottogruppo ciclico H_1 d'ordine p prendiamo quello generato dalla seguente sostituzione U di Γ

$$U) \left\{\begin{array}{l} r' \equiv r + s \\ s' \equiv s, \end{array}\right.$$

e basterà limitarsi a cercare quelle sostituzioni di G che trasformano U in una sua potenza. Ora si osservi che la sostituzione U e le sue potenze sono *caratterizzate* da ciò che sono le uniche sostituzioni di Γ per le quali le singole radici

$$(19) \qquad y_{10},\ y_{20},\ \ldots,\ y_{p-1,0}$$

restano fisse [1]). Tutte le sostituzioni di Γ della forma

$$(20) \qquad \left\{\begin{array}{l} r' \equiv \alpha r + \gamma s \\ s' \equiv \qquad \delta s \end{array}\right., \quad \alpha\delta \equiv 1$$

permutano le radici (19) fra loro e per ciò trasformano U in una potenza di U. Se decomponiamo U nei suoi cicli, abbiamo i $\frac{p-1}{2}$ cicli

$$(y_{0,s},\ y_{s,s},\ y_{2s,s},\ \ldots,\ y_{(p-1)s,s}),\quad s = 1, 2, \ldots \frac{p-1}{2},$$

e con una conveniente sostituzione (20) di Γ portiamo le lettere di un ciclo in quelle di un altro ciclo arbitrario.

Ciò premesso, sia g' una sostituzione di G che trasformi U in una sua potenza e però le lettere di un ciclo in quelle di un altro ciclo. Combinando g' con una sostituzione (20) di Γ, potremo cangiare g' in una equivalente di G che trasformerà ancora U in una sua potenza, in guisa da cangiare per es. il primo ciclo

$$(y_{01}\, y_{11}\, y_{21} \ldots y_{p-1,1})$$

in una sua potenza. Di più, combinando la g con una conveniente potenza di U stessa, potremo sostituire una $\bar{g}$ equivalente che lasci fissa y_{01}. Ma allora, avendosi per le formole di moltiplicazione dell'argomento

$$(\alpha) \qquad y_{0s} = f(y_{01}),$$

[1]) Una sostituzione di Γ che lasci fissa y_{10} ha necessariamente la forma

$$\left\{\begin{array}{l} r' \equiv r + \gamma s \\ s' \equiv \quad s \end{array}\right.$$

e coincide per ciò con U^γ.

dove f è razionale in y_{01}, con coefficienti razionali in g_2, g_3, e qualunque sostituzione $\bar{g}$ del gruppo di Galois essendo permessa in una tale relazione razionale, segue che la nostra sostituzione $\bar{g}$ lascerà fissa ogni radice

$$y_{0s}, \quad \left(s = 1,\ 2,\ 3,\ \dots,\ \frac{p-1}{2}\right).$$

Supposto che la $\bar{g}$ trasformi U in U^{ν}, dovrà dunque trasformare ogni ciclo

$$(y_{0s}\, y_{ss}\, y_{2s,s},\ \dots,\ y_{(p-1)s,s})$$

nella sua potenza ν

$$(y_{0s}\, y_{\nu s,s}\, y_{2\nu s,s},\ \dots)$$

e per ciò in generale

$$y_{r,s} \text{ in } y_{\nu r,s} \text{ per } s \not\equiv 0.$$

Diciamo che ciò vale non solo per $s \not\equiv 0$, ma anche per $s \equiv 0$, che cioè $\bar{g}$ dovrà portare

$$y_{r0} \text{ in } y_{\nu r,0}.$$

Si consideri per ciò l'altra sostituzione V di Γ

$$r' \equiv r, \quad s' \equiv r + s,$$

che lascia fisse le radici

$$y_{01},\ y_{02},\ \dots,\ y_{0,\frac{p-1}{2}}$$

e contiene il ciclo

$$(y_{r0}\, y_{rr}\, y_{r,2r}\ \dots).$$

La $\bar{g}$ deve trasformare anche la V in una potenza di V, e per ciò tutte le lettere del ciclo scritto in quelle di un altro ciclo

$$(y_{r'0}\, y_{r'r'}\, y_{r'2r'}\ \dots),$$

e in questo precisamente la y_{r0} in $y_{r'0}$, giacchè la $\bar{g}$ deve permutare fra loro

$$y_{10}\, y_{20}\, y_{30}\ \dots\ y_{\frac{p-1}{2},0}.$$

D'altronde

$$y_{rr},\ y_{r,2r},\ y_{r,3r}\ \dots \quad \left(r = 1,\ 2,\ \dots\ \frac{p-1}{2}\right)$$

sono portate da $\bar{g}$ in

$$y_{\nu r,r},\ y_{\nu r,2r},\ y_{\nu r,3r}\ \dots,$$

dunque è $r' \equiv \nu r$. Concludiamo adunque:

La sostituzione cercata $\bar{g}$ di G ha l'espressione analitica

$$r' \equiv \nu r, \quad s' \equiv s \pmod p$$
$$(\nu = 1,\ 2,\ 3,\ \dots,\ p-1).$$

Combinando colle sostituzioni (18) del gruppo di monodromia Γ si deduce:

Le sostituzioni del gruppo algebrico G dell'equazione per la divisione dei periodi hanno tutte la forma lineare

$$\left.\begin{aligned} r' &\equiv a r + b s \\ s' &\equiv c r + d s \end{aligned}\right\} \pmod p \quad a d - b c \not\equiv 0. \tag{21}$$

Tutte le sostituzioni (21) formano un gruppo d'ordine

$$\frac{(p-1)^2\, p\,(p+1)}{2}$$

e dalla nostra dimostrazione risulta soltanto che il gruppo algebrico G è un suo sottogruppo (contenente Γ). Ciò basta al nostro scopo, ma con ulteriori ricerche si dimostrerebbe che G comprende *tutte* le sostituzioni (21) e che l'irrazionale numerico la cui aggiunta abbassa G a Γ è precisamente la radice p^{ma} dell'unità $e^{\frac{2\pi i}{p}}$.

