Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

Confronto tra un approccio analitico e un approccio aritmetico alle curve ellittiche

Tesi di Laurea in Geometria Algebrica

Relatore:
FATIGHENTI ENRICO

Presentata da:
PALLOTTA ALBA

Anno Accademico 2024-2025

Introduzione

Le curve ellittiche hanno suscitato interesse nella matematica per le loro proprietà straordinarie e le numerose applicazioni in diversi ambiti. Storicamente, il loro nome deriva dal legame con gli integrali ellittici, introdotti per calcolare la lunghezza dell'arco di un'ellisse: al di là di questa origine etimologica, non hanno una relazione diretta con le ellissi.

Le curve ellittiche sono un oggetto che può essere studiato in branche distinte della matematica: esse vengono trattate in geometria algebrica, in analisi complessa, in teoria dei numeri e trovano persino applicazione in crittografia.

È proprio da questa loro trasversalità che nasce l'idea della tesi, che confronta due prospettive fondamentali nello studio delle curve ellittiche: quella analitica e quella aritmetica.

La tesi è articolata in tre capitoli, di cui di seguito riassumiamo brevemente i contenuti.

Il primo capitolo adotta il punto di vista dell'analisi complessa, con l'obiettivo di fornire gli strumenti necessari per comprendere il capitolo successivo, includendo anche alcuni approfondimenti utili al contesto.

In particolare, tratteremo nel dettaglio le funzioni ellittiche, introducendo i reticoli del piano complesso, dai quali emergerà naturalmente il concetto di isogenia. Concluderemo poi con lo studio della funzione più significativa di questo quadro analitico: la $\wp$ di Weierstrass.

Nel secondo capitolo, verrà per la prima volta fornita una definizione formale di curva ellittica, seguendo il linguaggio della geometria algebrica. Verrà poi illustrata la più importante interpretazione geometrica delle curve ellittiche: esse sono equivalenti ai tori complessi. Non solo, tale corrispondenza è resa possibile proprio grazie alla $\wp$ di Weierstrass, introdotta nel capitolo analitico.

Questo è un risultato estremamente rilevante, poiché rende le curve ellittiche particolarmente versatili: in base alla branca della matematica in cui vengono studiate, possono essere interpretate in modi differenti, a seconda dell'aspetto della loro struttura che si vuole evidenziare.

Il terzo capitolo adotta un approccio aritmetico allo studio delle curve ellittiche (o, equivalentemente, dei tori complessi), con l'obiettivo di descriverne la struttura modulare.

Il risultato più significativo in questo contesto è il teorema di modularità, che può essere formulato in diverse versioni per via della sua evoluzione storica lunga e articolata.

L'idea alla base del teorema venne proposta come congettura negli anni '50 da Taniyama e fu successivamente riformulata in forma più precisa da Shimura. Qualche anno dopo, Weil fornì un fondamento teorico più solido e per questo il teorema venne chiamato a lungo congettura Taniyama-Shimura-Weil. Negli anni '90 Wiles dimostrò che l'enunciato era valido per una particolare classe di curve ellittiche, il che ebbe una conseguenza fondamentale: permise a Wiles, insieme a Taylor, di dimostrare l'ultimo teorema di Fermat. Anni dopo, Breuil, Diamond, Conrad e Taylor, sfruttando i risultati di Wiles, completarono una dimostrazione generale del teorema di modularità.

Introdurremo dunque, in quest'ultimo capitolo, le forme modulari, i sottogruppi di congruenza e le curve modulari, con l'intento di fornire tutti gli strumenti necessari a comprendere l'effettiva potenza del teorema di modularità, che verrà enunciato solamente in forma complessa, senza esibirne una dimostrazione.

Tale scelta è motivata dal fatto che una trattazione dettagliata richiederebbe di lavorare sul campo dei razionali $\mathbb{Q}$, anziché sul campo dei complessi $\mathbb{C}$, spostando l'attenzione dal tema principale di questa tesi, ossia offrire una panoramica che mostri come le curve ellittiche costituiscano un argomento profondamente trasversale in matematica.

Indice

1 Strumenti di analisi complessa **7**
- 1.1 Funzioni ellittiche . . . 7
  - 1.1.1 Teoremi di Liouville sulle funzioni ellittiche . . . 9
  - 1.1.2 Funzioni ellittiche come funzioni sul toro complesso . . . 15
- 1.2 Reticoli: struttura algebrica e interpretazione geometrica . . . 17
  - 1.2.1 Reticoli visti come sottogruppi discreti . . . 18
  - 1.2.2 Dai reticoli ai tori complessi . . . 20
- 1.3 Isogenie e loro strumenti fondamentali . . . 25
  - 1.3.1 Definizioni e proprietà delle isogenie . . . 26
  - 1.3.2 Il gruppo di torsione e l'accoppiamento di Weil . . . 33
  - 1.3.3 Introduzione alla moltiplicazione complessa . . . 33
- 1.4 $\wp$ di Weierstrass . . . 35
  - 1.4.1 Costruzione $\wp$ di Weierstrass . . . 35
  - 1.4.2 Proprietà $\wp$ di Weierstrass . . . 37
  - 1.4.3 Equazione differenziale algebrica di $\wp$ . . . 43

2 Curve ellittiche e tori complessi **49**
- 2.1 Verso la definizione di curva ellittica . . . 49
  - 2.1.1 Nozioni preliminari . . . 50
  - 2.1.2 Definizione e riduzione a una forma standard . . . 51
- 2.2 Corrispondenza tra tori complessi e curve ellittiche . . . 53
  - 2.2.1 Costruzione della biezione . . . 53
  - 2.2.2 La funzione discriminante . . . 54
  - 2.2.3 Passaggio tra toro e curva ellittica . . . 56

3 Strutture modulari delle curve ellittiche **61**
- 3.1 Forme modulari . . . 62
  - 3.1.1 Funzioni debolmente modulari . . . 62
  - 3.1.2 Verso la definizione di forme modulari . . . 64
  - 3.1.3 Esempi e osservazioni . . . 65
- 3.2 Sottogruppi di congruenza . . . 67

3.2.1 Definizioni e osservazioni fondamentali 68
3.2.2 Forme modulari rispetto a sottogruppi di congruenza 71
3.3 Curve ellittiche potenziate e curve modulari 73
3.3.1 Definizioni e considerazioni iniziali 74
3.3.2 Corrispondenza tra curve modulari e spazi di parametri di curve ellittiche potenziate 76
3.3.3 Teorema di modularità - versione complessa 79

Bibliografia **81**

Capitolo 1

Strumenti di analisi complessa

In questo capitolo verranno fornite alcune nozioni di base di analisi complessa, che saranno utili a comprendere i capitoli successivi.

