Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di laurea in Matematica

Periodi di curve ellittiche e funzioni ipergeometriche

Calcolo dei periodi del toro associato ad una curva ellittica con il metodo delle funzioni ipergeometriche

Relatore:
Prof. Matteo Longo

Candidato:
Luca Alvise Vianello
Matricola 2033949

Anno accademico 2024/2025 - 19.09.2025

Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di laurea in Matematica

Periodi di curve ellittiche e funzioni ipergeometriche

Calcolo dei periodi del toro associato ad una curva ellittica con il metodo delle funzioni ipergeometriche

Relatore:
Prof. Matteo Longo

Candidato:
Luca Alvise Vianello
Matricola 2033949

Anno accademico 2024/2025 - 19.09.2025

Luca Alvise Vianello

Ai miei genitori e ai miei nonni per avermi supportato,
A Bea e ai miei amici per avermi sopportato.

Indice

Indice **v**

Introduzione **1**

1 Curve e tori **5**
1.1 *Curve proiettive e affini* 5
1.2 *Curve ellittiche complesse* 6
1.3 *Operazione di gruppo* 10
1.4 *Curve ellittiche in forma di Legendre* 12
1.5 *Tori complessi* 14

2 Isomorfismo da toro a curva **17**
2.1 *Funzioni ellittiche* 17
2.2 *$\wp$-function di Weiestrass* 20
2.3 *Divisori e teorema di Abel-Jacobi* 22
2.4 *Equazione differenziale per la p-function di Weiestrass* 24
2.5 *Isomorfismo analitico fra tori complessi e curve ellittiche* 26

3 Funzioni ipergeometriche e calcolo dei periodi **29**
3.1 *Generalità sulla funzione Γ di Eulero* 29
3.2 *Funzioni ipergeometriche* 32
3.3 *Uniformizzazione* 33
3.4 *Calcolo dei periodi* 34

Bibliografia **39**

Introduzione

Le curve ellittiche sono un importante oggetto di studio della Teoria dei Numeri. Storicamente nascono da un problema analitico: il calcolo della lunghezza degli archi di un'ellisse. Tale calcolo avviene tramite una classe di integrali (detti *integrali ellittici del primo tipo*) che si rivelò sin da subito insidiosa poiché non risolvibile in termini di funzioni elementari. Nella forma originale di Jacobi questi erano integrali del tipo

$$F(y) = \int_0^y \frac{ds}{\sqrt{(1-s^2)(1-k^2s^2)}}$$

dove k è un parametro che indica l'eccentricità dell'ellisse. Più precisamente, tratteremo una classe analoga di integrali definita come:

$$F(x) = \int_{-\infty}^x \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}$$

Nel Teorema **3.12** (risultato finale di questo lavoro) vedremo come questi due integrali sono legati da cambi di coordinate e li risolveremo proponendo la soluzione tramite le funzioni ipergeometriche. Valutando questi integrali in $\mathbb{C}$, il problema principale dello studio degli integrali ellittici è rappresentato dal fatto che questi non sono indipendenti dalla scelta del cammino, ciò è dovuto all'indeterminazione della radice quadrata nel campo complesso. Ad ogni radice quadrata corrispondo infatti due possibili valori, questo è problematico quando si considerano i cammini chiusi attorno alle singolarità; fuori da questi punti la radice è analitica. Per ovviare a questo problema di indeterminazione è necessario costruire uno spazio in cui la radice possa essere valutata oppportunamente. Iniziamo col fare dei tagli nei segmenti $[0, \infty)$ e $[1, \lambda]$; questi tagli, detti *branch cuts*, impediscono di avere circui attorno alle singolarità. Per costruire questo spazio è poi necessario prendere due copie di $\mathbb{P}^1(\mathbb{C})$ ovvero $\mathbb{C} \cup \{\infty\}$ (topologicamente, due sfere) con tagli come quelli fatti in precedenza; incollando queste due superfici in corrispondenza dei tagli fatti si ottiene una superficie di Riemann, ovvero un toro. Questa varietà è dunque lo spazio naturale in cui studiare questi integrali.

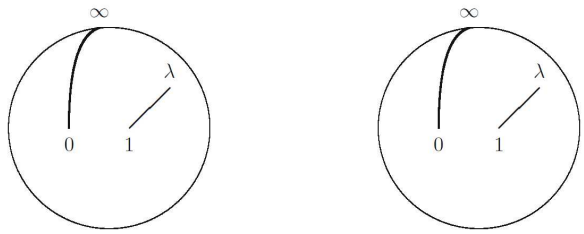

Figura 1: Tagli su due copie di $\mathbb{P}^1(\mathbb{C})$. Sulle sfere prese singolarmente la radice è ben definta.

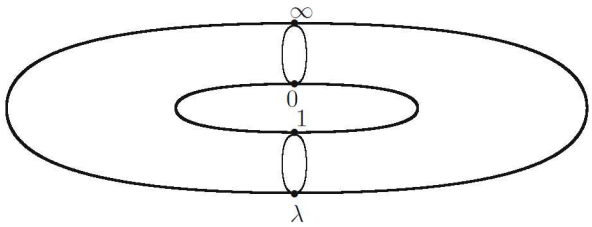

Figura 2: Incollamento lungo i tagli. La radice è ben definita e può prendere entrambi i valori possibili.

Questa procedura viene spiegata in modo molto approfondito in [**3**]. Il toro complesso è una superficie di Riemann (una varietà differenziale complessa di dimensione uno) che si può definire in come $\mathbb{C}/\Lambda$ dove $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ è un reticolo complesso; doteremo il toro della struttura algebrica di gruppo additivo e della topologia indotte da $\mathbb{C}$. Possiamo allora definre le funzioni ellittiche (associate ad un toro) come tutte e sole le funzioni $f : \mathbb{C} \to \mathbb{C}$ meromorfe che rispettano la struttura di Λ, ovvero le funzioni definite sul toro. Rispettare la struttura di reticolo significa che per ogni $z \in \mathbb{C}$

$$f(z) = f(z + w_1) = f(z + w_2)$$

Queste funzioni sono duque biperiodiche; lo studio di queste mappe ci porterà a capire come sono nate le curve ellittiche e che relazione hanno gli integrali ellittici con tori e periodi.
Nel primo capitolo introdurremo separatamente i concetti di curva ellittica e di toro complesso, definendo per entrambi delle quantità chiamate *periodi* apparentemente diverse fra di loro. In una curva ellittica E, i periodi sono integrali di forme differenziali olomorfe sui generatori del primo gruppo di omologia della curva simili a quelli descritti sopra; nei tori i periodi sono numeri complessi w_1 e w_2 $\mathbb{R}$-linearmente indipendenti che generano il reticolo con cui sono costruiti i tori stessi. Una volta definiti questi oggetti, nel secondo capitolo inizieremo a studiare il campo delle funzioni ellittiche associate ad un reticolo. Tramite le $\wp$-function di Weierstrass, che

sono l'esempio più esplicito di funzioni biperiodiche associate ad un toro, riusciremo a parametrizzare le curve ellittiche, ovvero fornire un'espressione analitica per le coordinate locali di E. Nel terzo capitolo, col Teorema **3.10** dimostreremo un risultato classico: ogni curva ellittica è analiticamente isomorfa ad uno ed un solo toro complesso, a meno di equivalenze. Nasce naturale a questo punto porsi il problema inverso: individuare il toro isomorfo ad una curva ellittica. Ciò che permette di passare dalla curva ellittica al toro associato sono proprio i periodi: calcolare i periodi della curva, ovvero risolvere un integrale ellittico, significa, in ultima analisi, ricavare i valori complessi $\mathbb{R}$-linearmente indipendenti che generano un reticolo. Tali valori sono i periodi di un toro.
Nell'ultima parte del lavoro, forti dei risultati precedentemente dimostrati, ci occuperemo di calcolare in modo esplicito gli integrali ellittici che a questo punto chiameremo semplicemente periodi. Questo sarà posssibile grazie alle considerazioni fatte nel secondo capitolo e all'uso delle funzioni ipergeometriche per la risoluzione degli integrali ellittici. Il Teorema **3.12** sarà la sintesi di tutti i concetti trattati nella tesi. Mostreremo quindi come lo studio dei tori associati agli integrali ellittici portò a definre le curve ellittiche e di come questi tre oggetti siano legati dal concetto di periodo.
Come si può intuire, i periodi delle curve ellittiche non sono semplici numeri: essi incarnano una profonda interazione tra geometria algebrica e analisi complessa. In un contesto più ampio, possiamo definire i periodi come valutazioni di forme differenziali su cicli topologici in varietà algebriche

$$p = \int_\gamma \omega$$

I periodi sono oggetto di studio in una delle congetture più profonde della matematica moderna: la congettura di Grothendieck sui periodi. Secondo questa congettura, ogni relazione algebrica tra periodi, ovvero fra integrali con valore simile, non è una semplice coincidenza analitica bensì dovrebbe avere una spiegazione geometrica, ossia derivare da corrispondenze tra le varietà sottostanti (o, in termini tecnici, tra i loro motivi). Così, anche il semplice calcolo dei periodi associati a una curva ellittica può essere visto come un esempio specifico in un quadro teorico più ampio, che cerca di comprendere la natura aritmetica e geometrica dei numeri complessi (soprattutto trascendenti) che emergono dall'integrazione su varietà algebriche.

Capitolo 1

Curve e tori

In questo capitolo daremo un'introduzione generale ai concetti di toro complesso e di curva ellittica definendoli e mostrando le proprietà che ci seriviranno nelle successive costruzioni.

1.1 *Curve proiettive e affini*

Iniziamo col definire gli ambienti in cui lavoreremo con le curve ellittiche.

Definizione 1.1. Sia k un campo; il piano proiettivo $\mathbb{P}^2(k)$ consiste nelle classi di equivalenza delle $(2+1)$-tuple $(w : x : y)$ con le entrate non tutte nulle. Due tuple $(w : x : y)$ e $(w' : x' : y')$ sono equivalenti se e solo se esite $a \in k \setminus \{0\}$ tale che $(w : x : y) = (aw' : ax' : ay')$

Definizione 1.2. Un iperpiano proiettivo (in dimensione 2 diremo *retta* proiettiva) è l'insieme dei punti $(w : x : y)$ tali che:

$$a_1x_0 + a_2x_1 + a_3x_2 = 0$$

Gli a_i sono in k e non sono tutti nulli. Di particolare importanza sarà la retta $r_\infty : x_0 = 0$.

Chiamiamo r_∞ la *retta all'infinito* e definiamo il sottoinsieme di $\mathbb{P}^2(k)$ dato da

$$\mathbb{A}(k) = \mathbb{P}^2(k) \setminus r_\infty$$

Quando parleremo di *disomogeneizzazione* di $\mathbb{P}^2(k)$, intendiamo l'insieme dei punti $(1 : x/w : y/w)$, ovvero i punti con prima coordinata proiettiva non nulla. Questo spazio è ciò chiameremo *spazio affine bidimensionale*, ovvero il piano cartesiano. Possiamo ora dare una definizione algebrica di curva proiettiva.

Definizione 1.3. Sia $F(w : x : y)$ un polinomio omogeneo di grado d. Una curva algebrica proiettiva è definita dal luogo degli zeri di F, ovvero:

$$C_F = \{(w : x : y) \in \mathbb{P}^2(k) \mid F(w : x : y) = 0\}$$

La condizione di omogeneità del polinomio implica che per ogni punto di $\mathbb{P}^2(k)$ valga $F(qw : qx : qy) = 0$ se e solo se $q^d F(w : x : y) = 0$ per ogni $q \in k$. L'omogeneità di F è, dunque, essenziale affinchè la definizione si ben posta per le classi di quivalenza di $\mathbb{P}^2(k)$.

Definizione 1.4. Un punto di C_F è singolare se e solo se:

$$\frac{\partial F}{\partial x_0}(P) = \frac{\partial F}{\partial x_1}(P) = \frac{\partial F}{\partial x_2}(P) = 0$$

Una curva è detta *non-singolare* se e solo se ogni suo punto è non-singolare.

Parleremo di *disomogeneizzazione* di C_F per indicare l'insieme

$$C_F \cap (\mathbb{P}^2(k) - r_\infty)$$

In questi casi lavoreremo con la corrispondente curva affine. Il poliniomo F affinizzato (ovvero ponendo w costantemente uguale ad 1) non è necessariamente omogeneo. In questo procedimento si possono perdere dei punti, ovvero quelli con coordinata w nulla. Tali punti si chiameranno punti all'infinito.

1.2 *Curve ellittiche complesse*

Possiamo ora dare una definizione generale di curva ellittica su un generico campo k. Indicheremo con $k(E)$ il campo delle funzioni razionali definite su E a coefficienti in k; il genere di una curva è il numero dei sui buchi.

Definizione 1.5. Una curva ellittica E è una coppia (E, O), dove E è una curva non singolare di genere uno e $O \in E$. Diremo che E è definita su k, quando E è definita su k come curva e $O \in E(k)$.

Enunciamo il seguente teorema che ci permette di trattere le curve ellittiche come varietà proiettive.