§ 211. — Abbassamento del gruppo nel caso delle funzioni ellittiche a moltiplicazione complessa.

Supponiamo ora che la nostra funzione ellittica $\wp u$ sia una funzione $\wp$ a moltiplicazione complessa, appartenente ad una classe K primitiva di prima specie a determinante D. Il gruppo di Galois della sua equazione per la divisione dei periodi in p parti uguali (p primo) sarà certo un sottogruppo del gruppo generale G definito dalle formole (21) del paragrafo precedente

$$\text{(G)} \qquad \left\{\begin{array}{l} r' \equiv a r + b s \\ s' \equiv c r + d s \end{array}\right. \pmod{p}, \quad a d - b c \not\equiv 0\,;$$

ed anzi sappiamo già, dalle nostre ricerche al § 199, che G devesi in tal caso abbassare ad un suo sottogruppo risolubile per radicali. Ciò vogliamo constatare ora direttamente, per trovare la forma effettiva delle sostituzioni del gruppo di Galois. Ci limiteremo per altro al caso che importa soltanto al nostro scopo, al caso cioè in cui p non divida D e sia $-D$ residuo quadratico di p:

$$\left(\frac{-D}{p}\right) = +1.$$

Prenderemo allora la forma $(A,\ B,\ C)$ rappresentante della classe K, come al § 209, in guisa che siano $A,\ C$ divisibili per p e conseguentemente $2B$ non divisibile.

Consideriamo dapprima il campo naturale di razionalità, cioè quello dei soli numeri razionali, ampliato coll'aggiunta di $g_2,\ g_3$, e in esso determiniamo il gruppo di Galois (o un limite superiore del gruppo) per l'equazione (17) della divisione dei periodi. Per le formole di moltiplicazione complessa elementare si ha

$$\wp(\varepsilon u) = F(\wp u), \quad (\varepsilon = i\sqrt{D}),$$

dove la F è razionale in $\wp u$ e con coefficienti razionali, appartenendo $(A,\ B,\ C)$ alla prima specie. In particolare facendo nella precedente $u = \dfrac{2 r \omega + 2 s \omega'}{p}$, avremo

$$\text{(22)} \qquad \wp\left(\frac{2 r \varepsilon \omega + 2 s \varepsilon \omega'}{p}\right) = F\left(\wp\left(\frac{2 r \omega + 2 s \omega'}{p}\right)\right).$$

Ora avendosi (§§ 195, 196):

$$\text{(23)} \qquad \left\{\begin{array}{l} \varepsilon \omega \ = \ B\omega + A\omega' \\ \varepsilon \omega' = -C\omega - B\omega', \end{array}\right.$$

indi

$$\varepsilon\,\frac{2 r \omega + 2 s \omega'}{p} = 2\,\frac{r(B\omega + A\omega') - s(C\omega + B\omega')}{p},$$

ed essendo inoltre

$$A \equiv C \equiv 0 \pmod{p},$$

la (22) può scriversi, come relazione fra le radici dell'equazione per la divisione dei periodi:

$$(\alpha) \qquad y_{Br,\,-Bs} = F(y_{rs}),$$

formola che vale per un sistema qualunque di valori degli indici $r,\ s$.

Sia ora

$$\left.\begin{array}{l} r' \equiv a r + b s \\ s' \equiv c r + d s \end{array}\right. \pmod{p}, \quad a d - b c \not\equiv 0$$

una sostituzione qualunque del gruppo di Galois per la nostra equazione. Per le proprietà fondamentali del gruppo di Galois, la (α) resterà verificata eseguendo sugli indici delle due radici $y_{r,s},\ y_{Br,-Bs}$ la sostituzione $\begin{pmatrix} a, b \\ c, d \end{pmatrix}$; si avrà cioè

$$y_{B(ar-bs),\,B(cr-ds)} = F(y_{ar+bs,\,cr+ds}).$$

D'altronde, se cangiamo direttamente nella (α) r, s in $ar + bs$, $cr + ds$, otteniamo

$$y_{B(ar+bs),\,-B(cr+ds)} = F(y_{ar+bs,\,cr+ds});$$

dunque si ha, qualunque siano $r,\ s$:

$$y_{B(ar-bs),\,B(cr-ds)} = y_{B(ar+bs),\,-B(ar+ds)},$$

e poichè $B \not\equiv 0 \pmod{p}$ sarà quindi

$$a\,r - b\,s \equiv \pm (a\,r + b\,s)$$
$$c\,r - d\,s \equiv \mp (c\,r + d\,s).$$

Se valgono i segni superiori ne segue

$$b \equiv 0, \quad c \equiv 0 \pmod{p},$$

e quando valgano gli inferiori invece

$$a \equiv 0, \quad d \equiv 0.$$

Di qui deduciamo intanto: *Il gruppo di Galois (nel campo assoluto di razionalità, ampliato coll'aggiunta di g_2, g_3) per l'equazione per la divisione dei periodi in p parti eguali* [1]) *nella nostra funzione ellittica $\wp\, u$ contiene soltanto sostituzioni dell'una e dell'altra delle due forme*