Inizieremo introducendo le *funzioni ellittiche* e studiandone le loro proprietà fondamentali, come ad esempio i teoremi di Liouville.

Nella seconda sezione ci soffermeremo sui *reticoli*: ne studieremo la struttura algebrica e ne daremo un'interpretazione geometrica mostrando come questi diano origine ai tori complessi. Seguirà in maniera naturale la necessità di trattare di *isogenie*, alle quali dedicheremo la terza sezione.

Infine, l'ultima sezione sarà dedicata alla funzione $\wp$ di Weierstrass: ne illustreremo la costruzione passo passo e approfondiremo le sue principali proprietà, che vedremo saranno necessarie, nel capitolo successivo, per studiare le curve ellittiche dal punto di vista dell'analisi complessa.

Seguiremo principalmente gli approcci di [BF09] e [DS05], ma faremo anche riferimento ad alcune nozioni presenti in [Mir95] e in [SS10].

1.1 Funzioni ellittiche

In questa sezione, definiremo i reticoli nel piano complesso, le funzioni ellittiche e altri strumenti fondamentali per il loro studio. Ci concentreremo innanzi tutto sui teoremi di Liouville sulle funzioni ellittiche, risultati essenziali per approfondirne le proprietà. In

seguito, vedremo come queste possano essere interpretate come funzioni definite sul toro complesso.

Per rendere più chiara la lettura delle sezioni successive, introduciamo alcune notazioni e definizioni di base di analisi complessa e teoria dei gruppi.

Cominciamo con quelle relative all'analisi complessa.

Notazione 1.1.1. Indichiamo con $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ lo spazio proiettivo complesso di dimensione 1, con tale corrispondenza data da

$$\begin{aligned} \mathbb{C} \cup \{\infty\} &\longrightarrow \mathbb{P}^1(\mathbb{C}) \\ x \in \mathbb{C} &\longmapsto [x : 1] \\ \infty &\longmapsto [1 : 0] \end{aligned}$$

dove con $[x : 1]$ indichiamo le usuali coordinate omogenee.

Definizione 1.1.1. Sia $U \subseteq \mathbb{C}$ un insieme aperto. Una funzione

$$f \colon U \longrightarrow \mathbb{P}^1(\mathbb{C})$$

si dice *meromorfa* se soddisfa le seguenti proprietà:

- la controimmagine del punto all'infinito $A = f^{-1}(\infty)$ è discreta;
- la restrizione
$$f|_{U \setminus A} \colon U \setminus A \longrightarrow \mathbb{C}$$
è analitica;
- i punti di A sono poli di f.

Notazione 1.1.2. Sia $U \subseteq \mathbb{C}$ un aperto e sia $f \colon U \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione meromorfa. Indichiamo con $\mathcal{P}(f)$ l'insieme dei poli di f.

Definizione 1.1.2. Sia $f \colon U \subseteq \mathbb{C} \longrightarrow \mathbb{C}$. Lo *sviluppo in serie di Laurent* di f è una rappresentazione in serie che include termini positivi e negativi. Dunque, nel caso in cui f sia olomorfa, coincide con lo sviluppo in serie di Taylor.

Passiamo ora ad una definizione preliminare della teoria dei gruppi, che ci sarà utile in seguito.

Definizione 1.1.3. Un gruppo abeliano G si dice *finitamente generato* se esistono $g_1, ..., g_r \in G$ tali che ogni elemento $g \in G$ si scrive

$$g = a_1 g_1 + ... + a_r g_r$$

per certi $a_1, ..., a_r \in \mathbb{Z}$ o, equivalentemente, se esiste

$$p : \mathbb{Z}^r \longrightarrow G$$

omomorfismo di gruppi suriettivo.

In particolare, G si dice *libero di rango* r se tale scrittura è unica o, equivalentemente, se p è un isomorfismo.

1.1.1 Teoremi di Liouville sulle funzioni ellittiche

In questa sottosezione introdurremo le definizioni di base relative alle funzioni ellittiche ed enunceremo i tre teoremi di Liouville su queste funzioni.

Definizione 1.1.4. Siano $\omega_1, \omega_2 \in \mathbb{C}$ due vettori $\mathbb{R}$-linearmente indipendenti, cioè non nulli e tali che il loro quoziente è reale. Chiamiamo *reticolo* il gruppo abeliano da essi generato, ossia:

$$L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\} \subset \mathbb{C} \, .$$

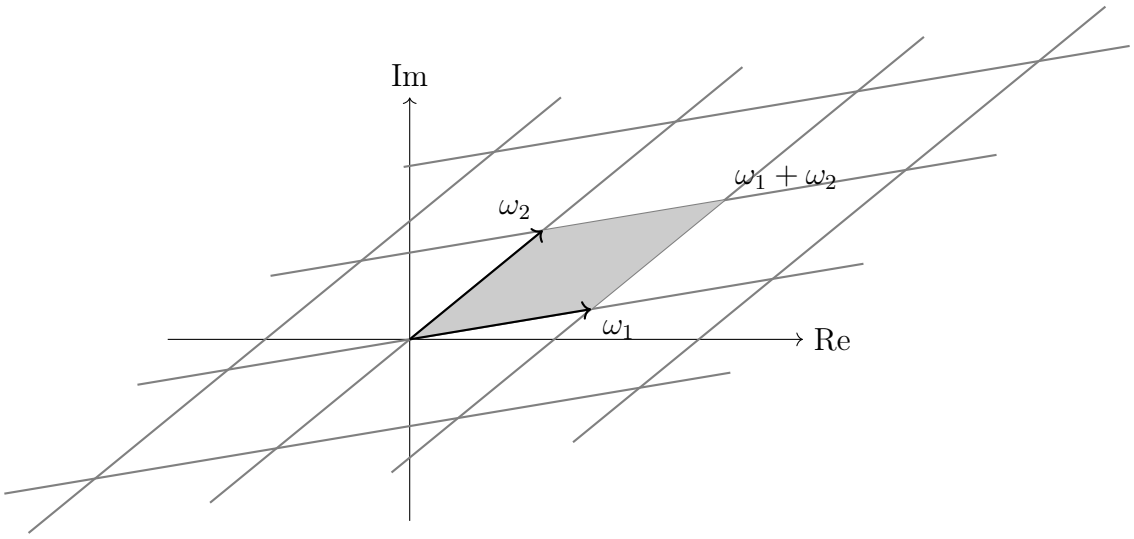


Figura 1: Reticolo generato da ω_1 e ω_2

Definizione 1.1.5. Una *funzione ellittica* associata al reticolo L è una funzione meromorfa