Teorema 1.6. *Sia E una curva ellittica definita su k.*
i) Esistono funzioni $x, y \in K(E)$ tali che la mappa

$$\varphi : E \longrightarrow \mathbb{P}^2(k), \quad \varphi = (1 : x : y),$$

dà un isomorfismo di $E(K)$ su una curva data da un'equazione di Weierstrass

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

con coefficienti $a_1, \ldots, a_6 \in K$ e tale che $\varphi(O) = (0 : 0 : 1)$ (punto all'infinito). Le funzioni x e y sono dette coordinate di Weierstrass per la curva ellittica E.
ii) Qualsiasi due equazioni di Weierstrass per E come in i) sono collegate da un cambiamento lineare di variabili della forma

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t,$$

con $u \in K \setminus \{0\}$ e $r, s, t \in K$.
iii) Viceversa, ogni curva cubica liscia C data da un'equazione di Weierstrass come in i) è una curva ellittica definita su K con punto base $O = (0 : 0 : 1)$.

Dimostrazione. Per una dimostrazione del teorema consultare **[2]**. □

D'ora in avanti quando parleremo di una curva ellittica intenderemo la curva non singolare fornita da un polinomio in forma di Weiestrass. Con E/k si intende che E è definita su k; le funzioni x e y dell'enunciato saranno del coordinate locali di E, e con $E(k)$ si indicano i punti di E a coordinate in k. Si può usare la forma affine proposta nell'enunciato a cui bisogna aggiungere lo zero, oppure si può usare la versione proiettiva (omogeneizzata) della forma di Weiestrass:

$$C : wy^2 + a_1xyw + a_3yw^2 = x^3 + a_2x^2w + a_4xw^3 + a_6w^3$$

Da cui, ponendo $w = 0$, si ottiene un punto aggiuntivo $(0 : 0 : 1)$ che altro non è che il punto O della curva ellittica che giace sulla retta all'infinito. Disomogeneizzando le rette che passano per $(0 : 0 : 1)$ otteniamo rette affini parallele all'asse x. Quando $k = \mathbb{R}$, se vogliamo tracciare una retta passante per $P = (x, y) \in E$ ed O basterà tracciare la verticale passante per P.
Un cambio di variabile è *ammissibile* se e solo se è della forma descritta in *ii*). Diremo che 2 polinomi di Weiestrass (o 2 curve ellittiche) sono equivalenti se legati da un cambio di coordinate ammissibile. Vediamo allora come possiamo trovare scritture più agevoli per E. Partiamo da $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ che insieme ad O forma una curva ellittica. Se $\mathrm{char}(\overline{K}) \neq 2$, allora possiamo semplificare l'equazione completando il quadrato ($\overline{K}$ è la chiusa algebrica del campo). Sotto il seguente cambio di coordinate ammissibile:

$$y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$$

l'equazione si presenta nella forma

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

dove i coefficienti sono legati da

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Definiamo inoltre le quantità

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

hiameremo Δ il *discriminate* del polinomio in forma di Weiestrass.
Possiamo che mostrare come un cambio di coordinate ammissibile agisce sulle quantità usate:

$$u_2'b_2 = b_2 + 12r,$$

$$u_4'b_4 = b_4 + rb_2 + 6r^2,$$

$$u_6'b_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3,$$

$$u_8'b_8 = b_8 + 3rb_6 + 3r^2b_4 + 3r^4$$

Osservazione 1.7. Un conto diretto mostra che, sotto un cambio di coordinate ammissibili, Δ e Δ' (discriminante nelle nuove coordinate) sono legati della relazione:

$$u^{12}\Delta' = \Delta$$

Definiamo le quantità

$$c_4 = b_2^2 - 24b_4$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

Definizione 1.8. Per una curva tale che $\Delta \neq 0$ definiamo il j-invariant come

$$j(E) = j = \frac{c_4^3}{\Delta}$$

Osservazione 1.9. Sotto un cambio di coordinate ammissibili c_4' e c_6' sono: $u^4c_4' = c_4$ e $u^6c_6' = c_6$. Dunque $j(E') = \frac{c_4'^3}{\Delta'} = \frac{c_4^3}{u^12}\frac{u^{12}}{\Delta} = \frac{c_4^3}{\Delta} = j(E)$. Possiamo dunque affermare j è un invariante per trasformazioni ammissibili.

Se $\mathrm{char}(\overline{K}) \neq 2, 3$, allora la sostituzione

$$(x, y) \longrightarrow \left(x - \frac{3b_2}{36}, \frac{y}{108}\right)$$

elimina il termine in x^2, ottenendo l'equazione semplificata

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Osservazione 1.10. Se chiamiamo $A = -27c_4$ e $B = -54c_6$ otteniamo:

$$E : y^2 = x^3 + Ax + B.$$

In questa forma il discriminante è $\Delta = -16(4A^3 + 27B^2)$.

Teorema 1.11. *Sia k un campo algebricamnete chiuso di caratteristica 0. Siano $E : y^2 = x^3 + Ax + B$ ed $E' : y'^2 = x'^3 + Ax' + B$. tali che $j(E) = j(E')$. E ed E' sono legate da un cambio di coordinate ammissibili.*

Dimostrazione. Come abbiamo notato nell'Osservazione **1.10**, $\Delta = -16(4A^3+27B^2)$. La condizione di uguaglianza degli invarianti si scrive dunque come: $\frac{(4A)^3}{4A^3+27B^2} = \frac{(4A')^3}{4A'^3+27B'^2}$ che determina la condizione $A^3B'^2 = A'^3B^2$, che è equivalente a $(A/A')^{\frac{1}{4}} = (B/B')^{\frac{1}{6}}$. Il cambio di coordinate che cerchiamo sarà del tipo:

$$x = x'u^2$$

$$y = y'u^3$$

Dobbiamo distinguere 3 casi per esplicitare u. Il primo caso è $A = 0$: essendo $\Delta \neq 0$, B non potrà essere nullo. Inoltre, $A = 0$ implica $j = 0$, e quindi $A' = 0$. Il cambio di coordinate cercato sarà allora $u = (B/B')^{\frac{1}{6}}$. Infatti, sostituendo otteniamo:

$$y'^2(B/B') = x'^3(B/B') + B$$

Dividere per B, e moltiplicare per B' porta all'equazione di E'. Il secondo caso è per $B = 0$, in questo casa j sarà costante per ogni scelta di A. Il cambio di coordinate in questo caso è $(A/A')^{\frac{1}{4}}$ che con un conto analogo al precedento porta all'euazione cercata. Infine, per caso $AB \neq 0$ con j non nullo vanno bene entrambi i cambi precenti (sono lo stesso numero se i coeffincienti non sono nulli). □

Diamo ora una condizione di non singolarità per i polinomi (e le relative curve ellittiche) in forma di Weiestrass.

Teorema 1.12. *Un polinomio in forma di Weiestrass individua una curva non singolare (e quindi una curva ellittica) se e solo se* $\Delta \neq 0$.

Dimostrazione. Sia E definita dall'equazione di Weierstrass

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Iniziamo mostrando che il punto all'infinito non è mai singolare. Consideriamo quindi la curva in $\mathbb{P}^2(k)$ con equazione omogenea

$$F(w, x, y) = y^2w + a_1xyw + a_3yw^2 - x^3 - a_2x^2Z - a_4xw^2 - a_6w^3 = 0$$

e il punto $O = (0 : 0 : 1)$. Poiché

$$\frac{\partial F}{\partial w}(O) = 1 \neq 0,$$

concludiamo che O non è mai un punto singolare di E. Possiamo allora limitarci a studiari i punti della curva affinizzata.
Supponiamo ora che E sia singolare nel punto $P_0 = (x_0, y_0)$; in P_0 si annullano le derivate parziali di f. La sostituzione

$$x = x' + x_0, \quad y = y' + y_0$$

lascia invariato Δ $(u = 1)$, quindi senza perdita di generalità possiamo assumere che E sia singolare in $(0, 0)$. Allora

$$a_6 = f(0, 0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(0, 0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(0, 0) = 0,$$

quindi l'equazione di E assume la forma

$$E : f(x, y) = y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

Questa equazione ha quantità associate

$$\Delta = 0.$$

Per l'osservazione **1.8** la condizione di nullità del discriminante varrà per ogni possibile polinomio definiente di E.
Per completare la dimostrazione, resta da mostrare che se E è non singolare, allora

$\Delta \neq 0$ (contronominale di '$\Delta = 0$ implica curva singolare'). Per semplificare il calcolo, assumiamo che $\mathrm{char}(K) \neq 2$ e consideriamo un'equazione di Weierstrass della forma

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

La curva E è singolare se e solo se esiste un punto $(x_0, y_0) \in E$ tale che

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

In altre parole, i punti singolari sono esattamente i punti della forma $(0, x_0)$ con x_0 radice doppia di $4x^3 + b_2x^2 + 2b_4x + b_6$. Questo polinomio ha una radice doppia se e solo se il suo discriminante, che è uguale a 16Δ, si annulla. □

1.3 *Operazione di gruppo*

Possiamo ora concentrarci sull'aspetto algebrico delle curve ellittiche, ovvero dotare questa struttura di un'operazione fra punti.

Definizione 1.13. Siano $P, Q \in E$, dove E è una curva ellittica. Sia L la retta passante per P e Q; se $P = Q$, allora L è la tangente ad E nel punto P. Sia R il terzo punto di intersezione tra L ed E.

Sia L' la retta passante per R e per il punto all'infinito O, ovvero la retta verticale per R. Allora L' interseca E nei punti R, O, e in un terzo punto.
Denotiamo questo terzo punto con: $P + Q$.
Col prossimo teorema mostriamo come una curva ellittica con l'operazione appena descritta sia una gruppo abeliano di elemente neutro O

Teorema 1.14. *Sia E una curva ellittica dotata dell'operazione appena descritta.*
i)Se una retta L interseca E nei punti (non necessariamente distinti) P, Q, R, allora

$$(P + Q) + R = O.$$

ii) Per ogni $P \in E$, vale

$$P + O = P.$$

iii) Per ogni $P, Q \in E$, vale

$$P + Q = Q + P.$$

iv)Sia $P \in E$. Esiste un punto di E, denotato con $-P$, tale che

$$P + (-P) = O.$$

v) Siano $P, Q, R \in E$. Allora

$$(P + Q) + R = P + (Q + R).$$

Dimostrazione. La dimostrazione di tutti i punti è banale dalla definizione dell'operazione. L'unico che richede attenzione è il v). Siano A e B punti di E, denotermo il terzo punto di intersezione fra la retta per A e B con la curva con AB. L'associatività è assicurata se mostriamo che $(P+Q)R = P(R+Q)$ poichè O è fissato. Vediamo il caso in cui P, Q, R siano distinti. Per costruire $P(Q+R)$, troviamo prima QR, uniamo questo punto a O, e prendiamo il terzo punto di intersezione, che è $Q+R$. Ora uniamo $Q+R$ a P, ottenendo il punto $P(Q+R)$. Ora dobbiamo mostrare che coincide con $(P+Q)R$. Questo si può ottenere con un argomento grafico, o con un algoritmo per la somma fra punti su una curva ellittica. Il risultato è chiaro dalla figura sotto. Un argomento simile è valido anche per il caso in 2 punti siano coincidenti. □

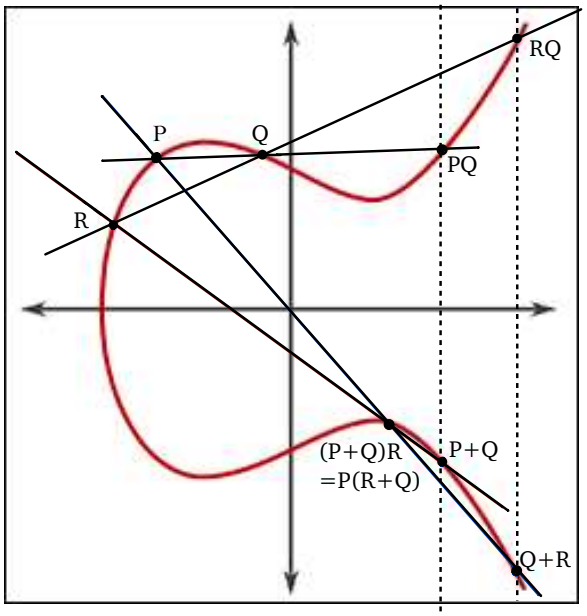

Figura 1.1: Rappresentazione grafica sul piano affine dell'associatività della legge di addizione sullla curva ellittica di equazione $E : y^2 = x^3 - 3x + 3$; il discriminante della curva è $\Delta = 2160$. Se E è definita sul campo complesso, il disegno rappresenta la parte reale della sua affinizzazione.

Osservazione 1.15. Dal punto i) segue che $P + Q = -PQ$.

Per una dimostrazione numerica dell'associatività della somma fra punti consultare [**2**].

Definizione 1.16. Chiameremo punti di n-torsione i punti di E che sommati n volte danno O. I punti di 2-torsione sono i $P \in E$ tali che $P + P = O$.