α) $\qquad r' \equiv a\,r, \quad s' \equiv d\,s \pmod{p}$

β) $\qquad r' \equiv b\,s, \quad s' \equiv c\,r \pmod{p}.$

Queste sostituzioni α) β) formano un gruppo d'ordine $(p-1)^2$, nel quale è contenuto, come sottogruppo invariante d'indice 2, il gruppo di sostituzioni permutabili formato dalle α). Coll'aggiunta di una radice quadrata di un numero razionale, l'equazione diventa quindi Abeliana, conformemente ai risultati del § 199. Anzi, per quanto si è visto al citato paragrafo, è facilmente prevedibile che il detto radicale quadratico è precisamente $\sqrt{-D} = i\sqrt{D}$. Ciò constatiamo ora nel modo seguente. Per le formole di moltiplicazione complessa abbiamo (§ 196)

$$\wp\,((1+\varepsilon)\,u) = \Phi\,(\wp\,u),$$

dove la Φ è razionale in $\wp\,u$, con coefficienti razionali nel campo

$$(g_2,\ g_3,\ i\sqrt{D}).$$

[1]) Si ricordi che ciò vale nell'ipotesi che D non sia divisibile per p e si abbia

$$\left(\frac{-D}{p}\right) = +1.$$

Ponendo nuovamente

$$u = \frac{2\,r\,\omega + 2\,s\,\omega'}{p},$$

abbiamo

$$(22^*) \qquad \wp\left((1+\varepsilon)\,\frac{2\,r\,\omega + 2\,s\,\omega'}{p}\right) = \Phi\left(\wp\left(\frac{2\,r\,\omega + 2\,s\,\omega'}{p}\right)\right),$$

ed ora procedendo su questa come dianzi sulla (22) troveremo

$$y_{(1+B)\,r,\ (1-B)\,s} = \Phi\,(y_{r\,s}),$$

indi eseguendo la sostituzione $\begin{pmatrix} a\,r + b\,s, & c\,r + d\,s \\ r\ \ , & s \end{pmatrix}$ dell'attuale gruppo di Galois, avremo le congruenze

$$\begin{cases} \pm\,(1+B)\ \ (a\,r + b\,s) \equiv a\,(1+B)\,r + b\,(1-B)\,s \\ \pm\,(1-B)\ \ (c\,r + d\,s) \equiv c\,(1+B)\,r + d\,(1-B)\,s. \end{cases}$$

Queste sono bensì soddisfatte dalle sostituzioni della forma α), ma non da quelle della forma β), onde concludiamo:

Se si amplia il campo di razionalità precedente (g_2, g_3) coll'aggiunta di $i\sqrt{D}$, il gruppo di Galois per l'equazione della divisione dei periodi in p parti eguali $\left(\textit{nell'ipotesi}\ \left(\frac{-D}{p}\right) = +1\right)$ *consta di sostituzioni tutte della forma α)*

α) $\qquad r' \equiv a\,r, \quad s' \equiv d\,s \pmod{p}.$

§ 212. — Dimostrazione della formola fondamentale (15), § 209.

Dopo queste ricerche preparatorie siamo in grado di ritornare alle ricerche del § 209 sulla trasformazione degli invarianti di classi per completarle colla dimostrazione dei teoremi enunciati alla fine di questo paragrafo. Riprendiamo adunque la considerazione dell'invariante j_K della classe K e della corrispondente equazione modulare (11)

$$F_p\,(j',\ j_K) = 0,$$

colle $p+1$ radici

$$j'_\infty,\ j'_0,\ j'_1,\ j'_2,\ \ldots,\ j'_{p-1}.$$

Il suo gruppo di Galois nel campo assoluto di razionalità, ampliato coll'aggiunta di j_K è certamente contenuto nel gruppo

$$\nu' \equiv \frac{\alpha\nu+\beta}{\gamma\nu+\delta} \pmod p, \quad \alpha\delta-\beta\gamma \not\equiv 0.$$

Ma siccome questa equazione modulare non è altro che una risolvente di grado $p+1$ dell'equazione per la divisione dei periodi, il suo gruppo sarà subordinato a quello determinato al paragrafo precedente, quando si ponga

$$\nu \equiv \frac{r}{s} \pmod p$$

(Cfr. § 116), e però non potrà contenere che sostituzioni della forma derivata da α) o β), cioè

$$\alpha^*)\ \nu' \equiv \lambda\nu, \quad \beta^*)\ \nu' \equiv \frac{\lambda}{\nu};$$

e poichè queste sostituzioni lasciano ferme le radici j'_0, j'_∞, o le scambiano fra loro, si conclude nuovamente che le funzioni simmetriche elementari

$$j'_\infty + j'_0, \quad j'_\infty \cdot j'_0$$

sono esprimibili razionalmente per j_K con coefficienti razionali (§ 209). Ma ampliamo ora il campo coll'aggiunta di $i\sqrt{D}$; allora nel gruppo della equazione per la divisione dei periodi restano solo sostituzioni della forma α) e per ciò nel gruppo della equazione modulare solo le sostituzioni della forma α^*), le quali lasciano *singolarmente* invariate

$$j'_0 = j_{PK}, \quad j'_\infty = j'_{P^{-1}K}.$$

Ne segue, come era stato enunciato al § 209, che

$$j_{PK}, \quad j_{P^{-1}K}$$

si possono esprimere razionalmente per j_K, con coefficienti razionali in $i\sqrt{D}$.