$$f\colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$$

invariante per traslazioni nel reticolo, cioè tale che per ogni $z \in \mathbb{C}$

$$f(z) = f(z+w)$$

per ogni $\omega \in L$.

È sufficiente richiedere la periodicità solo rispetto ai due generatori ω_1 e ω_2 di L, ossia:

$$\forall z \in \mathbb{C} \quad f(z+\omega_1) = f(z+\omega_2) = f(z)\ ;$$

per cui le funzioni ellittiche sono dette anche *doppiamente periodiche*.

Osservazione 1.1.1. Consideriamo $f\colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione ellittica associata a un reticolo L. Allora:

$$\mathcal{P}(f) + L = \mathcal{P}(f)\ .$$

Dimostrazione (dell'Osservazione 1.1.1). Preso $p \in \mathcal{P}(f)$, si ha che:

$$|f(z)| \xrightarrow{z\to p} \infty \Rightarrow \text{ per } w \in L \quad |f(z+w)| = |f(z)| \xrightarrow[z+w\to p+w]{z\to p} \infty \Rightarrow p+w \in \mathcal{P}(f)\ .$$

□

Lemma 1.1.2 (Teorema di Liouville classico)**.** *Sia f una funzione intera, ovvero $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ olomorfa. Se f è limitata, allora è costante.*

Dimostrazione. Poiché f è limitata, applicando la disuguaglianza di Cauchy sui dischi di raggio arbitrario si ottiene che f' è identicamente nulla. Da questo segue che f è costante. □

Teorema 1.1.3 (Primo teorema di Liouville sulle funzioni ellittiche)**.** *Una funzione ellittica senza poli è costante.*

Dimostrazione. Mostriamo che una qualsiasi funzione che verifica le ipotesi è limitata. Consideriamo l'insieme:

$$\mathcal{F} = \{t_1\omega_1 + t_2\omega_2 : 0 \le t_1, t_2 \le 1\}\ ,$$

detto *parallelogramma fondamentale* associato alla base $\{\omega_1, \omega_2\}$ di un reticolo L.

Per ogni punto $z \in \mathbb{C}$ esiste un punto del reticolo $w \in L$ tale che $z - w \in L$; grazie alla periodicità delle funzioni ellittiche, è quindi sufficiente studiare la funzione su $\mathcal{F}$. Tale parallelogramma è chiuso e limitato in $\mathbb{C}$, quindi qualsiasi funzione continua definita su $\mathcal{F}$ è limitata. Una funzione ellittica senza poli è olomorfa su tutto il dominio di definizione e dunque, per quanto osservato, sarà limitata su $\mathcal{F}$ e di conseguenza, per l'arbitrarietà di $\mathcal{F}$, anche su tutto $\mathbb{C}$. Per il Lemma 1.1.2, una tale funzione è necessariamente costante. □

Dall'Osservazione 1.1.1 si ricavano le osservazioni seguenti:

Osservazione 1.1.4. Sia $U \subseteq \mathbb{C}$ e sia $f : U \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione meromorfa. Allora si ha che:

$$z \in \mathcal{P}(f) \Rightarrow [z]_L \subseteq \mathcal{P}(f) \ .$$

Osservazione 1.1.5. Per ogni $z \in \mathbb{C}$

$$Res(f, z) = Res(f, z + w)$$

per ogni $w \in L$. Si può quindi definire il residuo rispetto alla classe di equivalenza $[z]_L$ come:

$$Res(f, [z]_L) := Res(f, z)$$

senza ambiguità.

Teorema 1.1.6 (Secondo teorema di Liouville sulle funzioni ellittiche)**.** *Una funzione ellittica* $f \colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$ *ha un numero finito di poli modulo* L *e vale:*

$$\sum_z Res(f, z) = 0 \ .$$

Dimostrazione. Per mostrare che il numero di poli modulo L è finito, è sufficiente considerare i rappresentanti all'interno di un parallelogramma fondamentale $\mathcal{F}$. L'insieme dei poli $\mathcal{P}(f)$ è discreto e, poiché $\mathcal{F}$ è compatto, la loro intersezione $\mathcal{P}(f) \cap \mathcal{F}$ è necessariamente finita.

Calcoliamo la somma dei residui integrando lungo il bordo di una regione delimitata da un parallelogramma fondamentale, opportunamente traslato in modo da evitare la possibile presenza di poli nella frontiera di tale parallelogramma. Consideriamo dunque:

$$\mathcal{F}_a = a + \mathcal{F} = \{a + z : z \in \mathcal{F}\}$$

il parallelogramma ottenuto traslando $\mathcal{F}$ di un certo $a \in \mathbb{C}$, scelto opportunamente. Questo parallelogramma, così come $\mathcal{F}$, è tale che: ogni orbita ha almeno un rappresentante in $\mathcal{F}_a$, quando due punti in $\mathcal{F}_a$ sono equivalenti allora sono necessariamente punti di

frontiera e due punti interni a $\mathcal{F}_a$ non possono essere in relazione tra loro.

Integrando f lungo $\partial\mathcal{F}_a$ otteniamo:

$$\int_{\partial\mathcal{F}_a} f = 2\pi i \sum_{z\in\mathcal{F}_a} Res(f,z) \quad .$$

Per costruzione, non ci sono poli in $\partial\mathcal{F}_a$ quindi la somma è effettuata su un insieme di rappresentanti modulo L.