Graficamente, i punti di 2-torsione sono quelli con tangente verticale. Per esempio in figura, il punto di minimo assoluto per le x è un punto di 2-torsione. Possiamo

enunciare un teorema che specifica ancora di più il perché i cambi di coordinate ammissibili siano tutti e soli quelli definiti in **1.6**.

Teorema 1.17. *Ogni isomorfismo di gruppo fra curve ellittiche è dato da un cambio di coordinate ammissibile.*

Il j-invariant classifica così le curve ellittiche a meno di isomorfismo. Vedere [**1**] per la dimostrazione.

1.4 *Curve ellittiche in forma di Legendre*

D'ora in avanti k sarà sempre $\mathbb{C}$ anche quando ometteremo la dipendenza dal campo.

Definizione 1.18. Un'equazione di Weiestrass è in forma di Legendre se si lascia scrivere come:

$$y^2 = x(x-1)(x-\lambda), \lambda \in \mathbb{C} \setminus \{0,1\}$$

Teorema 1.19. *Ogni curva ellittica complessa è isomorfa ad una curva ellittica il cui polinomio definiente è in forma di Legendre.*

Dimostrazione. Poiché $\mathrm{char}(\mathbb{C}) \neq 2$, sappiamo che E ha un'equazione di Weierstrass della forma

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Essendo $\mathbb{C}$ algebricamente chiuso, possiamo sempre fattorizzare questo polinomio ottenendo tre valori complessi tali per cui:

$$y^2 = (x-e_1)(x-e_2)(x-e_3)$$

Inoltre, poiché

$$\Delta = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2 \neq 0,$$

vediamo che gli e_i sono distinti. Ora la sostituzione

$$x = (e_2-e_1)x' + e_1, \quad y = (e_2-e_1)^{3/2}y'$$

fornisce un'equazione in forma di Legendre con

$$\lambda = \frac{e_3-e_1}{e_2-e_1} \in \mathbb{C}, \quad \lambda \neq 0,1.$$

□

Questa forma sarà spesso il rappresentante della classe di equivalenza delle curve ellittiche che tratteremo. Mostriamo ora che ad ogni curva ellittica complessa si possono associare 6 diversi λ che inducono curve fra loro isomorfe. Supponiamo che $E(\lambda)$ sia equivalente ad $E(\mu)$ entrambe in forma di Legendre. Esisterà allora un cambio di variabili ammissibile che mappa l'una nell'altra. Un cambio di coordinate

è del tipo $(x', y') = (u^2x + r, u^3y + su^2x + t)$. Sia $E(\lambda) : y'^2 = x'(x' - 1)(x' - \lambda)$; apllicando la trasormazione all'equzione di $E(k)$ si ottiene:

$$(u^2x + r)(u^2x + r - 1)(u^2x + r - \lambda) = (u^3y + su^2x + t)^2$$

Se vogliamo preservare la forma di Legendre dobbiamo porre $s = t = 0$ così da potere raccogliere correttamente il polinomio nella variabile x. Dividiamo entrambi i membri per u^3, ottenendo così:

$$y^2 = (x + \frac{r}{u^2})(x + \frac{r-1}{u^2})(x + \frac{r-\lambda}{u^2})$$

Vogliamo l'uguaglianza dei polinomi in x, dobbiamo quindi porre:

$$(x + \frac{r}{u^2})(x + \frac{r-1}{u^2})(x + \frac{r-\lambda}{u^2}) = x(x-1)(x-\mu)$$

Dobbiamo quindi porre i fattori di destra uguali a quelli di sinistra. Ci sono 6 possibili associazioni, vediamo quella che associa il primo fattore al secondo, il secondo al primo, e il terzo al terzo:

$$(x + \frac{r}{u^2}) = (x - 1) \to r = -u^2$$

$$(x + \frac{r-1}{u^2}) = x \to 1 = r, -1 = u^2, u = i$$

$$(x + \frac{r-\lambda}{u^2}) = (x - \mu)$$

ma $\frac{r-\lambda}{u^2} = -1 + \lambda$ e $\mu = 1 - \lambda$. Gli altri possibili abbinamenti forniscono queste possibili scelte di λ:

$$\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}.$$

L'ultima quantità importante da definire è l'invariante differenziale associato ad una curva elliittica.

Definizione 1.20. Per una curva ellittica nella forma:
$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$, definiamo l'*invariant differntial* come:

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

Osservazione 1.21. Dall'equzione di Weiestrass è immediato notare che

$$\omega = \frac{dx}{f_y} = -\frac{dy}{f_x}.$$

Questa forma differenziale è olomorfa poichè per la condizione di non singolarità le derivate parziali non si annulleranno mai. Si veda [**2**].

Osservazione 1.22. Sotto un cambio di coordinate ammissibile l'invariante differenziale cambia nel seguente modo:

$$u^{-1}\omega' = \omega$$

Definizione 1.23. Siano α e β due cammini chiusi non omotopi su $E(\mathbb{C})$, definiamo periodi una curva ellittica i valori complessi

$$w_1 = \int_\alpha \omega \quad \text{e} \quad w_2 = \int_\beta \omega$$

Se $E(\mathbb{C})$ è in forma di Legendre possiamo esprimerli come

$$w_1 = \int_\alpha \frac{dx}{2y} \quad \text{e} \quad w_2 = \int_\beta \frac{dx}{2y}$$

A questo punto della trattazione non è però chiaro se esistano cammini non omotopi su $E(\mathbb{C})$ e quanti siano, lasciamo pertanto questa definizione alla sua vaghezza. Nel terzo capitolo vedremo che questa definizione è ben posta.

1.5 *Tori complessi*

Definiamo ora il secondo oggetto di intersse per la trattazione: il toro complesso. Otterremo questo oggetto come quoziente di $\mathbb{C}$ (inteso come gruppo additivo) e un suo sottoinsieme discreto massimale. Questi sottoinsiemi sono i reticoli.

Definizione 1.24. Un reticolo di $\mathbb{C}$ è un gruppo discreto della forma

$$\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z} = \{nw_1 + mw_2 \mid n, m \in \mathbb{Z}\}$$

per $w_1, w_2 \in \mathbb{C}$ e $w_1/w_2 \in \mathbb{C} \setminus \mathbb{R}$. Chiameremo w_1 e w_2 i *periodi* del reticolo Λ.

Osservazione 1.25. La condizione $w_1/w_2 \in \mathbb{C} \setminus \mathbb{R}$ è equivalente a dire che w_1 e w_2 sono $\mathbb{R}$-linearmente indipendenti. Due numeri complessi di questo tipo generano $\mathbb{C}$ come $\mathbb{R}$-spazio vettoriale.

Teorema 1.26. *Ogni sottogruppo discreto di $\mathbb{C}$ è della forma $w_1\mathbb{Z}$ o $w_1\mathbb{Z} + w_2\mathbb{Z}$ con $w_1, w_2 \in \mathbb{C}$ e $w_1/w_2 \in \mathbb{C} \setminus \mathbb{R}$.*

Dimostrazione. Se $\Lambda = 0$, allora $\Lambda = \mathbb{Z}w1$ e $w_1 = 0$. Altrimenti, per r sufficientemente grande, il disco compatto $|z| \leq r$ contiene elementi di $\Lambda \setminus \{0\}$ e solo un numero finito, poiché Λ è discreto. Scegliamo w_1 un elemento non nullo di Λ con valore assoluto minimo. Se ogni $w \in \Lambda$ si scrive come $w = w_1\mathbb{Z}$ siamo nel primo caso, supponiamo allora che esista $w \in \Lambda \setminus \mathbb{Z}w_1$. Tra questi w, sia w_2 uno con valore assoluto minimo. Osserviamo che w_2/w_1 non è reale: se lo fosse, esisterebbe un intero n tale che $n < w_2/w_1 < n + 1$, e quindi $|w_2 - nw_1| < |w_1|$, contraddicendo la minimalità di $|w_1|$. Rimane da mostrare che $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Poiché w_2/w_1 non è reale, per l'osservazione **1.19** segue che $\mathbb{C} = \mathbb{R}w_1 + \mathbb{R}w_2$. Per $w \in \Lambda$ possiamo

scrivere $w = aw_1 + bw_2$ con $a, b \in \mathbb{R}$ e trovare interi m, n tali che $|a - m| \leq \frac{1}{2}$ e $|b - n| \leq frac12$. Poiché $w, w_1, w_2 \in \Lambda$, abbiamo

$$w' = w - mw_1 - nw_2 \in \Lambda,$$

dove $|w'| \leq \frac{1}{2}|w_1| + \frac{1}{2}|w_2| \leq |w_2|$, e la prima disuguaglianza è stretta poiché w_2 non è un multiplo reale di w_1. Dal carattere minimo di $|w_2|$ deduciamo che $w' \in \mathbb{Z}w_1$, questo mostra che $w \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Questo termina la dimostrazione.

□

Siamo pronti a definire il toro complesso come quozionente di gruppi.

Definizione 1.27. Sia $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ un reticolo. Definiamo il toro associato al reticolo come il gruppo topologico

$$T = \mathbb{C}/\Lambda$$

L'operazione e la topologia sono quelle ereditate di $\mathbb{C}$ e i sui *periodi* sono quelli di Λ.

Segue dalla definizone che ad ogni reticolo corrisponde uno ed un solo toro e viceversa. Capiamo ora come sono fatte le classi di equivalenza del gruppo.

$$[x]_\Lambda = \{y \in \mathbb{C} \mid x \equiv_\Lambda y\} = \{y \in \mathbb{C} \mid x - y \in \Lambda\} = x + \Lambda$$

Per studiare la topologia indotta da $\mathbb{C}$ sul quoziente bisogna identificare le classi di equivalenza in un solo punto. Per avere l'intuizione geometrica di questo insieme come spazio topologcio prendiamo un sottinsieme di $\mathbb{C}$ che ci permetta di visualizzare le classi di equivalenza: il più naturale è il parallelogramma di cui un vertice è l'origine, i cui lati sono w_1, w_2 e i rispettivi segmenti paralleli. Se lo consideriamo chiuso i lati opposti sono equivalenti. Questo insieme è omemeomorfo al prodotto cartesiano di due circonferenze $\mathbb{S}^1 \times \mathbb{S}^1 \in \mathbb{R}^3$, qui possiamo visualizzare i periodi di Λ (intesi come lati del parallelogramma con vertice in 0) come le circonferenze fondamentali del toro di $\mathbb{R}^3$. Si veda il **[5]** per una dimostrazione. Possiamo perciò affermare che $\mathbb{C}/\Lambda$ è compatto per la topologia euclidea.
Il parallelogramma di rappresentanti non è unico: ogni parallelogramma di lati w_1 e w_2 contiene un rappresentante per classe, a prescindere dal punto di appoggio.

Definizione 1.28. Un parallelogramma fondamentale associato a $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ un qualsiasi parallegramma del tipo $P = z_0 + aw_1 + bw_2$ con $z_0 \in \mathbb{C}$ qualsiasi e a, b parametri reali tali che $0 \leq a, b < 1$.

Osservazione 1.29. Il toro è isomorfo al prodotto cartesiano di 2 circonfernze unitarie, questo implica che il suo primo gruppo fondamentale è $\pi_1(\mathbb{C}/\Lambda) = \mathbb{Z} \times \mathbb{Z}$. Questo gruppo è abeliano, dunque $\pi_1(\mathbb{C}/\Lambda) \simeq H_1(\mathbb{C}/\Lambda, \mathbb{Z})$, dove $H_1(\mathbb{C}/\Lambda, \mathbb{Z})$ è il primo gruppo di omologia del toro.

Definizione 1.30. Diremo che due reticoli Λ e Λ' sono equivalenti se e solo se esiste $\lambda \in \mathbb{C} \setminus \{0\}$ tale che $\Lambda = \lambda\Lambda'$. Questa funzione induce naturalmente un'equivalenza di tori data da:

$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$

$$z \mapsto \lambda z$$

Tale applicazione induce un isomorfismo di gruppi discreti. Diremo che due tori (o due reticoli) sono nella stessa classe di equivalenza se sono equivalenti.

Nel prossimo capitolo tratteremo in dettaglio le funzioni moromorfe (analititiche a meno di poli isolati) fra tori complessi, data la loro definizione come quozionete su un reticolo avrenno delle particolari periodicità.

Capitolo 2

Isomorfismo da toro a curva

In questo capitolo ci occuperemo delle funzioni ellitiche, ovvero le funzioni $f : \mathbb{C} \to \mathbb{C}$ che rispettano la struttura di Λ. Studieremo in particolare un'importante classe di funzioni, le $\wp$-function: ad ogni reticolo si può infatti associare una $\wp$-function. Capiremo quindi il collegamento fra il toro e la struttura algebrica indotta dai divisori associati alle funzioni ellittiche tramite il teorema di Abel-Jacobi. Infine, nell'ulitma parte, discuteremo come ogni toro complesso sia legato ad una curva ellittica parametrizzata dalla sua $\wp$-function e di come questi gruppi siano analiticamente isomorfi.