Resta soltanto da provare che nella corrispondente formola (15):

$$j_{PK} = \varphi_P(j_K, \ i\sqrt{D})$$

la funzione razionale φ_P dipende solo dal numero p, o dalla classe P, e resta la stessa sostituendo a j_K una qualsiasi altra radice di

$$H_D(j) = 0.$$

La dimostrazione sarebbe immediata se avessimo stabilita la proprietà che effettivamente sussiste: *L'equazione $H_D(j) = 0$ per gli invarianti delle classi è irriducibile, anche se al campo assoluto di razionalità si aggiunge l'irrazionalità $i\sqrt{D}$*. Ma non volendo inoltrarci nelle considerazioni della teoria dei numeri algebrici che servono allo scopo [1]), ricorriamo nuovamente alla equazione per la divisione dei periodi

$$\psi_p(y) = 0$$

per separarne razionalmente (dopo aggiunta $i\sqrt{D}$) i fattori che contengono rispettivamente l'uno le radici

$$y_{10}, \ y_{20}, \ \ldots, \ y_{\frac{p-1}{2}, 0}$$

e l'altro le radici

$$y_{01}, \ y_{02}, \ \ldots, \ y_{0, \frac{p-1}{2}}.$$

Essendo sempre (A, B, C) la forma cui corrisponde la nostra $\wp u$ e scelta in guisa che

$$A \equiv C \equiv 0 \pmod p,$$

si esprimano colle formole di moltiplicazione complessa

$$\wp[(B+\varepsilon)u], \quad \wp[(B-\varepsilon)u]$$

razionalmente per $\wp u$, ciò che si otterrà colla formola

$$\wp[(B+\varepsilon)u] = \frac{U(\wp u, \ i\sqrt{D})}{V(\wp u, \ i\sqrt{D})}, \tag{24}$$

[1]) Cf. PICK, *Math. Annalen*, 26; WEBER, loc. cit.

essendo U, V polinomii razionali interi in $\wp u$ con coefficienti razionali in g_2, g_3, $i\sqrt{D}$, e deducendosi manifestamente la formola per $\wp((B-\varepsilon)u)$ col cangiare il segno di $i\sqrt{D}$ (Cfr. § 196):

$$\wp[(B-\varepsilon)u] = \frac{U(\wp u, -i\sqrt{D})}{V(\wp u, -i\sqrt{D})}. \tag{24*}$$

Si consideri ora l'equazione

$$V(\wp u, i\sqrt{D}) = V(y, i\sqrt{D}) = 0,$$

e si cerchi se e quali radici ha a comune con

$$\psi_p(y) = 0,$$

cioè si cerchino i valori

$$y_{r,s} = \wp\left(\frac{2r\omega + 2s\omega'}{p}\right)$$

che annullano $V(\wp u, i\sqrt{D})$. Per essi $\wp[(B+\varepsilon)u]$ deve diventare infinita senza che lo diventi $\wp u$, e viceversa ogni valore di u della forma $\frac{2r\omega+2s\omega'}{p}$, esclusa la combinazione $(r, s) \equiv (0, 0)$, tale che renda $\wp[(B+\varepsilon)u]$ infinita, è uno dei richiesti.

Per ciò è necessario e sufficiente che r, s siano tali da rendere

$$(B+\varepsilon)\frac{2r\omega+2s\omega'}{p}$$

eguale a un multiplo di periodi. Ora, per le formole (23), si può scrivere

$$(B+\varepsilon)\frac{2r\omega+2s\omega'}{p} = 2\frac{rB\omega+sB\omega'}{p} + $$
$$+ 2\frac{r(B\omega+A\omega')-s(C\omega+B\omega')}{p}$$

ossia, poichè $A \equiv C \equiv 0 \pmod{p}$, se trascuriamo multipli di periodi:

$$(B+\varepsilon)\frac{2r\omega+2s\omega'}{p} \equiv 4\frac{rB\omega}{p}.$$

Dunque è necessario e sufficiente che sia

$$r \equiv 0 \pmod{p};$$

cioè: *Il massimo comun divisore di* $V(y, i\sqrt{D})$, $\psi_p(y)$ è

$$\chi(y) = (y - y_{01})(y - y_{02}) \ldots (y - y_{0,\frac{p-1}{2}}).$$

Questo polinomio $\chi(y)$ si calcolerà quindi razionalmente, e i suoi coefficienti conterranno razionalmente g_2, g_3, $i\sqrt{D}$; di più, a causa della natura delle formole di moltiplicazione complessa, *l'espressione così trovata per* $\chi(y)$ *varrà indistintamente per tutte le* $\wp u$ *a moltiplicazione complessa*, corrispondenti a forme primitive di prima specie a determinante D.