Per concludere ci basta dunque mostrare che l'integrale è nullo. Questo segue immediatamente dal fatto che gli integrali sui lati opposti del parallelogramma $\mathcal{F}_a$ si eliminano perché il valore assunto da f, poiché periodica, è lo stesso e i lati sono orientati in maniera opposta. □

Definizione 1.1.6. Sia $U \subseteq \mathbb{C}$ un aperto e sia $f : U \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione meromorfa con un polo $a \in U$. Per un noto risultato di analisi complessa, sappiamo che esiste un numero naturale n e una funzione olomorfa h tali che possiamo scrivere

$$f(z) = (z-a)^{-n} \cdot h(z) \ .$$

Chiamiamo *ordine di f in a* tale intero

$$n = ord(f,a) \ .$$

Proposizione 1.1.7. *Sia $f\colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione ellittica associata a un reticolo L e sia $\mathcal{F}$ un parallelogramma fondamentale tale che f non ha né zeri né poli in $\partial\mathcal{F}$. Allora il numero degli zeri di f in $\mathcal{F}$, contati con molteplicità, è uguale al numero di poli di f in $\mathcal{F}$, contati con molteplicità, e vale:*

$$\sum_{p\in\mathcal{F}} ord_p(f)\cdot p \equiv 0 \pmod{L} \ .$$

Dimostrazione. Per il principio dell'argomento, la differenza tra il numero di zeri e il numero di poli di f in $\mathcal{F}$, contati con molteplicità, è data da:

$$\frac{1}{2\pi i}\int_{\partial\mathcal{F}} \frac{f'(z)}{f(z)}dz \quad .$$

Osserviamo che $\frac{f'}{f}$ è L-periodica, dunque

$$\int_{\partial\mathcal{F}} \frac{f'(z)}{f(z)}dz = 0$$

da cui segue il primo punto dell'enunciato.

Osserviamo poi che

$$\int_{\partial\mathcal{F}} z\frac{f'(z)}{f(z)}dz = \omega_1 \int_0^{\omega_2} \frac{f'(z)}{f(z)}dz - \omega_2 \int_0^{\omega_1} \frac{f'(z)}{f(z)}dz \ , \tag{1.1}$$

dove ω_1 e ω_2 sono i vettori che generano $\mathcal{F}$. Per $i = 1, 2$ si ha che esistono $k_i \in \mathbb{Z}$ tali che

$$\int_0^{\omega_i} \frac{f'(z)}{f(z)}dz = 2\pi i k_i \ . \tag{1.2}$$

Inoltre, per il teorema dei residui, si ha che

$$\frac{1}{2\pi i}\int_{\partial\mathcal{F}} z\frac{f'(z)}{f(z)}dz = \sum_{p\in\mathcal{F}} ord_p(f)\cdot p \ . \tag{1.3}$$

Combinando l'eq. (1.1). l'eq. (1.2) e l'eq. (1.3), otteniamo

$$\sum_{p\in\mathcal{F}} ord_p(f)\cdot p = \omega_1 k_2 - \omega_2 k_1 \in L \ .$$

□

Da ora in avanti considereremo una funzione ellittica associata a un reticolo L, come una funzione il cui dominio è il toro $\mathbb{C}/L$. Il motivo per cui questa assunzione è lecita verrà chiarito nella prossima sottosezione.

Definizione 1.1.7. L'*ordine dei poli* di una funzione ellittica f è il numero di tutti i suoi poli sul toro $\mathbb{C}/L$, contati con la loro molteplicità:

$$Ord(f) = -\sum_a ord(f, a) \ \ ,$$

dove a è un polo di f preso in un sistema di rappresentanti modulo L.
Per convenzione si assume $Ord(f) = 0$ se $\mathcal{P}(f) = \varnothing$.

Osservazione 1.1.8. Dal Teorema 1.1.3, si deduce che:

$$\mathrm{Ord}(f) = 0 \iff f \text{ è costante.}$$

Osservazione 1.1.9. Dal Teorema 1.1.6 si deduce che non esistono funzioni ellittiche di ordine 1.

Dimostrazione (dell'Osservazione 1.1.9). L'insieme dei poli modulo L non può ridursi a un solo elemento perché un polo semplice ha sempre residuo diverso da 0 per definizione. □

Discorsi analoghi valgono anche per gli zeri di una funzione ellittica.

Definizione 1.1.8. Per $b \in \mathbb{C}$ chiamiamo:

- *punti di livello b di f* = zeri di $f(z) - b$;
- *insieme dei punti di livello b di f* = insieme degli zeri di $f(z) - b$;
- *ordine dell'insieme dei punti di livello b di f* = ordine di zero di $f(z) - b$ = numero dei punti di livello b di f in $\mathbb{C}/L$ contati con la molteplicità (in notazione b-Ord_f).

Osserviamo che ∞-$Ord_f = \mathrm{Ord}(f)$.

Teorema 1.1.10 (Terzo teorema di Liouville sulle funzioni ellittiche)**.** *Una funzione ellittica non costante f assume su $\mathbb{C}/L$ ogni valore lo stesso numero di volte contate con molteplicità, ovvero:*

$$\mathrm{Ord}(f) = b\text{-}\mathrm{Ord}_f \quad \textit{per ogni} \quad b \in \mathbb{P}^1(\mathbb{C}) \, .$$

Dimostrazione. Se $b = \infty$, la tesi segue direttamente.

Sia dunque $b \in \mathbb{C}$. Chiamiamo

$$g(z) = f(z) - b \quad \text{e} \quad h(z) = \frac{f'(z)}{g(z)}.$$

Poiché f è ellittica, lo è anche f' . Infatti, per $z \in \mathbb{C}$ e $l \in L$ si ha

$$f'(z+l) = \lim_{t \to 0} \frac{f(z+l+t) - f(z+l)}{t} = \lim_{t \to 0} \frac{f(z+t) - f(z)}{t} = f'(z) \, .$$

Segue che anche h è ellittica e quindi possiamo applicare il secondo teorema di Liouville.