2.1 *Funzioni ellittiche*

Le funzioni che tratteremo sono tutte *meromorfe*, ovvero funzioni $f : \mathbb{C} \to \mathbb{C}$ olomorfe a meno di un insime $N \subset \mathbb{C}$ privo di punti di accumulazione, i cui punti sono poli di f.

Definizione 2.1. Sia $\Lambda = w_1\mathbb{Z}+w_2\mathbb{Z}$ un reticolo; una funzione $f : \mathbb{C} \to \mathbb{C}$ meromorfa tale che $f(z + w) = f(z)$ per ogni $w \in \Lambda$, si dice funzione ellittica (associata a Λ). Equivalentemente, una funzione è ellittica associata a Λ se e solo se è biperiodica per w_1 e w_2, ovvero $f(z + w_1) = f(z)$ e $f(z + w_2) = f(z)$ per ogni $z \in \mathbb{C}$.

Definizione 2.2. Sia f una funzione meromorfa, diremo che *m è l'ordine di f in a* e scriviamo $\operatorname{ord}_a f = m$ quando $f(z) = (z - a)^m g(z)$ dove $g(z)$ è olomorfa in un intorno di a e $g(a) \neq 0$. Se $\operatorname{ord}_a f > 0$ allora a è uno zero e m è la sua molteplicità. Se $\operatorname{ord}_a f < 0$ allora a é un polo di f di grado m. Chiameremo poli semplici i poli di ordine 1 e poli doppi i poli di ordini 2. Ogni punto di ordine non nullo è detto punto singolare.

Studieremo ora le principali prorpietà delle funzioni ellittiche tramite la loro integrazione sul bordo di un parallelogramma fondamentale; denoteremo con $\mathcal{P}$ un parallelogramma e con Φ il suo bordo, ovvero il cammino chiuso composto dai segmenti $[a, a + w_1]$, $[a + w_1, a + w_1 + w_2]$, $[a + w_1 + w_2, a + w_2]$ e $[a + w_2, a]$. Notiamo innanzituto che per ogni funzione ellittica esiste un parallelogramma fondamentale

che non ha punti singolari sul bordo.
Sia $\mathcal{P}$ un parallelogramma fondamentale ed f funzione ellittica con punti singolari sul bordo di $\mathcal{P}$; f è meromorfa, dunque ha poli e zeri isolati (gli zeri sono isolati poichè $1/f$ è meromorfa). Per definizione di funzione meromorfa non ci sono punti singolari di accumulazione su $\mathcal{P}$ (l'unione di due insiemi senza punti di accumulazione non ha punti di accumulazione), perciò esistono due rette $r_1 = z_1 + \mathbb{R}w_1$ ed $r_2 = z_2 + \mathbb{R}w_2$ per qualche $z_1, z_2 \in \mathbb{C}$ che tagliano $\mathcal{P}$ e si incotrano in $z \in \mathcal{P}$ che non contengono punti singolari. Il parallelogramma $z + aw_1 + bw_2$ con $0 \leq a, b < 1$ non ha punti singolari sul bordo infatti se y fosse un punto singolare su $z + aw_1$, sarebbe, per costruzione, fuori da $\mathcal{P}$, ma allora $y - w_1 \in r_1 \cap \mathcal{P}$ sarebbe un punto singolare, e questo è assurdo. Se f non ha singolarità su questo lato, non ne ha nemmeno su quello opposto. Il ragionamento è analogo per l'altra coppia di lati.
I seguenti teoremi sono utilli per studiare i punti singolari delle funzioni ellittiche.

Teorema 2.3. *Se $f(z)$ è una funzione ellittica senza zeri o poli sul bordo del parallelogramma fondamentale, allora la somma dei residui di f è nulla.*

Dimostrazione. Per il Teorema dei Residui:

$$\frac{1}{2\pi i}\int_{\Phi} f(z)\,dz = \sum_{a\in\mathcal{P}} \mathrm{Res}(f(a)$$

Dove gli $a \in \mathcal{P}$ sono i poli di f. Calcoliamo dunque l'integrale a sinistra: possiamo spezzarlo in 4 integrali, ovvero i contributi dei 4 lati. Per la condizione di periodicità: $f(z + w_1) = f(z)$ e $f(z + w_2) = f(z)$ per ogni $z \in \mathbb{C}$ Questo vuol dire che la funzione valutata sui lati opposti ha lo stesso valore, ed essendo percorsa in direzioni opposte i contributi si annullano a due a due. □

Corollario 2.4. *Una funzione ellittica non può avere un unico polo semplice* $\bmod \Lambda$.

Teorema 2.5. *Sia f una funzione ellttica senza zeri e zenza poli sul bordo di $\mathcal{P}$ e siano gli $a \in \mathcal{P}$ i punti singolari di f, allora:*

$$i) \sum_{a\in\mathcal{P}} \mathrm{ord}_a f = 0$$

$$ii) \sum_{a\in\mathcal{P}} a\,\mathrm{ord}_a f \equiv_\Lambda 0$$

Dimostrazione. i) notiamo che gli zeri e i poli di f sono poli semplici di f'/f; ovvero

$$\frac{f'(z)}{f(z)} = \sum_{a\in\mathcal{P}} \frac{\mathrm{ord}_f(a)}{z-a} + g(z)$$

dove $g(z)$ è olomorfa in $\mathbb{C}$ non nulla in a. Da questa scrittuta è evidente che i residui di f'/f saranno gli ordini dei realativi valori per f. Possiamo notare che se f è ellittica lo è anche la sua drivate, infatti per ogni $z_0 \in \mathbb{C}$, $w \in \Lambda$ vale:

$$f'(z_0) = \lim_{z\to z_0} \frac{f(z) - f(z_0)}{z - z_0} = \lim_{z\to z_0} \frac{f(z+w) - f(z_0+w)}{z - z_0} = f'(z_0 + w)$$

Segue che f'/f è ellittica, vale il teorema **2.3** e quindi

$$\sum_{a\in\mathcal{P}} \mathrm{Res}_a(f'/f) = \sum_{a\in\mathcal{P}} \mathrm{ord}_a(f) = 0$$

ii) Il secondo risultato segue dal considerare l'integrale:

$$\frac{1}{2\pi i}\int_\Phi \frac{f'(z)}{f(z)} z\, dz$$

Si può calcolarne il valore col teorema dei residui. I poli sono tutti semplici, per calcolarli basta moltiplicare la funzione per $(z-a)$ e calcolare il limite per z che tende ad a, ottenendo:

$$\sum_{a\in\mathcal{P}} a\cdot \mathrm{ord}_f(a)$$

Scegliamo un parallelogramma fondamentale $a + w_1\mathbb{Z} + w_2\mathbb{Z}$. Calcoliamo esplicitamente l'integrale spezzandolo nei contributi dati dai 4 lati di $\mathcal{P}$. Se consideriamo i lati opposti otteniamo

$$\frac{1}{2\pi i}\int_a^{a+w_1} \frac{f'(z)}{f(z)} z\, dz - \frac{1}{2\pi i}\int_{a+w_2}^{a+w_1+w_2} \frac{f'(z)}{f(z)} z\, dz = \frac{w_2}{2\pi i}\int_a^{a+w_1} \frac{f'(z)}{f(z)}\, dz$$

Dove abbaimo traslato z di $-w_2$ nel secondo integrale. Tralasciando le costanti moltiplicative, stiamo dunque studiando l'integrale di f'/f lungo un segmento. Effettuiamo il cambio di variabile $f(z) = 1/k$ e quindi $f'(z)dz = -\frac{1}{k^2}dk$:

$$\int_a^{a+w_1} \frac{f'(z)}{f(z)}\, dz = -\int_\gamma \frac{1}{k} dk = 2\pi i N$$

Per qualche cammino γ di punto iniziale γ_o e punto finale γ_1.
La condizione $\frac{f'(a)}{f(a)} = \frac{f'(a+w_1)}{f(a+w_1)}$ implica che $\frac{1}{\gamma_0} = \frac{1}{\gamma_1}$ e quindi $\gamma_0 = \gamma_1$. Il segmento $[a, a+w_1]$ diventa un qualche cammino chiuso percorso un certo numero di volte. Dal teorema dei residui segue che il valore dell'integrale è $N2\pi i$ dove $N \in \mathbb{Z}$ è il numero di avvolgimenti di $1/k$ su γ. Il segno di N è determinato dal verso di percorrenza In maniera analoga se studiamo l'altra coppia di integrali sui lati otteniamo $w_1 M$ per quache M un numero intero. Il valore dell'integrale è del tipo $Nw_1 + Mw_2$ dunque apparterrà a Λ. Per una dimostrazione del teoremo dei residui consultare [**4**]. □

Osservazione 2.6. Abbiamo mostrato che data un curva ellittica è sempre possibile gtrovare un parallelogramma fondamentale che non abbia punti singolari sul bordo, pertanto i teoremi **2.3** e **2.5** si applica quindi ad ogni funzione ellittica.

Osservazione 2.7. L'insieme M_Λ delle funzioni ellittiche associate ad un reticolo con le operazioni di addizione e moltiplicazione fra funzioni forma unn campo. Un sottocampo importante di M_Λ è $\mathbb{C}$ stesso, inteso come spazio delle funzioni costanti.

Osservazione 2.8. Una funzione ellittica f è una funzione dal piano complesso in se stesso, ma data la sua biperiodicità è possibile considerare f^* ottenuta componendo f con $p : \mathbb{C} \to \mathbb{C}/\Lambda$ priezione canonica di $\mathbb{C}$ sul toro. Ad ogni f ellittica corrisponderà una ed una sola f^* sul toro e viceversa. Possiamo dunque interpretare M_Λ come il campo delle funzioni meromorfe sul toro $T = \mathbb{C}/\Lambda$.

Osservazione 2.9. Per il teorema Liouville se f ellittica non ha poli, allora è costante.. In particolare, vale che $\sup_f \mathbb{C} = \sup_f C(\mathcal{P})$ dove $C(\mathcal{P})$ è la chiusura topologica di $\mathcal{P}$; f è dunque limititata e si applica il teorema. Per una dimostrazione del teorema di Liouville consultare [**4**].

2.2 $\wp$-*function di Weiestrass*

A questo punto della trattazione l'unico esempio esplicito di funzione ellittica è la funzione costante $f \equiv z_0$, $z_0 \in \mathbb{C}$. Daremo ora degli esempi significativi di funzioni meromorfe biperiodiche associate ad un reticolo; useremo spesso delle somme sugli elementi di un reticolo. Diamo dunque un criterio di covergenza per tali serie.

Lemma 2.10. *Sia $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ con w_2/w_1 non reale un reticolo ed $s \in \mathbb{R}$; se $s > 2$, la seguente somma converge assolutamente*

$$\sum_{w \in \Lambda \setminus \{0\}} \frac{1}{w^s}$$

Dimostrazione. Poichè Λ è un sottogruppo discreto di $\mathbb{C}$, esiste $c > 0$ tale che per ogni coppia di interi n_1 e n_2 vale $|n_1 w_1 + n_2 w_2| \geq c(|n_1| + |n_2|)$, dove la costante c dipende dalla minima distanza di $\Lambda \setminus \{0\}$ dall'origine. Passando ai reciproci la disuguaglianza cambierà verso. Per ogni $n \in \mathbb{N}$ esistono $4n$ coppie di naturali tali che $n = n_1 + n_2$, infatti ogni naturale si può scrivere come somma di $n+1$ coppie ordinate di naturali ovvero: $(0, n), (1, n-1), (2, n-2), \ldots, (n-1, 1), (n, 0)$. Escludendo le coppie $(0, n)$ ed $(n, 0)$, abbiamo $4(n-1)$ coppie di interi che sommano ad n. Questo poichè se (k, m) sono una coppia di naturali non nulli che somma ad n, anche $(k, m), (-k, m), (k, -m), (-k, -m)$ hanno questa proprietà. A queste $4(n-1)$ coppie $(n, 0), (-n, 0), (0, n), (0, -n)$, ottenendo così $4(n-1)+4 = 4n$ coppie ordinate. Quindi, per $(n_1, n_2) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$:

$$\sum_{w \in \Lambda \setminus \{0\}} \frac{1}{|w|^s} = \sum_{n_1} \sum_{n_2} \frac{1}{|(w_1 n_1 + w_2 n_2)|^s} \leq \sum_{n_1} \sum_{n_2} \frac{1}{(c(|n_1| + |n_2|))^s} =$$

$$= \frac{4}{c^s} \sum_{n>0} \frac{1}{n^{s-1}}$$

L'ultima somma converge se e solo se $s - 1 > 1$ ovvero quando $s > 2$. $\square$

Definizione 2.11. Definiamo la $\wp$-function di Weiestrass e la ζ-function associata ad un reticolo

$$\wp(z;\Lambda) := \wp(z) = \frac{1}{z^2} + \sum_{w\in\Lambda\setminus\{0\}} \left[\frac{1}{(z-w)^2} - \frac{1}{w^2}\right]$$
$$\zeta(z;\Lambda) := \zeta(z) = \frac{1}{z} + \sum_{w\in\Lambda\setminus\{0\}} \left[\frac{1}{(z-w)} + \frac{1}{w} + \frac{z}{w^2}\right]$$