Se, invece di considerare il polinomio $V(y, i\sqrt{D})$, avessimo considerato l'altro

$$V(y, -i\sqrt{D}),$$

manifestamente pel suo massimo comun divisore $\chi_1(y)$ con $\psi_p(y)$ avremmo trovato

$$\chi_1(y) = (y - y_{10})(y - y_{20}) \ldots (y - y_{\frac{p-1}{2},0}).$$

Per venire infine alla nostra ricerca, si consideri che j'_0 è funzione simmetrica di

$$y_{01}, y_{02} \ldots y_{0,\frac{p-1}{2}}$$

(vedi formole (III), pag. 204) e però esprimibile razionalmente per g_2, g_3, $i\sqrt{D}$, con coefficienti razionali. Ma poichè l'invariante assoluto dipende solo dal rapporto dei periodi, mentre g_2, g_3 si cangiano a volontà in $\lambda^4 g_2$, $\lambda^6 g_3$, con osservazioni perfettamente analoghe a quelle del § 168 per le equazioni generali modulari, ne concludiamo che si avrà

$$j'_0 = j_{PK} = \varphi_p(j_K, i\sqrt{D})$$

e la funzione φ, indicata al § 209, formola (15), con φ_p dipenderà appunto unicamente, come ivi era stato asserito, dalla classe P, non da K. Vediamo ora di più che l'altra radice j'_∞ si ottiene semplicemente cangiando in φ_p il segno di $i\sqrt{D}$, cioè si hanno le formole

$$\text{(A)} \qquad \begin{cases} j_{PK} = \varphi_P(j_K, \quad i\sqrt{D}) \\ j_{P^{-1}K} = \varphi_P(j_K, -i\sqrt{D}). \end{cases}$$

§ 213. — Gruppo di Galois per l'equazione $H_D(j) = 0$ e sua risolubilità per radicali.

Applicando le formole ora trovate e il teorema del § 208, secondo il quale qualunque forma (o classe) può comporsi con successive forme

$$P = (p, b, c), \; P' = (p', b', c'), \; P'' = (p'', b'', c'') \; ....$$

i cui primi coefficienti siano numeri primi, siamo ora in grado di estendere le formole (A) a qualunque classe e pervenire così al risultato finale, dimostrando la risolubilità per radicali della equazione per gli invarianti delle classi

$$H_D(j) = 0.$$

Cominciamo dallo scrivere le due formole (A)

$$\text{(B)} \qquad \begin{cases} j_{PK} = \varphi_P(j_K, i\sqrt{D}) \\ j_{P'K} = \varphi_{P'}(j_K, i\sqrt{D}) \end{cases}$$

e mutando, come è lecito, nella prima j_K in $j_{P'K}$ avremo

$$j_{PP'K} = \varphi_P(j_{P'K}, i\sqrt{D}) = \varphi_P(\varphi_{P'}(j_K, i\sqrt{D}), i\sqrt{D}),$$

che scriveremo

$$j_{PP'K} = \varphi_{PP'}(j_K, i\sqrt{D}),$$

ove la funzione razionale $\varphi_{PP'}$ resterà la medesima cangiando comunque la classe K. Se si cangia invece, nella seconda delle (B), K in PK si trova

$$j_{PP'K} = \varphi_{P'}(\varphi_P(j_K, i\sqrt{D}), i\sqrt{D}) = \varphi_{P'P}(j_K, i\sqrt{D}),$$

onde si vede che

$$\varphi_{PP'}(j_K, i\sqrt{D}) = \varphi_{P'P}(j_K, i\sqrt{D})$$

e la funzione $\varphi_{PP'}$ dipende in sostanza unicamente dalla classe composta PP'. Similmente si stabilirebbe la formola

$$j_{PP'P''K} = \varphi_{PP'P''}(j_K, i\sqrt{D}),$$

e così via per un numero qualunque di classi P componenti. Se ne conclude quindi il teorema:

Essendo K, K' due classi qualunque fra

$$K_1, \; K_2, \; ..., \; K_h,$$

si ha la formola

$$\text{(C)} \qquad j_{K'K} = \varphi_{K'}(j_K, i\sqrt{D}),$$

la funzione razionale $\varphi_{K'}$ dipendendo unicamente dalla seconda classe K', non dalla prima K.

Cangiando in $\varphi_{K'}$ il segno del radicale $i\sqrt{D}$ si passa alla classe opposta K'^{-1}; si ha cioè

$$\text{(C*)} \qquad j_{K'^{-1}K} = \varphi_{K'}(j_K, -i\sqrt{D}).$$

Ed ora possiamo determinare, nel campo di razionalità dei numeri razionali ampliato coll'aggiunta di $i\sqrt{D}$, la natura del gruppo di Galois per l'equazione degli invarianti delle classi

$$H_D(j) = 0,$$

le cui radici sono

$$j_{K_1}, j_{K_2} \; .... \; j_{K_h}.$$

Supponiamo infatti che, essendo $K_1 = 1$ la classe principale, una sostituzione S del gruppo di Galois porti j_{K_1} in j_{K_r}. Essendo K_s una qualunque delle classi, si ha per la (C)

$$j_{K_s K_r} = \varphi_{K_s}(j_{K_r}, i\sqrt{D}),$$

ed anche

$$j_{K_s} = \varphi_{K_s}(j_1, i\sqrt{D}).$$

In quest'ultima relazione eseguiamo, come è lecito, la sostituzione S del gruppo di Galois la quale porta per ipotesi j_1 in j_{K_r} e ne risulterà che S porterà j_{K_s} in

$$\varphi_{K_s}(j_{K_r}, i\sqrt{D}) = j_{K_s K_r}.$$

Dunque la S produce sulle radici

$$j_{K_1}, j_{K_2}, \ldots, j_{K_h}$$

la permutazione

$$j_{K_1 K_r}, j_{K_2 K_r}, \ldots, j_{K_h K_r},$$

cioè cangia i loro indici secondo la sostituzione K_r del gruppo di composizione delle classi (§ 207). Se ne conclude:

Nel campo dei numeri razionali, ampliato coll'aggiunta di $\sqrt{D}$, il gruppo G di Galois per l'equazione

$$H_D(j) = 0$$

degli invarianti delle classi è contenuto nel gruppo di composizione delle forme.