Per $a \in \mathbb{C}$ si ha che:

$$a \text{ è un polo per } f \iff \begin{cases} a \text{ è un polo per } g \quad (\text{o equivalentemente per } f) \\ \text{oppure} \\ a \text{ è uno zero per } g \end{cases}$$

Inoltre:

$$Res(h,a) = ord(g,a) \begin{cases} < 0 \text{ se } a \text{ è un polo per } g \text{ (o equivalentemente per } f) \\ > 0 \text{ se } a \text{ è uno zero per } g \end{cases}$$

Otteniamo quindi:

$$0 = \sum_a Res(h, a) = \sum_{a \in Z(g)} ord(g, a) + \sum_{a \in \mathcal{P}(f)} ord(g, a) = b\text{-Ord}_f - Ord(f)$$

e dunque $Ord(f) = b\text{-Ord}(f)$. □

1.1.2 Funzioni ellittiche come funzioni sul toro complesso

In questa sottosezione descriveremo come le funzioni ellittiche possano essere interpretate come funzioni definite sul toro complesso.

Ai fini del nostro discorso, e per quelli che affronteremo nei capitoli successivi, è utile richiamare un lemma sulle superfici di Riemann. Prima di enunciarlo, forniamo una definizione.

Definizione 1.1.9. Diciamo che uno spazio topologico X è una *superficie di Riemann* se è connesso, di Hausdorff, a base numerabile ed è dotato di una classe di equivalenza di atlanti. Per una definizione formale di *atlante complesso* si rinvia a [Mir95].

Lemma 1.1.11. *Siano S_1 e S_2 superfici di Riemann e sia $f\colon S_1 \longrightarrow S_2$ una mappa olomorfa. Se S_1 è compatta, allora f è suriettiva.*

Dimostrazione. Per il Teorema della mappa aperta, l'immagine $f(S_1)$ è aperta in S_2. Poiché f è continua e S_1 è compatta, $f(S_1)$ è compatta. Le superfici di Riemann sono spazi di Hausdorff quindi $f(S_1)$ è anche chiusa, poiché compatta in uno spazio di Hausdorff. Essendo S_2 connessa, necessariamente sarà $f(S_1) = S_2$. □

Poiché per definizione una funzione ellittica f è periodica rispetto a un certo reticolo L, risulta naturale considerare la relazione di equivalenza:

$$z \equiv w \pmod{L} \iff z - w \in L\ .$$

Osserviamo inoltre che la somma in $\mathbb{C}$ induce la somma in $\mathbb{C}/L$

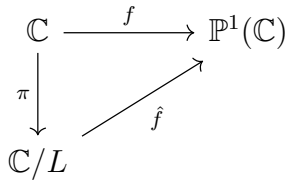
$$[z]_L + [w]_L := [z + w]_L\ ,$$

operazione che non dipende dai rappresentanti e che quindi conferisce a $\mathbb{C}/L$ una struttura di gruppo abeliano.

Per la proprietà fondamentale del quoziente di spazi topologici, data una funzione ellittica $f\colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$ associata al reticolo L, esiste un'unica funzione continua

$$\hat{f}\colon \mathbb{C}/L \longrightarrow \mathbb{P}^1(\mathbb{C})$$

tale che il diagramma



commuta.

Una qualsiasi funzione ellittica $f\colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$, associata al reticolo L, può quindi essere considerata come una funzione sul toro $\mathbb{C}/L$. Per semplicità di notazione, indicheremo ancora tale funzione con f invece che con $\hat{f}$; ma prima di proseguire, sfruttiamo questo discorso per dimostrare il seguente lemma, che risulterà utile più avanti nella trattazione.

Lemma 1.1.12 (Lemma di Picard per funzioni ellittiche)**.** *Una funzione ellittica*

$$f \,:\, \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$$

non costante associata al reticolo L assume ogni valore (complesso e ∞) di $\mathbb{P}^1(\mathbb{C})$.

Dimostrazione. Per il discorso precedente, f passa al quoziente con

$$\hat{f} \,:\, \mathbb{C}/L \longrightarrow \mathbb{P}^1(\mathbb{C}) \,,$$

funzione meromorfa con poli in $\pi(\mathcal{P}(f))$. Si può dunque interpretare come mappa olomorfa su tutto il toro $\mathbb{C}/L$, se pensiamo ai poli come punti che vengono mandati all'infinito.

Poiché f è non costante, lo sarà anche $\hat{f}$; quindi, per il Lemma 1.1.11, $\hat{f}$ è suriettiva. Segue che anche $f = \hat{f} \circ \pi$ è suriettiva in quanto composizione di funzioni suriettive. □

Definizione 1.1.10. Sia $U \subseteq \mathbb{C}$ un aperto e sia $f\colon U \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione meromorfa. Un punto $a \in U$ si dice *punto di ramificazione per f* se la molteplicità di f in a (intesa come il numero di fogli sopra $f(a)$) è maggiore di 1.
Un punto $b \in \mathbb{P}^1(\mathbb{C})$ si dice *punto di biforcazione per f* se è immagine di almeno un punto di ramificazione.

Indichiamo con $R(f) \subseteq \mathbb{C}/L$ l'insieme dei punti di ramificazione e con $B(f) = f(R(f)) \subseteq \mathbb{P}^1(\mathbb{C})$ l'insieme dei punti di biforcazione.

Osservazione 1.1.13. Sia $f\colon \mathbb{C}/L \longrightarrow \mathbb{P}^1(\mathbb{C})$ ellittica non costante con $Ord(f) = N$.

L'insieme $R(f)$ è finito perché discreto in un compatto e l'insieme $B(f)$ è finito in quanto immagine di un insieme finito. Per $z \in \mathbb{P}^1(\mathbb{C})$, si ha:

$$\#f^{-1}(z) = \begin{cases} < N \text{ se } z \in B(f) \\ = N \text{ altrimenti} \end{cases} .$$

Osservazione 1.1.14. Sia $f\colon \mathbb{C}/L \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione ellittica non costante e sia $b \in \mathbb{C}$.
Allora $b \in B(f)$ se e solo se esiste $a \in \mathbb{C}$ tale che

$$f(a) = b, \quad f'(a) = 0 ;$$

inoltre $\infty \in B(f)$ per f non identicamente nulla se e solo se $0 \in B\left(\frac{1}{f}\right)$.