Siccome, gaurdando gli argomenti delle somme, per $\wp$ vale

$$\frac{1}{(z-w^2)} - \frac{1}{w^2} = \frac{2wz - z^2}{w^2(z-w)^2}$$

e per ζ vale

$$\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} = \frac{z^2}{w^2(z-w)}$$

Notiamo che entrambe asintoticamente si comporatano come $1/w^3$ per $|w|$ abbastanza grandi e quindi per il Lemma **2.10** sono assolutamente convergenti fuori da Λ. Definiscono inoltre funzioni meromorfe su $\mathbb{C}$ con poli del secondo oridne per $\wp$, e poli del primo ordine per ζ in ogni $z \in \Lambda$; non hanno altri poli e $\wp$ è pari.
Data la covergenza assoluta ha senso derivare sotto il segno di sommatoria: possiamo quindi osservare come le due funzioni siano legate dall'espressione:

$$\zeta'(z) = -\wp(z)$$

ed inoltre:

$$\wp'(z;\Lambda) = -2 \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{(z-w)^3}$$

Fissando un qualsiasi $\bar{w} \in \Lambda$ possiamo notare come $\wp'$ sia biperiodica:

$$f(z+\bar{w}) = -2 \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{(z+\bar{w}-w)^3} = -2 \sum_{w+\bar{w}\in\Lambda\setminus\{-\bar{w}\}} \frac{1}{(z-w)^3} =$$

$$= -2 \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{(z-w)^3} = f(z)$$

e poichè $\wp$ è pari $\wp'$ è chiaramente dispari.
Integrando l'espressione $\wp'(z+w_i) = \wp'(z)$ otteniamo $\wp(z+w_i) = \wp(z) + c_i$ per $i = 1, 2$. Sfruttiamo ora la parità di $\wp$:

$$\wp(\frac{w_i}{2}) = \wp(-\frac{w_i}{2} + w_i) = \wp(-\frac{w_i}{2}) + c_i = \wp(\frac{w_i}{2}) + c_i$$

Da cui segue che $c_i = 0$, $i = 1, 2$. Questo mostra come la $\wp - function$ di Weiestrass sia ellittica.

Osservazione 2.12. Per disparità e biperiodicità vale che:

$$\wp'(\frac{w_i}{2}) = \wp'(\frac{w_i}{2} - w_i) = \wp'(-\frac{w_i}{2}) = -\wp'(\frac{w_i}{2})$$

Questo implica che $\wp'(\frac{w_i}{2}) = 0$ per $i = 1, 2, 3$ dove $w_3 = w_1 + w_2$. Siccome $\wp'$ ha solo un polo triplo mod_Λ, per il Teorema **2.6** può avere solo queste tre radici.

Osservazione 2.13. Per l'osservazione **2.7** la somma dei punti singolari di $\wp$ è nulla. Questa funzione presenta un polo doppio di zero e non ha altri poli, per compensarlo $\wp$ deve avevre 2 zeri.

Col prossimo teorema mostriamo come possiamo ottenere tutte le funzione ellittiche associate a Λ solo in terminni di $\wp(z)$ e $\wp'(z)$.

Teorema 2.14. *Sia Λ un reticolo, il campo M_Λ si ottiene come:*

$$\mathbb{C}(\wp(z;\Lambda), \wp'(z;\Lambda))$$

Dimostrazione. Per una dimostrazione consultare [**1**]. □

2.3 *Divisori e teorema di Abel-Jacobi*

Torneremo a studiare la $\wp-function$ nella prossima sezione tramite le sue espansioni in serie di Laurent. Ora concentriamoci sul capire cosa siano i divisori e che struttura algebrica inducano nel caso toro.

Definizione 2.15. Un divisore D di $\mathbb{C}/\Lambda$ è una somma formale finita del tipo $D = \sum_u n_u(u)$ dove gli u sono punti di $\mathbb{C}/\Lambda$ e gli n_u interi nulli a meno di un numero finito. Definiamo il grado di un divisore come $deg(D) = \sum_u n_u \in \mathbb{Z}$.

Definizione 2.16. Denoteremo con $Div(\mathbb{C}/\Lambda)$ il gruppo dei divisori associati al Toro $\mathbb{C}/\Lambda$. L'operazione di gruppo è definita nel seguente modo:

$$D + D' = \sum_u n_u(u) + \sum_{u'} n'_u(u')$$

Dove i coefficienti si sommano se e solo se $u = u'$. In particolare diremo che D è principale se è del tipo $D = (f) = \sum_u \text{ord}_u(f)(u)$ con $f \in M_\Lambda$ non costantemente nulla.
Indicheremo con $Div_p(\mathbb{C}/\Lambda)$ e $Div_0(\mathbb{C}/\Lambda)$ rispettivamente il sottogruppo dei divisori principali e il sottogruppo dei diviosri di grado 0.

Possiamo notare come, per l'osservazione **2.6**, $Div_p(\mathbb{C}/\Lambda)$ sia un sottogruppo di $Div_0(\mathbb{C}/\Lambda)$; vale dunque la seguente sequenza esatta dove le prime inclusioni sono canoniche e il morfismo tra $Div(\mathbb{C}/\Lambda)$ e $\mathbb{Z}$ è la mappa grado. Risulta chiaro che il nucleo di questa mappa sia dato dai divisori di grado zero.

$$0 \to Div_0(\mathbb{C}/\Lambda) \to Div(\mathbb{C}/\Lambda) \to \mathbb{Z} \to 0$$

Teorema 2.17. *(Abel-Jacobi) Sia $\mathbb{C}/\Lambda$ un toro complesso.*
La funzione $f : Div_0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$ con $f(\sum_u n_u(u)) = \sum_u n_u u$, induce sul quoziente un isomomorfismo di gruppi F

$$F : Div_0(\mathbb{C}/\Lambda)/Div_p(\mathbb{C}/\Lambda) \longrightarrow \mathbb{C}/\Lambda$$

Per dimostrare agilmente questo teorema ci servirà un Lemma. Introduciamo a tal proposito la funzione *sigma* di Weiestrass.

Definizione 2.18. La funzione *sigma* di Weiestrass è definita dal prodotto

$$\sigma(z;\Lambda) = z \prod_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(1 - \frac{z}{\omega}\right) e^{\left(\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)}$$

Questa funzione gode di diverse proprietà:
i)σ è olomorfa in $\mathbb{C}$ e i sui zeri (semplici) sono tutti e soli i punti $w \in \Lambda$;
ii) $\frac{d^2}{dz^2}\log\sigma(z) = -\wp(z)$ per ogni $z \in \Lambda$;
iii) per ogni $z \in \Lambda$ esistono a,b (che dipendono da Λ) tali che $\sigma(z+w) = e^{az+b}\sigma(z)$.

La prima proprietà è conseguenza delle generali regole di convergenze delle produttorie; per la seconda notiamo che

$$\log(\sigma(z)) = \log\left(z \prod_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(1 - \frac{z}{\omega}\right) e^{\left(\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)}\right) = \log z + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\left(1 - \frac{z}{\omega}\right) - \frac{z}{\omega} - \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)$$

derivando due volete termine a termine si ottiene $-\wp(z)$.
Per la terza è necessario integrare 2 volte la formula $\wp(z+w) = \wp(z)$ e usare *ii)* ottenendo:

$$\log\sigma(z+w) = \log\sigma(z) + az + b$$

con a e b costanti di integrazione. Il risultato è chiaro passando agli esponenziali da entrambi i lati.

Lemma 2.19. *Sia $n_1, \ldots, n_r$ una sequenza di interi, e $z_1, \ldots, z_r$ una sequenza di punti complessi tali che*

$$\sum_i n_i = 0 \qquad \sum_i n_i z_i = 0$$

allora esiste $f \in M_\Lambda$ tale che $(f) = \sum_i n_i(z_i)$

Dimostrazione. Costruiamo f ellittica sul Λ associata a questo divisore usando la funzione σ di Weiestrass:
La condizione i) implica che la funzione

$$f(z) = \prod_i \sigma(z - z_i)^{n_i}$$

abbia gli zeri e i poli corretti, dove $\sigma(z)$ è la funzione *sigma* di Weierstrass associata al reticolo Λ. Inoltre, la condizione iii) ci permette di calcolare, per ogni $\omega \in \Lambda$,

$$\frac{f(z+w)}{f(z)} = \frac{\prod_i e^{(a(z-z_i)+b)n_i}\sigma(z-z_i)^{n_i}}{\prod_i \sigma(z-z_i)^{n_i}} = \prod_i e^{(a(z-z_i)+b)n_i} =$$

$$= \prod_i e^{-an_iz_i+z_i(az+b)} = e^{-a\sum_i n_iz_i}e^{(az+b)\sum_i z_i} = 1.$$

Poiché $\sum_i n_i = 0$ e $\sum_i n_iz_i = 0$, otteniamo

$$\frac{f(z+\omega)}{f(z)} = 1.$$

Quindi, $f(z)$ è una funzione meromorfa ben definita sul toro complesso $\mathbb{C}/\Lambda$, cioè $f(z) \in M_\Lambda$. □

Abbiamo ora tutti gli strumenti per dimostrare il teorema di Abel Jacobi.

Dimostrazione. Consideriamo f da $Div_0(\mathbb{C}/\Lambda)$ a $\mathbb{C}/\Lambda$; fissiamo $u \in \mathbb{C}/\Lambda$.
Sia $D = (u) - (0)$, la condizione $deg(D) = 1 - 1 = 0$ assicura che D appartenga a $Div_0(\mathbb{C}/\Lambda)$. Poichè $f(D) = 1u - 0 = u$ allora f è suriettiva. Per il Primo Teorma di Isomorfismo, basta mostrate che $ker(f) = Div_p(\mathbb{C}/\Lambda)$.
Se D è principale allora la sua immagine è zero per il teormea **2.5**; questo mostra anche come F sia ben definita sul quoziente. Sia ora $D \in \ker(F)$: le ipotesi di grado zero ed appartenenza al nucleo ci consentono di applicare il Lemma **2.19** così da mostrare che di $D \in Div_p(\mathbb{C}/\Lambda)$. Questo è sufficiente per provare il teorema. □

2.4 *Equazione differenziale per la p-function di Weiestrass*

In questa sezione vogliamo trovare un'equazione differenziale del primo ordine che leghi $\wp^2$ e $\wp'$; l'equazione avrà una forma molto semplice perchè la parte in $\wp$ ha forma di polinomio di grado 3. Per fare questo ci servirà espandere in serie di Laurent ζ, $\wp'$ e $\wp'^2$. Iniziamo con l'espadere ζ. Ricordiamo la definizione di $\zeta(z, L)$:

$$\zeta(z,\Lambda) = \frac{1}{z} + \sum_{w\in\Lambda\setminus\{0\}} \left(\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2}\right)$$

Per le proprietà della serie geometrica abbiamo:

$$\frac{1}{z-w} = -\frac{1}{w}\sum_{n=0}^{\infty}\left(\frac{z}{w}\right)^n$$

Tale serie converge assolutamnete per $|z| < |w|$. Applicando questa espansione a ζ otteniamo:

$$\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} = -\frac{1}{w}\sum_{n=2}^{\infty}\left(\frac{z}{w}\right)^n.$$

Quindi:

$$\zeta(z,\Lambda) = \frac{1}{z} - \sum_{w\in\Lambda\setminus\{0\},\, n\geq 2} \frac{z^n}{w^{n+1}}$$

Possiamo notare che grazie alla simmetria del reticolo le potenze dispari di w, associate a potenza pari di z, si annullano a due a due:

$$\sum_{w\in\Lambda\setminus\{0\}} \frac{w^{-2k+1}}{z^{-2k}} = 0 \quad \text{per ogni } k\in\mathbb{N}, z\in\mathbb{C}\setminus\Lambda.$$

Possiamo allora scrivere ζ nella foorma contratta

$$\zeta(z,\Lambda) = \frac{1}{z} - \sum_{k\geq 2} G_k(\Lambda) z^{2k-1}$$

dove i coefficienti $G_k(L)$ sono definiti come:

$$G_k(L) = \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{w^{2k}}$$

Questi termini convergono tutti per il Lemma **2.10**. La relazione $\zeta'(z) = -\wp(z)$ e la convergenza assoluta dell'espanziose di ζ ci consentono di ottenere un'espressione analitica per $\wp$ e per $\wp'$ intorno all'origine differnziando l'espansione in serie di ζ:

$$\zeta(z,\Lambda) = \frac{1}{z} - \sum_{k\geq 2} G_k(\Lambda) z^{2k-1}$$

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{k\geq 2} (2k-1) G_k(\Lambda) z^{2k-2}$$

$$\wp'(z,\Lambda) = -\frac{2}{z^3} + \sum_{k\geq 2} (2k-1)(2k-2) G_k(\Lambda) z^{2k-3}$$

Per ricavare l'equazione differnziale sarà utile avere i primi termini dell'espansione scritti esplicitamente:

$$\wp(z,\Lambda) = \frac{1}{z^2} + 3G_2 z^2 + 5G_3 z^4 + \cdots$$

$$\wp'(z,\Lambda) = -\frac{2}{z^3} + 6G_2 z + 20G_3 z^3 + 42G_8^5 + O(z^7)$$

$$\wp'(z,\Lambda)^2 = \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_6 + (36G_4^2 - 168)z^2 + O(z^4)$$

$$\wp(z,\Lambda)^3 = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + O(z^4)$$

Si può notare la seguente realazione fondamentale:

$$\wp'(z,\Lambda)^2 - 4\wp(z,\Lambda)^3 + 60G_2\wp(z,\Lambda) + 140G_3 = O(z^2)$$

La funzione a sinistra è priva di poli e termini costanti, valutata in $z = 0$ restituisce 0 quindi per l'Osservazione **2.9** è costantemente 0. Possiamo così ricavare un'equazione per $\wp'$ che, snellendo la notazione, risulta essere:

$$\wp'(z, \Lambda)^2 = 4\wp(z, \Lambda)^3 - g_2(\Lambda)\wp(z, \Lambda) - g_3(\Lambda)$$

dove $g_2(\Lambda) = 60G_2(\Lambda)$ e $g_3(\Lambda) = 140G_3(\Lambda)$. Di seguito ometteremo la dipendanza dal reticolo.