In ogni caso G è un gruppo Abeliano e per ciò si ha il teorema finale d'Abel a cui miravano le nostre ricerche:

L'equazione $H_D(j) = 0$ è risolubile per radicali.

L'incertezza lasciata dalle nostre ricerche se il gruppo di Galois di $H_D(j) = 0$ coincida col gruppo di composizione, o ne sia soltanto un sottogruppo, si toglierebbe colla dimostrazione già sopra accennata della *irriducibilità* dell'equazione; e poichè il gruppo di composizione sulle forme è semplicemente transitivo, si avrebbe il risultato definitivo: *Il gruppo di Galois per $H_D(j) = 0$, nel campo di razionalità $(1, i\sqrt{D})$, coincide (è oleodricamente isomorfo) col gruppo di composizione delle classi.*

In fine possiamo determinare il gruppo di Galois di $H_D(j) = 0$ nel campo assoluto di razionalità, prima cioè dell'aggiunta di $i\sqrt{D}$. I teoremi generali ci assicurano che questo nuovo gruppo Γ, se è effettivamente più ampio, conterrà G come sottogruppo invariante d'indice 2, abbassandosi Γ a G per l'aggiunta della radice quadrata $\sqrt{-D}$. Ora associamo alle sostituzioni del gruppo di composizione G quella sostituzione S che consiste nel cangiare

ogni forma nella propria opposta (inversa); la S non appartiene a G (salvo quando, essendo ancipiti tutte le classi, S è l'identità) ed è permutabile, come subito si vede con G. Per ciò

$$\Gamma = [G, SG]$$

è un gruppo d'ordine $2h$, che contiene G come sottogruppo invariante.

Ora dimostriamo facilmente che: *Il gruppo dell'equazione $H_D(j) = 0$, nel campo assoluto di razionalità, coincide col gruppo Γ così ampliato dal gruppo di composizione (ovvero ne è un sottogruppo).*

Consideriamo infatti una funzione razionale *a coefficienti razionali*

$$F(j_{K_1}, j_{K_2}, \ldots, j_{K_h})$$

delle radici di $H_D(j) = 0$, che rimanga invariata per tutte *e sole* le sostituzioni di Γ e dimostriamo che il suo valore è quello di un numero razionale, dopo di che sarà appunto provato il teorema. Certamente se aggiungiamo $i\sqrt{D}$, la F è razionalmente nota, perchè le sostituzioni di G la lasciano invariata; dunque si ha

$$F(j_{K_1}, j_{K_2}, \ldots, j_{K_h}) = a + ib\sqrt{D},$$

con a, b numeri razionali. Ma di più la F rimane invariata numericamente cangiando ogni classe nella propria opposta, cioè ogni radice j_K nella *coniugata* $j_{K^{-1}}$, e per ciò il suo valore è reale, onde $b = 0$, ciò che prova l'asserzione.

§ 214. — Decomposizione di $H_D(j)$ in fattori corrispondenti ai generi delle forme secondo Kronecker.

L'equazione $H_D(j) = 0$ è irriducibile, come già si è detto, non solo nel campo assoluto di razionalità, ma anche dopo l'aggiunta di $i\sqrt{D}$. Però Kronecker, nelle sue celebri comunicazioni all'Accademia di Berlino sulla teoria della moltiplicazione complessa, ha trovato che appena si aggiungono convenienti radici quadrate reali (di fattori del determinante D) il polinomio $H_D(j)$ diventa riducibile e si spezza nel prodotto di tanti fattori, di egual grado, quanti sono i *generi* delle forme quadratiche, secondo la definizione di Gauss [1]), le radici di ciascun fattore appartenendo appunto alle classi di un medesimo genere.

Di questi bei risultati, dovuti a Kronecker, vogliamo qui soltanto stabilire quella parte che discende senz'altro dalla natura del gruppo Γ della nostra equazione. Per ciò stabiliamo in primo luogo la ripartizione delle h classi in generi, sotto la forma più breve che ci consentono le nozioni acquistate sul gruppo di composizione.

Se si considerano tutte le seconde potenze delle h classi

$$K_1^2,\ K_2^2,\ K_3^2,\ \ldots,\ K_h^2,$$

e si indicano con

$$k_1,\ k_2,\ k_3,\ \ldots,\ k_s$$

le classi distinte così risultanti, è manifesto che queste classi, ottenute per duplicazione, formano per sè un gruppo, cioè un sottogruppo H del gruppo G di composizione. Quindi segue che il numero s è un divisore di h; e ripartendo le sostituzioni (o classi) del gruppo totale G rispetto a quelle del sottogruppo H, otterremo il quadro:

$$(\mathrm{D})\qquad \left\{\begin{array}{l} k_1 \quad k_2 \quad k_3\ ,\ \ldots,\ k_s \\ k_1k'_2,\ k_2k'_2,\ k_3k'_2,\ \ldots,\ k_sk'_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ k_1k'_q,\ k_2k'_q,\ k_3k'_q,\ \ldots,\ k_sk'_q, \end{array}\right.$$

dove con

$$1,\ k'_2,\ k'_3,\ \ldots,\ k'_q$$

abbiamo indicato le classi moltiplicatrici, il cui numero q è l'*indice* di H in G.