1.2 Reticoli: struttura algebrica e interpretazione geometrica

In questa sezione approfondiremo lo studio dei reticoli.

Inizieremo fornendo una definizione più generalizzata di reticolo, che ci permetta di estendere il discorso anche al contesto di $\mathbb{R}^n$, senza limitarci necessariamente nel piano bidimensionale $\mathbb{R}^2 \simeq \mathbb{C}$. Successivamente, ci concentreremo sulla relazione che c'è tra reticoli e tori complessi, già accennata nella sezione precedente.

Prima di tutto introduciamo una definizione e una notazione di base, che utilizzeremo frequentemente nelle sezioni successive.

Definizione 1.2.1. Chiamiamo *gruppo modulare* il gruppo delle matrici a coefficienti in $\mathbb{Z}$ con determinante 1, cioè:

$$SL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid det(A) = 1\} .$$

Notazione 1.2.1. Dato un numero complesso $z \in \mathbb{C}$, indichiamo la sua parte reale con $\Re(z)$ e la sua parte immaginaria con $\Im(z)$. Inoltre denotiamo:

$$\mathcal{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\} \subset \mathbb{C} .$$

1.2.1 Reticoli visti come sottogruppi discreti

Un reticolo può essere descritto come un sottogruppo discreto di $\mathbb{R}^n$. Osservato in questo modo, possiamo comprenderne meglio le proprietà.

Definizione 1.2.2. Diciamo che $L \subseteq \mathbb{R}^n$ è un *reticolo di grado n* se esistono n vettori $\mathbb{R}$-linearmente indipendenti $\omega_1, ..., \omega_n$ tali che

$$L = \omega_1\mathbb{Z} + ...\omega_n\mathbb{Z} \, .$$

Proposizione 1.2.1. *Sia $L \subseteq \mathbb{R}^n$ un sottogruppo additivo. Se L è discreto, allora esistono $k \leq n$ vettori $\mathbb{R}$-linearmente indipendenti $\omega_1, ..., \omega_k$ tali che*

$$L = \omega_1\mathbb{Z} + ... + \omega_k\mathbb{Z} \, .$$

In particolare L è un reticolo di rango n nel caso in cui $k = n$.

Per una dimostrazione di questa proposizione si rinvia a [Neu13].

Si consideri dunque $L \subseteq \mathbb{R}^n$ un sottogruppo additivo discreto.
Dalla Proposizione 1.2.1 deduciamo che esiste $k \in \mathbb{N}$, $k \leq n$ tale che $L \simeq \mathbb{Z}^k$ è libero di rango k .

Caso particolare: per $n = 2$ ci sono 3 possibili ranghi da cui

$$\text{3 possibili sottogruppi di } \mathbb{R}^2\text{: } \begin{cases} L = \{0\} \text{ , se } k = 0 \text{ ;} \\ L = w_1\mathbb{Z} \text{ gruppo ciclico, se } k = 1 \text{ ;} \\ L = w_1\mathbb{Z} + w_2\mathbb{Z} \text{ reticolo, se } k = 2 \text{ .} \end{cases}$$

Applichiamo ora questo discorso al nostro contesto.

Osservazione 1.2.2. Sia $f \colon \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$ una funzione meromorfa non costante. Allora l'insieme dei suoi periodi

$$L_f = \{w \in \mathbb{C} : f(z) = f(z + w) \quad \forall z \in \mathbb{C}\}$$

è un sottogruppo discreto di $\mathbb{C}$.

Per dimostrare questa osservazione, abbiamo bisogno di enunciare il principio di identità, noto risultato in analisi complessa.

Lemma 1.2.3 (Principio di identità)**.** *Se due funzioni olomorfe coincidono su un insieme con un punto di accumulazione all'interno di un dominio connesso, allora coincidono ovunque su quel dominio.*

Per una dimostrazione del Lemma 1.2.3 si veda [Mod04].

Dimostrazione (dell'Osservazione 1.2.2). Supponiamo per assurdo che L_f non sia discreto e che quindi esista un punto di accumulazione $w_0 \in L_f$. Allora esiste una successione $\{w_n\} \in L_f$, con $w_n \xrightarrow[n\to+\infty]{} w_0$.
Chiamiamo

$$g_n(z) = f(z + w_n) = f(z) \quad \forall n \in \mathbb{N} \quad \text{e} \quad g(z) = f(z + w_0) \, .$$

Fissato $z \in \mathbb{C}$, poiché $w_n \xrightarrow[n\to+\infty]{} w_0$, si ha:

$$g_n(z) = f(z + w_n) \xrightarrow[n\to+\infty]{} f(z + w_0) = g(z) \, .$$

Ma quindi, dato che $\forall n \in \mathbb{N} \quad g_n(z) \equiv f(z)$ converge puntualmente a $g(z)$, si ha che:

$$f(z) = g(z) = f(z + w_0)$$

e quindi f coincide con la sua traslata su un insieme che contiene il punto di accumulazione w_0. Dal principio di identità segue che f deve essere necessariamente costante. □

Si hanno quindi tre possibilità per L_f :

- $L_f = \{0\} \to$ non ci sono periodi non banali per f ;
- L_f è ciclico $\to f$ è semplicemente periodica ;
- L_f è un reticolo $\to f$ è doppiamente periodica (ellittica) .

Abbiamo dunque mostrato che i reticoli, visti come sottogruppi discreti di $\mathbb{C}$ descrivono la periodicità delle funzioni meromorfe. Come già detto, quozientando il piano complesso per un reticolo, questa struttura si traduce nella geometria dei tori.

1.2.2 Dai reticoli ai tori complessi

Vediamo ora una serie di risultati sui reticoli in relazione con i tori complessi. In particolare, in questa sottosezione mostreremo come due reticoli possano determinare tori isomorfi tra loro, come i generatori siano legati da trasformazioni del gruppo modulare $SL_2(\mathbb{Z})$ e come i reticoli determinino l'esistenza e la forma delle funzioni olomorfe tra tori complessi.