2.5 *Isomorfismo analitico fra tori complessi e curve ellittiche*

Grazie ai risulati della sezione **2.4** possiamo affermare che i punti $(\wp(z), \wp'(z)) \in \mathbb{C}^2$ giacciano su una cubica di equazione:

$$y^2 = 4x^3 - g_2x^2 - g_3$$

Consideriamo $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ e chiamiamo $e_i = \wp(w_1/2)$ dove $i = 1, 2, 3$. Abbiamo già notato nell'Osservazione **2.12** come $\wp'(e_i) = 0$; questo induce la seguente fattorizzazione del polinomio:

$$\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

Esplicitando così le radici del polinomio in $\wp(z)$. Mostriamo infine che le radici di questo polinomio sono distinte. Per fare ciò consideriamo la funzione ellittica $\wp(z) - \wp(w_i/2)$: essa ha un polo doppio in 0, quindi avrà 2 zeri in z_1 e z_2 tali che $z_1 + z_2 \in \Lambda$. Chiaramente $z_1 = w_i/2$, ma essendo z_i un punto di 2-torsione $z_1 + z_2 = 0$ implica che $z_2 \equiv z_1 \bmod_\Lambda$. Dunque $\wp(z) = \wp(w_1/2)$ se e solo se $z \equiv w_i/2 \bmod_\Lambda$. Siamo pronti a dimostrare il seguente teorma fondamentale.

Teorema 2.20. *Sia $\mathbb{C}/\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ un toro complesso e $E(\mathbb{C})$ una curva ellittica di $\mathbb{P}^2(\mathbb{C})$ di equazione $ky^2 = 4k^3 - g_2k^2x - g_3k^3$, ed E la sua disomogenizzazione per la retta $k = 1$. La funzione*

$$h : \mathbb{C}/\Lambda \to E(\mathbb{C})$$

$$h : z \bmod_\Lambda \mapsto (1 : \wp(z) : \wp'(z)), z \notin \Lambda$$

$$h : z \in \Lambda \mapsto (0 : 0 : 1)$$

è un isomorfismo analitico di gruppi.

Dimostrazione. Chiaramente un elemento di $\mathbb{C}/\Lambda$ viene mappato nell'elemento nuetro di $E(\mathbb{C})$ se e solo se è lo zero del toro. La funzione h è analitica per ogni $z \neq 0$ perchè lo sono $\wp$ e $\wp'$. In $z = 0$ $\wp$ ha un polo doppio e $\wp'$ ha un polo triplo, ma possiamo considerare $h(z \bmod_\Lambda) = (z^3, z^3\wp(z), z^3\wp'(z))$ che converge in zero, si annulla nelle prime due coordinate e restituisce un valore finito nella terza, ovvero vale

$(0:0:1)$. Si può quindi prolungare analiticamente h in $z=0$, dunque è analitica ovunque.
Mostriamo che $h:\mathbb{C}/\Lambda\setminus 0\to E$ è biiettiva.
Consideriamo quindi $E: y^2=f(x)=4x^3-g_2x-g_3$. Per la suriettività bisogna mostrare che preso un punto $(x,y)\in E$ esiste $z\in\mathbb{C}/\Lambda$ tale che $h(z)=(x,y)$, ovvero $\wp(z)=x$ e $\wp'(z)=y$:
Sia $g(z)=\wp(z)-x$, per x fissato g è ellittica con un polo doppio in zero indotto da $\wp$. Affinchè la somma degli ordini dei punti singolari sia nulla, g deve per forza avere almeno uno zero a cosicchè $\wp(a)=x$. A questo punto dall'equazione di E è evidente che $y^2=f(x)=f(\wp(a))=\wp'(a)^2$ e quindi $y=\pm\wp'(z)$. Nel caso $y=-\wp'(z)$ si può considerare $-a$, che per parità di $\wp$ induce la stessa x e $\wp'(-a)=-\wp'(a)=y$ per disparità di $\wp'$.
Per l'iniettività supponiamo che esistano z_1 e z_2 numeri complessi tali che
$h(z_1)=(\wp(z_1),\wp'(z_1))=(\wp(z_2),\wp'(z_2))=h(z_2)$, mostriamo ora che $z_1\equiv_\Lambda z_2$.
Supponiamo che $2z_1$ non appartenga a Λ e consideriamo la funzione $g=\wp(z)-\wp(z_1)$; g avrà necessariamonnte 2 zeri, uno di cui uno sarà z_1, chiamiamo l'altro a. Per il teorma di Abel-Jacobi il divisore principale indotto da g ha la proprietà di sommare a zero le singolarità, coisicchè $z_1+a\in\Lambda$. Per l'ipotesi fatta a non è z_1, e sicuramnete $-z_1$ e z_2 sono zeri di g. Ma g non può avere 3 zeri, dunque 2 sono equivalenti mod_Λ. Per l'ipotesi iniziale $z_1-(-z_1)=2z_1$ non può appartenere al reticolo e dunque abbiamo $z_2\equiv_\Lambda z_1$ o $z_2\equiv_\Lambda -z_1$. Discutiamo il secondo caso: Se in due numeri hanno stassa immagine tramite h, hanno anche la stessa derivata, ovvero: $\wp'(z_1)=\wp'(z_2)=\wp'(-z_1)=-\wp'(z_1)=0$, ma z_1 annulla la derivata se e solo se $z_1=w_i/2$ che è un punto di torsione, e dunque $z_1=z_2$. Nel caso in cui $2z_1\in\Lambda$ lo zero di g è doppio e quindi $z_1\equiv_\Lambda z_2$. Questo mostra inoltre che $-h(z\bmod\Lambda)=h(-z\bmod\Lambda)$.
Rimane da mostrare che h, o equivalentemente h^{-1}, preserva la struttura di gruppo. Ricordiamo che nelle curve ellittiche $P_1+P_2=-P_1P_2$ dove P_1P_2 è l'intersezione fra la retta passante per P_1, P_2 ed E, esattemente come nell'osservazione **1.12**.
Consideriamo la retta $y=\lambda x+\nu$ e studiamone le intersezioni con la curva ellittica E. Nella parametrizzazione indotta da h i punti di intersezione della retta con E sono individuati dagli $z\in\mathbb{C}/\Lambda$ per cui vale la condizione $\wp'(z)=\lambda\wp(z)+\nu$; questo ci porta a considerare la funzione $s(z)=\wp'(z)-(\lambda\wp(z)+\nu)$ che è ellittica. Questa retta presenta un polo di ordine 3 in ogni punto del rticolo e che avrà 3 zeri z_1,z_2 e z_3 con la proprietà di sommare a zero. Dati 2 punti sulla curva e la loro somma, possiamo affermare che la loro antiimmagine secondo h ha la proprietà di sommare a zero. Siano P_1,P_2 punti di E, per l'Osservazione **1.15** vale $P_1+P_2=-P_1P_2$, chiamiamo $P_3=P_1P_2$. Siano $z_i=h^{-1}(P_i)$:
chiaramente $h^{-1}(P_1+P_2)=h^{-1}(-P_1P_2)=-h^{-1}(P_1P_2)=-h^{-1}(P_3)$ come osservato in precedenza. Affinchè valga la seconda uguaglianza dobbiamo assicurarci che la disparità di h valga anche per la sua inversa. Sia h una biiezione fra gruppi tale che $h(x)=-h(-x)$; supponiamo che esista y nell'immagine tale che $h^{-1}(y)\neq -h^{-1}(-y)$. Siccome h è ben definita la disuguaglianza deve rimanere vera

se applichiamo h da entrambe le parti. Otteniamo

$$h(h^{-1}(y)) = y \neq h(-h^{-1}(-y)) = -h(h^{-1}(-y)) = -(-y) = y$$

questo è assurdo quindi la prorpietà è verifiata.
Poichè P_3 è il terzo punto di intersezione fra la retta per P_1, P_2 ed E, vale la relazione: $0 = z_1 + z_2 + z_3 = h^{-1}(P_1) + h^{-1}(P_2) + h^{-1}(P_3)$ e dunque
$h^{-1}(P_1) + h^{-1}(P_2) = -h^{-1}(P_3)$. Questo basta per provare il teorema □

Teorema 2.21. *Per due reticoli equivalenti Λ e $\Lambda' = \lambda\Lambda$ $\lambda \neq 0$, valgono le seguenti relazioni:*

$$\wp(z, \Lambda) = \lambda^2 \wp(\lambda z, \lambda\Lambda), \quad \wp'(z, \Lambda) = \lambda^3 \wp'(\lambda z, \lambda\Lambda),$$
$$G_{2k}(\Lambda) = \lambda^{2k} G_{2k}(\lambda\Lambda), \quad g_2(\Lambda) = \lambda^4 g_2(\lambda\Lambda), \quad g_3(\Lambda) = \lambda^6 g_3(\lambda\Lambda).$$

Dimostrazione. Queste formule seguono facilmente dalle definizioni. Ad esempio, calcoliamo:

$$\wp'(\lambda z, \lambda\Lambda) = -2 \sum_{w \in \lambda\Lambda \setminus \{0\}} \frac{1}{(\lambda z - w)^3} = \lambda^{-3}(-2) \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{(z - w)^3} = \lambda^{-3} \wp'(z, \Lambda).$$

□

Ora possiamo precisare come l'isomorfismo h nel teorema **2.20** si relazioni agli isomorfismi tra tori complessi e le corrispondenti curve ellittiche. Il teorma successiovo afferma che 2 reticoli equivalenti sono mappati da h in 2 curve ellittiche legate da un cambio di coordinate ammissibile.

Teorema 2.22. *Per due reticoli equivalenti Λ e $\Lambda' = \lambda\Lambda$, abbiamo il seguente diagramma commutativo, dove h è definito nel teorema **2.20**:*

$$\begin{array}{ccc} \mathbb{C}/\lambda\Lambda & \xrightarrow{\lambda^{-1}} & \mathbb{C}/\Lambda \\ \downarrow h & & \downarrow h \\ E'(\mathbb{C}) & \xrightarrow{f} & E(\mathbb{C}) \end{array}$$

La curva E è definita da $y^2 = 4x^3 - g_2 x - g_3$, la curva E' da $y'^2 = 4x'^3 - g_2' x' - g_3'$, e l'isomorfismo f è dato dal cambiamento di variabili ammissibile con $u = \lambda$.

Dimostrazione. La relazione $\wp(\lambda^{-1} z, \Lambda) = \lambda^2 \wp(z, \lambda\Lambda)$ corrisponde a $x = \lambda^2 x'$ sotto f; la relazione $\wp'(\lambda^{-1} z, \Lambda) = \lambda^3 \wp'(z, \lambda\Lambda)$ corrisponde a $y = \lambda^3 y'$; la relazione $g_2(\Lambda) = \lambda^4 g_2(\lambda\Lambda)$ corrisponde a $g_2 = \lambda^4 g_2'$; e la relazione $g_3(\Lambda) = \lambda^6 g_3(\lambda\Lambda)$ corrisponde a $g_3 = \lambda^6 g_3'$. Questo conclude la dimostrazione. □

Capitolo 3

Funzioni ipergeometriche e calcolo dei periodi

In quest'ultimo capitolo proponiamo il problema inverso a quello del capitolo precedente: data una curva ellittica vogliamo calcolare i periodi del toro $\mathbb{C}/\Lambda$ a cui essa è isomorfa, ovvero trovare due valori complessi $\mathbb{R}-$linearmente indipendenti che generano il reticolo Λ. Per fare questo bisogna innanzitutto mostrare che ad ogni curva ellittica corrisponde uno ed un solo toro isomorfo; il passo successiovo sarà capire come calcolare i periodi del toro tramite la curva ellittica. Proseguendo vedremo che questi corrispondono a degli integrali molto particolari che abbiamo già visto nel primo capitolo; dovremo infine capire come (e dove) valutare questi integrali detti *ellittici*. Una volta ottenuta un'espressione reale per questi integrali, daremo una formula esplicita per il calcolo tramite le funzioni ipergeometriche.
Per non interrompere la trattazione dei periodi, introduciamo ad inizio capitolo le funzioni ipergeometriche in modo da trarne le informazioni utili al prosieguo della trattazione.