Le classi contenute nel quadro (D) in una medesima orizzontale costituiscono un *genere* secondo Gauss, in particolare quelle della prima orizzontale il così detto *genere principale*; il numero q

[1]) *Disquisitiones*, art. 229-233; DIRICHLET-DEDEKIND, *Zahlentheorie*, Supplemento IV.

non è altro che il numero dei generi distinti. Facilmente dimostriamo che q è una potenza esatta del 2 e precisamente si ha il teorema:

Il numero q dei generi eguaglia il numero 2^n delle classi ancipiti (§ 207).

Se riprendiamo infatti la rappresentazione di ogni classe per mezzo di una base

$$K_1,\ K_2,\ \ldots,\ K_r$$

ricordata alla fine del citato § 207, quando sia

$$K = K_1^{\alpha_1} K_2^{\alpha_2} \ldots K_r^{\alpha_r},$$

vediamo che K apparterrà al genere principale (si otterrà per duplicazione) allora soltanto quando gli esponenti α siano tutti pari, o tali possano ridursi sostituendo a ciascuno di essi un esponente congruo rispetto al corrispondente modulo β. Ora ciò può sempre ottenersi per quegli esponenti α il cui corrispondente modulo (periodo) β è impari, mentre quando β è pari avremo solo $\frac{\beta}{2}$ valori possibili (pari) per α ed incongrui (mod β).

Dunque indicando, come al § 207, con n il numero delle β pari, si ha

$$s = \frac{\beta_1 \beta_2 \ldots \beta_r}{2^n},$$

e quindi

$$q = \frac{h}{s} = 2^n, \text{ c. d. d.}$$

Se si compongono fra loro due classi qualunque prese l'una nella orizzontale m^{ma}, l'altra nella m'^{ma}, il numero d'ordine della orizzontale cui appartiene la classe composta dipenderà unicamente da m, m'. In altre parole il gruppo di composizione sulle classi è imprimitivo e i singoli generi formano altrettanti sistemi d'imprimitività. Il gruppo di sostituzioni indotto da G sui generi, che diciamo il gruppo di composizione sui generi, è un gruppo Abeliano d'ordine 2^n semplicemente transitivo, e le sue sostituzioni

$$H_1,\ H_2,\ \ldots,\ H_{2^n}$$

sono tutte a periodo 2 (salvo naturalmente l' identità), perchè due classi del medesimo genere si compongono in una classe del genere principale.

Invece due generi diversi non possono comporsi nel genere principale, onde segue che due classi opposte (componendosi nella principale) appartengono necessariamente allo stesso genere. Se consideriamo dunque il gruppo Γ ampliato da G associandovi la sostituzione che cangia ogni classe nella sua opposta, non solo rispetto a G, ma ben anche rispetto a Γ, i 2^n generi costituiranno sistemi d' imprimitività. Ora Γ è il gruppo di $H_D(j) = 0$ nel campo assoluto di razionalità o almeno (stando soltanto a quello che abbiamo propriamente dimostrato) certamente lo contiene. Se ordiniamo le radici di $H_D(j) = 0$ nel quadro corrispondente al quadro (D)

$$(\mathrm{D}^*) \qquad \left\{\begin{array}{cccc} j_{k_1} & j_{k_2} & \dots & j_{k_s} \\ j_{k_1 k'_2} & j_{k_2 k'_2} & \dots & j_{k_s k'_2} \\ \cdot & \cdot & \cdot & \cdot \\ j_{k_1 k'_q} & j_{k_2 k'_q} & \dots & j_{k_s k'_q} \end{array}\right.$$

e prendiamo una funzione razionale simmetrica delle radici di una orizzontale, con coefficienti razionali reali, per es.

$$x = j_{k_1}^m + j_{k_2}^m + \dots + j_{k_s}^m \quad (m \text{ intero}), \tag{25}$$

questa, per le sostituzioni di Γ, assumerà solo $q = 2^n$ valori

$$x_1, \ x_2, \ \dots, \ x_{2^n}, \tag{26}$$

corrispondenti alle orizzontali del quadro (D*) e questi 2^n valori saranno numericamente distinti, ove si scelga opportunamente la detta funzione simmetrica. Inoltre essi saranno tutti reali, comparendo in essa funzione simmetrica insieme ad un invariante j_K il coniugato $j_{K^{-1}}$. Pei teoremi generali questi 2^n valori (26) saranno radici di una risolvente di grado 2^n, che indicheremo con

$$\psi_{2^n}(x) = 0; \tag{27}$$

la quale avrà coefficienti reali interi e radici pure reali. Inoltre si potrà supporre che il primo coefficiente sia eguale all'unità, sce-

gliendo la funzione risolvente intera e a coefficienti interi. La risoluzione di questa ausiliaria produce (in ordine ai detti teoremi) nel polinomio $H_D(j)$ appunto lo spezzamento in 2^n fattori, contenenti ciascuno le radici j_K che appartengono a classi del medesimo genere. Il gruppo della risolvente (27) è isomorfo col gruppo di composizione sui generi (o vi è contenuto come sottogruppo). Ma questo gruppo Σ è Abeliano di grado 2^n e non ha che sostituzioni a periodo 2, onde facilmente vediamo che l'equazione si risolve estraendo n radici quadrate separate