Lemma 1.2.4. *Dati due reticoli*

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}\ , \quad \Lambda' = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z} \quad con\ \frac{\omega_1}{\omega_2},\ \frac{\omega_1'}{\omega_2'} \in \mathcal{H}\ ,$$

si ha che $\Lambda = \Lambda'$ *se e solo se esiste una matrice* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *tale che*

$$\begin{pmatrix} w_1' \\ w_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\ .$$

Dimostrazione.
$\boxed{\Longrightarrow}$ Poiché $\Lambda' \subseteq \Lambda$, si ha che esistono $a, b, c, d \in \mathbb{Z}$ tali che

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2\ , \end{aligned} \tag{1.4}$$

cioè esiste una matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ tale che

$$\begin{pmatrix} w_1' \\ w_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\ .$$

Poiché vale anche $\Lambda \subseteq \Lambda'$, tale matrice è invertibile, cioè $A \in GL_2(\mathbb{Z})$ e quindi $detA = \pm 1$.

Dimostriamo che $detA > 0$. Scriviamo un numero complesso $v \in \mathbb{C}$ arbitrario come vettore

$$v = \begin{pmatrix} \Re(v) \\ \Im(v) \end{pmatrix} \in \mathbb{R}^2$$

e analogamente un vettore complesso $(v, w) \in \mathbb{C}^2$ come una matrice

$$M(v, w) = \begin{pmatrix} \Re(v) & \Re(w) \\ \Im(v) & \Im(w) \end{pmatrix} \in M_2(\mathbb{R})\ .$$

Osserviamo che $det(M(\omega_1, \omega_2)) = \Im(\omega_1 \cdot \overline{\omega_2})$.

Poiché

$$\frac{\omega_1}{\omega_2} = \frac{\omega_1 \cdot \overline{\omega_2}}{|\omega_2|^2} \ ,$$

si ha che

$$det(M(\omega_1, \omega_2)) = |\omega_2|^2 \cdot \Im\left(\frac{\omega_1}{\omega_2}\right) > 0$$

e analogamente si avrà

$$det(M(\omega_1', \omega_2')) = \Im(\omega_1' \cdot \overline{\omega_2'}) > 0 \ .$$

Dalle eq. (1.4) si evince che

$$M(\omega_1', \omega_2') = M(\omega_1, \omega_2) \cdot A^T \ ,$$

quindi, passando ai determinanti, si ottiene che

$$det(M(\omega_1', \omega_2')) = det(M(\omega_1, \omega_2)) \cdot det(A^T) \ .$$

Dunque $det(A) = det(A^T) > 0$ e quindi $det(A) = 1$.

$\boxed{\Longleftarrow}$ Per ipotesi, esiste una matrice $A \in SL_2(\mathbb{Z})$ tale che

$$\begin{pmatrix} w_1' \\ w_2' \end{pmatrix} = A \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \ .$$

Quindi

$$\omega_1' = a\omega_1 + b\omega_2 \in \Lambda$$
$$\omega_2' = c\omega_1 + d\omega_2 \in \Lambda \ ,$$

e dunque $\Lambda' \subseteq \Lambda$.
Essendo A invertibile, vale:

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A^{-1} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \ ,$$

quindi $\Lambda \subseteq \Lambda'$.

□

Definizione 1.2.3. Chiamiamo *trasformazione di Möbius* una funzione meromorfa definita da

$$\begin{aligned} f \ : \ \mathbb{P}^1(\mathbb{C}) &\longrightarrow \mathbb{P}^1(\mathbb{C}) \\ z &\longmapsto \frac{az+b}{cz+d} \end{aligned}$$

dove $a, b, c, d \in \mathbb{C}$ sono tali che $ad - bc \neq 0$.

Osservazione 1.2.5. Gli elementi di $SL_2(\mathbb{Z})$ possono essere visti come particolari trasformazioni di Möbius.

Osservazione 1.2.6 (Azione di $SL_2(\mathbb{Z})$ su $\mathcal{H}$)**.** Due reticoli sono uguali se e solo se i rapporti dei generatori sono legati da una qualche trasformazione di Möbius in $SL_2(\mathbb{Z})$.

Dimostrazione. Consideriamo due reticoli come sopra

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \ , \quad \Lambda' = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$$

e chiamiamo

$$\tau := \frac{\omega_1}{\omega_2} \ , \quad \tau' := \frac{\omega_1'}{\omega_2'} \ .$$

Il Lemma 1.2.4 afferma che $\Lambda = \Lambda'$ se e solo se esistono $a, b, c, d \in \mathbb{Z}$, con $ad - bc = 1$, tali che

$$\begin{aligned} \omega_1' =& a\omega_1 + b\omega_2 \\ \omega_2' =& c\omega_1 + d\omega_2 \ . \end{aligned}$$

Ma quindi si ha che

$$\tau' = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d} \ ,$$

cioè $\tau' = f(\tau)$ per una qualche f trasformazione di Möbius in $SL_2(\mathbb{Z})$.

In altre parole, due punti $\tau, \tau' \in \mathcal{H}$ definiscono lo stesso reticolo se e solo se sono nella stessa orbita dell'azione di $SL_2(\mathbb{Z})$ su $\mathcal{H}$. □

Nei capitoli successivi vedremo che il quoziente del piano $\mathcal{H}$ per l'azione del gruppo modulare può essere identificato con un sottoinsieme di $\mathbb{C}$ che denoteremo *dominio fondamentale.*

Proposizione 1.2.7. *Sia $\phi\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ una funzione olomorfa tra tori complessi. Allora esistono $m, b \in \mathbb{C}$ con $m\Lambda \subseteq \Lambda'$ tali che $\phi([z]_\Lambda) = [mz + b]_{\Lambda'}$.*
In particolare ϕ è invertibile se e solo se $m\Lambda = \Lambda'$.

Dimostrazione. Consideriamo le proiezioni al quoziente

$$\pi\colon \mathbb{C} \longrightarrow \mathbb{C}/\Lambda, \quad \pi'\colon \ \mathbb{C} \longrightarrow \mathbb{C}/\Lambda'$$

e la composizione

$$g = \phi \circ \pi\colon \mathbb{C} \longrightarrow \mathbb{C}/\Lambda' \ .$$

Questa verifica le ipotesi della proprietà di sollevamento delle mappe (perché $\mathbb{C}/\Lambda'$ è connesso per archi e localmente connesso per archi e $\mathbb{C}$ è semplicemente connesso), quindi

esiste $\overline{\phi}\colon \mathbb{C} \longrightarrow \mathbb{C}$ sollevamento continuo di ϕ, cioè tale che $\pi' \circ \overline{\phi} = g$. Abbiamo quindi che il seguente diagramma:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\overline{\phi}} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \mathbb{C}/\Lambda & \xrightarrow[\phi]{} & \mathbb{C}/\Lambda' \end{array}$$

commuta.