3.1 *Generalità sulla funzione* Γ *di Eulero*

Per parlare di funzioni ipergeomettriche, dobbiamo prima studiare le proprietà base della funzione Γ di Eulero e della generalizzazione del binomiale. Queste funzioni saranno indispensabili per calcolare una specifica classe di integrali.

Definizione 3.1. La funzione gamma $\Gamma(s)$ è definita per $\mathrm{Re}(s) > 0$ dal seguente integrale:

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx$$

Grazie al fattore esponenziale e^{-x}, l'integrale converge all'infinito per ogni s, e per $\mathrm{Re}(s) > 0$ il fattore x^{s-1} è integrabile vicino a 0.

Osservazione 3.2. Per $\mathrm{Re}(s) > 1$, inegrando per parti si può notare la natura ricorsiva della funzione:

$$\Gamma(s) = (s-1)\Gamma(s-1)$$

Poiché

$$\Gamma(1) = \int_0^\infty e^{-x}\,dx = 1,$$

questo, per induzione, mostra che per un numero naturale n si ha

$$\int_0^\infty x^{n-1}e^{-x}\,dx = (n-1)!.$$

Di conseguenza, la funzione $\Gamma(s)$ è una generalizzazione (o continuazione analitica) del fattoriale.

Cerchiamo ora di estendere la definizione dellla funzione analitica $\Gamma(s)$, definita per $\mathrm{Re}(s) > 0$, a tutto il piano complesso $\mathbb{C}$. Utilizzando la formula **3.2**, otteniamo la relazione

$$\Gamma(s) = \frac{\Gamma(s+n)}{s(s+1)(s+2)\cdots(s+n-1)},$$

valida per $\mathrm{Re}(s) > 0$. Il lato destro è una funzione meromorfa ben definita per $\mathrm{Re}(s) > -n$ e definisce una continuazione meromorfa di $\Gamma(s)$ al semipiano $\mathrm{Re}(s) > -n$ con poli negli interi negativi.

Questo procedimento è valido su tutti i semipiani $\mathrm{Re}(s) > -n$, e quindi su tutto $\mathbb{C}$. Vale la pena mostrare che la definizione estesa per s arbitrario è ben posta, ovvero che è indipendente dalla scelta di n. Sia $m \in \mathbb{N}$ tale che $\mathrm{Re}(s) > -m$ mostriamo che $\Gamma(s) = \frac{\Gamma(s+n)}{s(s+1)(s+2)\cdots(s+n-1)} = \frac{\Gamma(s+m)}{s(s+1)(s+2)\cdots(s+m-1)}$. Supponiamo $n > m$, allora:

$$\frac{\Gamma(s+m)}{s(s+1)(s+2)\cdots(s+m-1)} = \frac{\Gamma(s+m)(s+m)\dots(s+n-1)}{s(s+1)(s+2)\cdots(s+m-1)(s+m)\dots(s+n-1)}$$

Dai cui per la relazione $(s+m)\Gamma(s+m) = \Gamma(s+m+1)$ si ottiene $\Gamma(s+n)$ a numeratore. L'argomento è analogo per $m > n$. La definizione è ben posta.

Effettuiamo ora il seguente cambio di variabile; $x = t^2$, si ha $dx = 2t\,dt$. L'integrale che otteniamo ha una forma più agevole che usaremo nei conti successivi:

$$\Gamma(s) = 2\int_0^\infty t^{2s-1}e^{-t^2}\,dt.$$

Teorema 3.3. *Per $a, b > 0$, vale:*

$$2\int_0^{\frac{\pi}{2}} \cos^{2a-1}\theta \cdot \sin^{2b-1}\theta\,d\theta = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

Dimostrazione. Calcoliamo:

$$\Gamma(a)\Gamma(b) = 4\int_0^\infty\int_0^\infty \xi^{2a-1}\eta^{2b-1}\exp\left(-(\xi^2+\eta^2)\right)\,d\xi\,d\eta$$

Passando alle coordinate polari:

$$= 2\int_0^\infty r^{2a+2b-1}e^{-r^2}\,dr \cdot 2\int_0^{\frac{\pi}{2}} \cos^{2a-1}\theta \cdot \sin^{2b-1}\theta\,d\theta$$

Poiché:

$$\int_0^\infty r^{2(a+b)-1}e^{-r^2}\,dr = \frac{1}{2}\Gamma(a+b)$$

Segue:

$$\Gamma(a)\Gamma(b) = \Gamma(a+b)\cdot\int_0^{\frac{\pi}{2}} \cos^{2a-1}\theta\cdot\sin^{2b-1}\theta\,d\theta$$

Da cui:

$$2\int_0^{\frac{\pi}{2}} \cos^{2a-1}\theta\cdot\sin^{2b-1}\theta\,d\theta = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

Questo conclude la dimostrazione.

□

Un caso speciale del teorema **3.3** è quello con a e b ugauli ad $1/2$:

$$2\int_0^{\frac{\pi}{2}} d\theta = \frac{\Gamma(1/2)\Gamma(1/2)}{\Gamma(1)}$$

per cui $\Gamma(1/2) = \sqrt{\pi}$.
Esattamente come Γ è il prolungamento analitico del fattoriale, si può estendere al campo dei complessi anche il coefficiente binomiale tramite:

Definizione 3.4. Per ogni $s \in \mathbb{C}$ ed $n \in \mathbb{N}$ definiamo il coefficiente binomiale generalizzato come:

$$\binom{s}{n} = \frac{s(s-1)\cdots(s-n+1)}{n!}$$

La serie binomiale corrispondente è:

$$(1+x)^s = \sum_{n\geq 0}\binom{s}{n}x^n$$

che converge per $|x| < 1$ e $\mathrm{Re}(s) > 0$.

Teorema 3.5. *La relazione*

$$2\int_0^{\frac{\pi}{2}} \sin^{2m}\theta\,d\theta = \pi(-1)^m\binom{-\frac{1}{2}}{m}$$

vale per ogni numero naturale m.

Dimostrazione. Applichiamo il Teorema **3.3**, con $a = 1/2$ e $b = 1/2 + m$:

$$2\int_0^{\frac{\pi}{2}} \sin^{2m}\theta\,d\theta = \frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(m+\frac{1}{2}\right)}{\Gamma(m+1)} =$$

$$= \frac{\Gamma\left(\frac{1}{2}\right)\left(m-\frac{1}{2}\right)\left(m-\frac{3}{2}\right)\cdots\Gamma\left(\frac{1}{2}\right)}{m(m-1)\cdots 2\cdot 1} = \pi(-1)^m\binom{-\frac{1}{2}}{m}$$

Abbiamo applicato a $\Gamma(m+\frac{1}{2})$ l'integrazione per parti per m volte fino ad ottenere $(m+\frac{1}{2}-1)(m+\frac{1}{2}-2)\ldots(m-m++\frac{1}{2})\Gamma(m-m+\frac{1}{2})$. L'ultima uguaglianza segue dal fatto che $\Gamma(1/2) = \sqrt{\pi}$ e dalla definizione di binomiale.

□

3.2 *Funzioni ipergeometriche*

Introduciamo ora le funzioni ipergeometriche e vediamo la loro utilità nella risoluzione di una particolare classe di integrali trigonometrici.
Definiamo preliminarmente la segente notazione che utilizzeremo per il resto del capitolo: la successione $(k)_n$ è definita per ricorsione nel seguente modo:
$(k)_n = k(k+1)(k+2)\dots(k+n-1) = (k+n-1)(k)_{n-1}$ e $(k)_0 = 1$ per ogni $k \in \mathbb{C}$. Tali successioni hanno una rappresentazione molto agevole per i naturali, infatti: $(m)_n = m(m+1)\dots(m+n-1) = (m+n-1)!/(m-1)!$.

Definizione 3.6. La serie ipergeometrica associata ad $a, b \in \mathbb{C}$ e $c \in \mathbb{C} \setminus \mathbb{N}$ è data da

$$F(a,b,c,z) = \sum_{0 \le n} \frac{(a)_n (b)_n}{n!(c)_n} z^n.$$

Una semplice applicazione del criterio della radice mostra che la serie converge per ogni $|z| < 1$; la serie rappresenta dunque una funzione analitica sul disco unitario, chiamata *funzione ipergeometrica.*

Tali funzioni godono delle seguenti proprietà:

$$i) \quad F(a,b,c;z) = F(b,a,c;z) \tag{3.1}$$

$$ii) \quad F(a,b,b;z) = (1-z)^{-a} \tag{3.2}$$

$$iii) \quad F(a,a,1;z) = \sum_{n \ge 0} \binom{-a}{n}^2 z^n \tag{3.3}$$

Usiamo le relazioni:

$$(1)_n = n! \quad \text{e} \quad \frac{(a)_n}{n!} = (-1)^n \binom{-a}{n}$$

La seconda segue da:

$$\frac{(a)_n}{n!} = \frac{a(a+1)\dots(a+n-1)}{n!} = \frac{(-1)^n(-a)(-a-1)\dots(-a-n+1)}{n!}$$

Abbiamo moltiblicato per -1 tutti gli n fattori a numeratore, $(-1)^n$ serve per far tornare il segno corretto. Da qui si applica la definizione di binomiale. Queste relazioni servono per verificare ii) e iii).
Per *ii)* abbiamo $(a,b,b;z) = \sum_{0 \le n} \frac{(a)_n (b)_n}{n!(b)_n} z^n = \sum_{0 \le n} \frac{(a)_n}{n!} z^n = \sum_{0 \le n} (-1)^n \binom{-a}{n} z^n = \sum_{0 \le n} \binom{-a}{n} (-z)^n = (1-z)^{-a}$, per definizione di serie binomiale.
Per *iii)* otteniamo: $F(a,a,1;z) = \sum_{0 \le n} \frac{(a)_n (a)_n}{n!n!} z^n$ da cui segue la formula usando la seconda relazione, Utilizzeremo la iii) nel caso $a = \frac{1}{2}$:

$$F\left(\frac{1}{2}, \frac{1}{2}, 1; z\right) = \sum_{n \ge 0} \binom{-\frac{1}{2}}{n}^2 z^n$$

Con il seguente teorema introduciamo gli *integrali ellittici* che torneranno utili a fine capitolo.

Teorema 3.7. *Per un numero complesso λ con $|\lambda| < 1$, si ha:*

$$2\int_0^{\frac{\pi}{2}} \left(1 - \lambda \sin^2\theta\right)^{-1/2} d\theta = \pi F\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right).$$

Dimostrazione. Usando lo sviluppo in serie binomiale come in **3.4** per $x = -\lambda \sin^2\theta$ e $s = 1/2$, abbiamo:

$$\left(1 - \lambda \sin^2\theta\right)^{-1/2} = \sum_{n\geq 0} \binom{-\frac{1}{2}}{n} (-\lambda)^n \sin^{2n}\theta.$$

Per **3.5** e integrando da entrambe le parti, otteniamo:

$$2\int_0^{\frac{\pi}{2}} \left(1 - \lambda \sin^2\theta\right)^{-1/2} d\theta = \sum_{n\geq 0} \binom{-\frac{1}{2}}{n} (-1)^n \lambda^n \cdot \pi (-1)^n \binom{-\frac{1}{2}}{n}$$

$$= \pi \sum_{n\geq 0} \binom{-\frac{1}{2}}{n}^2 \lambda^n = \pi F\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right).$$

Questo dimostra il teorema. □

Lasciamo ora da parte le funzioni ipergeometriche e torniamo a parlare di curve ellittiche.

3.3 *Uniformizzazione*

Vogliamo raffinare il teorema **2.20** affinchè ogni curva ellittica abbia un toro associato; per fare questo abbiamo bisogno del teorema di uniformizzazione.

Teorema 3.8. *Siano $A, B \in \mathbb{C}$ tali che $4A^3 + 27B^2 \neq 0$, allora esiste un unico reticolo complesso Λ tale che $g_2(\Lambda) = A$ e $g_2(\Lambda) = B$.*

Dimostrazione. Per una dimostrazione rimandiamo a [**6**]. □

Il prossimo risultato va a raffinare il teorema **2.20** assicurando che ad ogni curva ellittica corrisponde uno ed un solo toro isomorfo.