$$\sqrt{a_1}, \ \sqrt{a_2}, \ \dots, \ \sqrt{a_n},$$

che portano sopra numeri interi e positivi. E infatti, se rappresentiamo le sostituzioni σ di Σ mediante una base, questa, avendo ogni sostituzione generatrice a periodo 2, consterà di n termini

$$\sigma_1, \ \sigma_2, \ \dots, \ \sigma_n$$

e si avrà

$$\sigma = \sigma_1^{\alpha_1} \ \sigma_2^{\alpha_2} \dots \sigma_n^{\alpha_n}, \tag{28}$$

ciascun esponente α avendo il valore 0 o 1. Ora consideriamo gli n sottogruppi di Σ d'ordine 2^{n-1}

$$\begin{aligned} \Sigma_1 &= [\sigma_2, \ \sigma_3, \ \dots, \ \sigma_n] \\ \Sigma_2 &= [\sigma_1, \ \sigma_3, \ \dots, \ \sigma_n] \\ \Sigma_n &= [\sigma_1, \ \sigma_2, \ \dots, \ \sigma_{n-1}], \end{aligned}$$

che hanno la sola sostituzione identica a comune. Se costruiamo una funzione razionale intera a coefficienti interi delle radici della (27) che rimanga invariata per tutte e sole le sostituzioni Σ_1, essa darà luogo ad una risolvente di secondo grado a radici reali della (27) e l'aggiunta di un radicale quadrato $\sqrt{a_1}$, che porta sopra un numero razionale intero e positivo a_1, abbasserà il gruppo Σ a Σ_1. Procedendo medesimamente per gli altri sottogruppi $\Sigma_2, \Sigma_3, \dots, \Sigma_n$, l'aggiunta simultanea degli indicati radicali

$$\sqrt{a_1}, \ \sqrt{a_2}, \ \dots, \ \sqrt{a_n}$$

abbasserà Σ al sottogruppo comune di

$$\Sigma_1, \ \Sigma_2, \ \ldots, \ \Sigma_n,$$

cioè all'identità, ciò che dimostra quanto sopra è asserito. Concludiamo adunque:

Per spezzare il polinomio $H_D(j)$ in 2^n fattori corrispondenti ai generi delle forme quadratiche, basta l'aggiunta al campo assoluto di razionalità di n radici quadrate

$$\sqrt{a_1}, \quad \sqrt{a_2}, \ \ldots, \ \sqrt{a_n}$$

estratte sopra n numeri $a_1, a_2, \ldots, a_n$ razionali, interi e positivi.

Un più profondo esame dimostrerebbe che questi numeri $a_1, a_2, \ldots, a_n$ non sono altro che fattori primi del determinante D, o loro prodotti [1]). Ma le ulteriori ricerche necessarie alla dimostrazione precisa dei teoremi di Kronecker, come quelle che riguardano la più volte mentovata irriducibilità dell'equazione $H_D(j) = 0$ per gli invarianti delle classi, eccederebbero i limiti imposti alle presenti lezioni.

[1]) Cf. WEBER, loc. cit., §§ 103-106.

INDICE.

CAPITOLO IX.

Le funzioni fondamentali σu, $\wp u$ di Weierstrass. — Le funzioni generali ellittiche espresse per la σu. — Equazione differenziale per la $\wp u$: $\wp'^2 u = 4\ \wp^3 u - g_2\ \wp u - g_3$.

CAPITOLO X.

Decomposizione di una funzione ellittica in elementi semplici. — Teorema d'addizione per la ζu e la $\wp u$. Le funzioni ellittiche espresse razionalmente per $\wp u$, $\wp' u$. — Moltiplicazione e divisione dell'argomento nella $\wp u$.

CAPITOLO XI.

Proprietà fondamentali della prima funzione modulare $J(\tau)$ (invariante assoluto). — La funzione $\wp(u\,;\,g_2\,,\,g_3)$, con assegnati invarianti. — Integrali ellittici di prima specie e loro inversione. — Integrali ellittici generali.

CAPITOLO XII.

Le tre funzioni σ pari di Weierstrass e le funzioni ellittiche di Jacobi $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$. **— Il quadrato k^2 del modulo come funzione modulare. — Formole d'addizione per** $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$.

CAPITOLO XIII.

Le funzioni $\wp u$, σu e $\sigma_r u$ per valori reali degli invarianti e le funzioni di Jacobi $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$, **per valori reali del modulo k fra 0 e 1. — Integrali ellittici di Legendre e Jacobi.**

CAPITOLO XIV.

Sviluppi in prodotti infiniti ed in serie trigonometriche delle funzioni σ. — Le serie θ di Jacobi e le loro proprietà.

CAPITOLO XV.

Teoria della trasformazione delle funzioni ellittiche. — Trasformazioni di grado primo della $\wp u$ e della σu. — Trasformazione di Landen.

CAPITOLO XVI.

Funzioni modulari ellittiche.

CAPITOLO XVII.

Equazioni modulari per l'invariante assoluto e per la funzione modulare $\sqrt[4]{k}$. — Metodo di Hermite per la risoluzione dell'equazione generale di quinto grado.

CAPITOLO XVIII.

Principî della teoria delle funzioni ellittiche a moltiplicazione complessa.

CAPITOLO XIX.

Composizione delle forme quadratiche e gruppo di Galois per l'equazione degli invarianti delle classi.

FINITO DI STAMPARE A FIRENZE

NELLA TIPOGRAFIA « ENRICO ARIANI »

IL XX GIUGNO MCMXXX