Teorema 3.9. *Sia $E(\mathbb{C})$ una curva ellittica. Esiste un reticolo $\Lambda \subset \mathbb{C}$, unico a meno di equivalenza di reticoli, analiticamente isomorfo ed E tramite la mappa:*

$$h : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \quad h(z) = \left(1, \wp(z, \Lambda), \wp'(z, \Lambda)\right),$$

Dimostrazione. Ricordando l'Osservaazione **1.10**, la condizione di discriminante non nullo permette di applicare il teorema di uniformizzazione al polinomio definiente della curva ellittica. Il teorema teorema **2.20** assicura che esista uno toro isomorfo a questa curva; il teorma di uniformizzazione ne assicura l'unicità. Il teorema **2.22** permette di estendere il risultato alle classi di equivalenza di curve e tori. □

Con questo teorema possiamo dare senso alla definizone di periodi in **1.23**: sapendo che ogni curva ellittica è analiticamente isomorfa (in particolare è omeomorfa) ad un toro complesso possiamo dunque affermare che il gruppo fondamentale di una curva ellittica, e quindi il suo primo gruppo di omologia, è $\mathbb{Z} \times \mathbb{Z}$. Questo implica che esistono α e β non omotopi su $E(\mathbb{C})$ e che due cammini di questo tipo generano $H_1(\mathbb{C})$.
Col prossimo teorema capiremo come sono effettivamente legati i cencetti di perioido sul toro e sulle curve curve ellittiche.

Teorema 3.10. *Sia $E(\mathbb{C})$ una curva ellittica con funzioni di coordinate di Weierstrass x e y; siano α e β cammini chiusi su $E(\mathbb{C})$ che forniscono una base per $H_1(E, \mathbb{Z})$. Allora i periodi*

$$w_1 = \int_\alpha \frac{dx}{y} \quad e \quad w_2 = \int_\beta \frac{dx}{y}$$

sono linearmente indipendenti su $\mathbb{R}$ e definiscono $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$ tale che $\mathbb{C}/\Lambda$ è analiticamente isomorfo ad E.

Dimostrazione. Il teorema **3.9** assicura l'esisenza di Λ_1 analiticamente isomorfo ad E tramite h.

Per l'osservazione **1.23** possiamo lavorare con il primo gruppo fondamentale invece che col primo gruppo di omologia del toro. Siccome α e β (intesi come mappe continue) sono cammini indipendenti, anche $h^{-1} \circ \alpha$ e $h^{-1} \circ \beta$ saranno indipendenti e dunque base per $\pi_1(\mathbb{C}/\Lambda)$. L'isomorfismo h ci permette di effettuare il cambio di variabile $x = \wp(z)$, $y = \wp'(z)$, $dx = \wp'(z)dz$ nel seguente integrale:

$$\int_\alpha \frac{dx}{y} = w = \int_{h^{-1}\circ\alpha} dz = w_1$$

Il valore w_1 è un generatore di Λ_1 poichè eiste un isomorfismo naturale di gruppi fra $\pi_1(\mathbb{C}/\Lambda_1)$ e Λ_1 dato da $\gamma \mapsto \int_\gamma dz$, che mappa basi di $\mathbb{C}/\Lambda_1$ in punti base di Λ_1. Così $\Lambda_1 = w_1\mathbb{Z} + w_2\mathbb{Z}$. Questo conclude la dimostrazione. □

3.4 *Calcolo dei periodi*

In quest'ultima sezione ci occupermo di calcolare i periodi di una curva ellittica, ovvero di individuare esplicitamente il toro a cui è analiticamente isomorfa.
Nel paragrafo precedente abbiamo capito che l'integrali da calcolare sono:

$$w_1 = \int_\alpha \frac{dx}{y} \quad \text{e} \quad w_2 = \int_\beta \frac{dx}{y}$$

L'uguaglianza rimane vera anche dividendo entrambi i membri per 2: otteniamo degli altri w_i che individuano il reticolo $\frac{1}{2}\Lambda$ equivalente a quello di partenza. Studieremo allora (senza rinominare w_i):

$$w_1 = \int_\alpha \frac{dx}{2y} \quad \text{e} \quad w_2 = \int_\beta \frac{dx}{2y}$$

Osservazione 3.11. Vale la pena notare che le definizioni di periodi di tori e periodi di curve ellittiche individuano, in ultima analisi, lo stesso oggetto. Con la sezione precedente abbiamo dunque mostrato che ad ogni toro di periodi w_1, w_2 esiste un'unica curva ellittica (a meno di isomorfismi) con gli stessi periodi e viceversa.

Ci rimane solo da esplicitare la forma dei cammini sui quali ha senso integrare. Partiamo da una considerazione generale sull'integrale che segue dalla struttura delle curve ellittiche. L'invariant differential ω è una forma differenziale olomorfa nelle coordinate x e y; localmente possiamo esprimere y in funzionne della coordinata x, cossicchè avremo $y = y(x)$. Consideriamo la valutazione dell'integrale nella coordinata locale x tramite la proiezione $p : E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ definita da:

$$(1, x, y) \mapsto x, (1, 0, 0) \mapsto \infty$$

Sotto la proiezione α e β diventeranno due cammini L_1 ed L_2 tali che $L_1 = p \circ \alpha$ e $L_2 = p \circ \beta$. Possiamo dunque considerare gli integrali su $\mathbb{C} \cup \{\infty\}$

$$w_1 = \int_\alpha \frac{dx}{2y} = \int_{L_1} \frac{dx}{y(x)} \quad \text{e} \quad w_2 = \int_\beta \frac{dx}{2y} = \int_{L_2} \frac{dx}{2y(x)}$$

Consideriamo ora $\mathbb{C}/\Lambda$ il toro complesso analiticamente isomorfo ad $E(\mathbb{C})$ con $\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z}$. Sia h come in **2.20** l'ismorfismo analitico fra $\mathbb{C}/\Lambda$ e $E(\mathbb{C})$. Un cammino fondamentale del toro è un percorso che possiamo supporre partire da zero e finire in w_1; di conseguenza l'altro cammino fondamentale sarà il cammino da zero a w_2. Nel quoziente questi corrispondono alle due circonfernze fondamentali del toro. Per continuità di h le immagini $h \circ w_1$ e $h \circ w_2$ sono cammini non omotopi su $E(\mathbb{C})$. L'unica richiesta fatta su α e β è che non siano omotopi: possiamo dunque supporre che $\alpha = h \circ w_1$ e che $\beta = h \circ w_2$. La funzione h parametrizza la curva ellittica, in particolare la prima coordinata sarà $x = \wp(z)$. La funzione $\wp$ è meromorfa e analitica con un unico polo in zero, è dunque la proiezione della coordionata locale x su $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, estendendo $\wp(0) = \infty$. Studiamo allora $L_1 = \wp(z)$ e $L_2 = \wp(z)$, per gli z appartenenti ai cammini fondamentali del toro. Possiamo considerare w_1 e w_2 come due lati del parallelogramma fondamentale associato a Λ con vertice in 0: il punto iniziale e il punto finale dei cammini saranno il punto all'infinito di $\mathbb{P}^1(\mathbb{C})$. Il primo cammino passa per $w_1/2$: quindi possiamo immaginare che parta da ∞, scenda fino a $\wp(w_1)/2$ e torni a chiudersi all'infinito. Siamo inoltre capaci di esplicitare il valore del punto attorno al quale L_1 gira poichè la condizione $y = \wp'(z)$ in questo punto asicura che $0 = \wp'(w_1/2) = y$: di conseguenza $y = y(x) = y(\wp(z)) = 0$. Segue che $\wp(w_1/2)$ è uno zero del polinomio definiente di E. Gli zeri di $f(x)$ sono inoltre distinti, come già osservato all'inzio della sezione **2.5**.
Senza perdere di generalità, essendo E una curva ellittica costruita sul campo complesso, possiamo assumere che $y(x)$ sia in forma di *Legendre*, ovvero $y(x) = x(x - \lambda)(x - 1)$; facciamo coincidere $w_1/2$ con 0 e $w_2/2$ con 1 e di conseguenza $(w_1 + w_2)/2$ sarà uguale a λ. Rimangono da esplicitare gli estremi di integrazione di L_1 ed L_2, cammini che, a meno dei circuiti attorno alle singolarià, sono omootopicamente equivalenti a cammini sull'asse reale. Vogliamo innanzitutto notare che i due integrali

valutati in un circuito chiuso attorno ad una loro singolarità danno contributo nullo. Questo è vero perchè intorno a 0 ed 1 gli integrali si comportano come una una funzione olomorfa moltiplicata per $\frac{1}{\sqrt{x}}$ o $\frac{1}{\sqrt{x-1}}$. Attorno ad infinito la funzione si comporterà come $\frac{1}{\sqrt{x}}$. Si può ottenere il valore dell'integrale sul circuito tramite il teorema dei residui notatndo che i residui nella singolarità sono nulli. L'unico contributo effettivo del girare attorno alle singolarità è dato dal fatto che, se il cammino compie un giro completo attorno ad una singolarità, la radice cambia argomento di π, ovvero cambia di segno. Dopo avere effettuato questo giro, si torna ad infinito sull'asse reale ripercorrendo il cammino da cui si era arrivati ma in verso contrario e segno opposto; possiamo allora trattare l'integrale come 2 volte un integrale su un cammino reale. Per w_1 il cammino parte da $-\infty$ ed arriverà a 0. L'altro cammino, simlmente, parte da infinito, gira intorno ad 1 e si chiude ad infinito. I due cammini si possono intersecare solo nel punto all'infinito e duque il secondo partirà da 1, arriverà a $+\infty$ e verrà percorso due volte. Sostituendo ora $y(x) = \sqrt{(x(x-1)(x-\lambda)}$ otteniamo

$$w_1(\lambda) = \int_{-\infty}^{0} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$$
$$w_2(\lambda) = \int_{1}^{\infty} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$$

L'ultimo accorgimento da prendere è sulla scelta di λ.
Per le considerazioni fatte nella sezione **1.4** sappiamo che alla classe di equivalenza di ogni curva ellittica complessa sono associate 6 possibili scelte di λ, ovvero:

$$\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}$$

Questo ci assicura che sia sempre possibile effetture una scelta di λ tale per cui $|\lambda| < 1$ e $|\lambda - 1| < 1$.
Vale la pena notare che nella trattazione sopra abbiamo ignorato un problema importante, ovvero che la funzione radice quadrata non è valutata singolarmente nel campo complesso. Questo può dare problemi quando si integra intorno alle singolarità. Per tale motivo, e per evitare ambiguità nel calcolo, lo spazio in cui studiare questo integrale è un doppio rivestimento di $\mathbb{C} \cup \{\infty\}$ ramificato in quattro punti, ovvero le preimmagini di 0,1,λ e ∞. Tale rivestimento è una superficie di Riemann. Per una trattazione più completa di questo tipo di integrali si rimanda a **[3]**.
Siamo ora pronti a trattare il teorema che esplicita i periodi di un toro analiticamennte isomorfo ad una curva ellittica tramite le funzioni ipergeometriche.

Teorema 3.12. *Sia $\lambda \in \mathbb{C}$ tale che $|\lambda| < 1$ e $|\lambda - 1| < 1$. I periodi associati hanno la seguente forma in termini della funzione ipergeometrica:*

$$w_1(\lambda) = i\pi F\left(\tfrac{1}{2}, \tfrac{1}{2}, 1; 1-\lambda\right), \quad w_2(\lambda) = \pi F\left(\tfrac{1}{2}, \tfrac{1}{2}, 1; \lambda\right).$$

*Per il reticolo $\Lambda_\lambda = \mathbb{Z}w_1(\lambda) + \mathbb{Z}w_2(\lambda)$ i tori complessi $\mathbb{C}/\Lambda_\lambda$ ed $E_\lambda(\mathbb{C})$ sono isomorfi tramite una mappa costruita come combinazione affine della funzione di Weierstrass $\wp$ e della sua derivata come nel teorma **2.20**.*

Dimostrazione. La seconda affermazione segue dalla sezione precedente. Resta da calcolare l'espressione integrale dei periodi. Tornerà utlile nell'ultimo passaggio del primo calcolo il teorema **3.5**.
Per $w_2(\lambda)$, si cambia variabile: $x = \frac{1}{t},\ t = s^2,\ s = \sin\theta$. Si ha:

$$w_2(\lambda) = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = \int_0^1 \frac{dt}{\sqrt{t(1-t)(1-\lambda t)}} = 2\int_0^1 \frac{ds}{\sqrt{(1-s^2)(1-\lambda s^2)}} =$$

$$= \int_0^{\pi/2} \frac{d\theta}{\sqrt{1-\lambda\sin^2\theta}} = \pi F\left(\tfrac{1}{2}, \tfrac{1}{2}, 1; \lambda\right).$$

Per $w_1(\lambda)$, ci si riconduce al caso precedente tramite il cambio variabile: $y = -x+1$, cioè $x = 1-y$. Si ottiene:

$$w_1(\lambda) = \int_{-\infty}^1 \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = \int_1^\infty \frac{dy}{\sqrt{y(y-1)(y-(1-\lambda))}} = i\pi F\left(\tfrac{1}{2}, \tfrac{1}{2}, 1; 1-\lambda\right).$$

Questo conclude la dimostrazione. □

Bibliografia

[1] Dale Husemöller *Elliptic Curves*, Springer, 2004.

[2] Joseph H. Silverman *The Arithmetic of Elliptic Curves*, Springer, 1986.

[3] Anthony W. Knapp *Elliptic Curves*, Princeton University Press, 1992.

[4] Giuseppe De Marco *Analisi Due, secondo corso di analisi matematica*, Zanichelli, 1999.

[5] Edoardo Sernesi *Geometria 2*, Bollati Boringhieri, 2019

[6] Goro Shimura *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971