Consideriamo ora, per $\lambda \in \Lambda$, la funzione

$$f_\lambda(z) = \overline{\phi}(z+\lambda) - \overline{\phi}(z)$$

e osserviamo che ha valori solo in Λ'. Infatti: preso $z \in \mathbb{C}$, si ha che:

$$[\overline{\phi}(z+\lambda)]_{\Lambda'} = \pi'(\overline{\phi}(z+\lambda)) = \phi(\pi(z+\lambda)) = \phi([z]_\Lambda) = \phi(\pi(z)) = \pi'(\overline{\phi}(z)) = [\overline{\phi}(z)]_{\Lambda'} \ ,$$

quindi $f_\lambda(z) \in \Lambda'$. Da questo deduciamo che $f_\lambda\colon \mathbb{C} \longrightarrow \Lambda'$ è costante, poiché funzione continua da un connesso a un discreto.
Derivando, otteniamo che per ogni $z \in \mathbb{C}$ si ha che

$$\overline{\phi}'(z+\lambda) = \overline{\phi}'(z)$$

che significa che $\overline{\phi'}$ è Λ-periodica. Dunque, per il teorema 2.1.1, $\overline{\phi}'$ è costante e di conseguenza $\overline{\phi}$ è un polinomio di primo grado $\overline{\phi}(z) = mz + b$.

Si osservi poi che $m\Lambda \subseteq \Lambda'$, cioè che per $\lambda \in \Lambda$ si ha che $m\lambda \in \Lambda'$. Infatti:

$$[mz+b]_{\Lambda'} = [\overline{\phi}'(z)]_{\Lambda'} = \phi([z]_\Lambda) = \phi([z+\lambda]_{\Lambda'}) = [\overline{\phi}'(z+\lambda)]_{\Lambda'} = [mz+m\lambda+b]_{\Lambda'} \ ,$$

quindi:

$$[m\lambda]_{\Lambda'} = [0]_{\Lambda'} \ .$$

Mostriamo ora che se tale contenimento è proprio, allora ϕ non può essere iniettiva: sia dunque $m\Lambda \subsetneq \Lambda'$.
Allora esiste $z \in \Lambda'$ tale che $\frac{z}{m} \notin \Lambda$ e quindi:

$$\phi\left(\left[\frac{z}{m}\right]_\Lambda\right) = \left[\overline{\phi}\left(\frac{z}{m}\right)\right]_{\Lambda'} = [z+b]_{\Lambda'} \overset{z\in\Lambda'}{=} [b]_{\Lambda'} = [\overline{\phi}(0)]_{\Lambda'} = \phi([0]_\Lambda) \ .$$

Se invece $m\Lambda = \Lambda'$, abbiamo che la funzione

$$\psi : \begin{array}{c} \mathbb{C}/\Lambda' \longrightarrow \mathbb{C}/\Lambda \\ [w]_{\Lambda'} \mapsto \left[\frac{w-b}{m}\right]_\Lambda \end{array}$$

inverte ϕ .

□

Corollario 1.2.8. *Sia $\phi\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ una funzione olomorfa tra tori complessi e siano m e b come sopra, cioè tali che $\phi([z]_\Lambda) = [mz+b]_{\Lambda'}$ e $m\Lambda \subseteq \Lambda'$. Allora sono equivalenti:*

1. *ϕ è un omomorfismo di gruppi;*
2. *$b \in \Lambda'$ e quindi $\phi([z]_\Lambda) = [mz]_{\Lambda'}$;*
3. *$\phi([0]_\lambda) = [0]_{\Lambda'}$.*

In particolare:

- *esiste un omomorfismo di gruppi olomorfo tra tori complessi se e solo se esiste $m \in \mathbb{C}^*$ tale che $m\Lambda \subseteq \Lambda'$;*
- *esiste un isomorfismo di gruppi olomorfo tra tori complessi se e solo se esiste $m \in \mathbb{C}$ tale che $m\Lambda = \Lambda'$.*

Dimostrazione.

$\boxed{1 \Rightarrow 3}$ Segue dalla definizione di omomorfismo.

$\boxed{3 \Rightarrow 2}$ Poiché

$$\phi([0]_\Lambda) = [0+b]_{\Lambda'} ,$$

allora $\phi([0]_\lambda) = [0]_{\Lambda'}$ se e solo se $b \in \Lambda'$.

$\boxed{2 \Rightarrow 1}$ Siano $[z_1]_\Lambda, [z_2]_\Lambda \in \mathbb{C}/\Lambda$. Allora

$$\phi([z_1+z_2]_\Lambda) = [m(z_1+z_2)+b]_{\Lambda'} = [mz_1+b]_{\Lambda'} + [mz_2+b]_{\Lambda'} = \phi([z_1]_\Lambda) + \phi([z_2]_\Lambda) .$$

Quindi ϕ è un omomorfismo di gruppi.

Vediamo ora la seconda parte dell'enunciato. Per quanto riguarda il primo punto, se esiste una funzione olomorfa tra tori complessi (non necessariamente lineare), dalla Proposizione 1.2.7 segue che esiste $m \in \mathbb{C}^*$ tale che $m\Lambda \subseteq \Lambda'$; viceversa, se tale m esiste, si può costruire un omomorfismo olomorfo definendo $\phi([z]_\Lambda) = [mz]_{\Lambda'}$. Il secondo punto segue direttamente.

□

Osservazione 1.2.9. Ogni toro complesso è isomorfo a un quoziente $\mathbb{C}/\Lambda_\tau$ dove $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ per un qualche $\tau \in \mathcal{H}$. Tale τ non è unico.

Dimostrazione. Sia $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ un reticolo arbitrario con $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Il Corollario 1.2.8 mostra che la mappa

$$\begin{array}{rccc} \phi_\tau & : & \mathbb{C}/\Lambda & \longrightarrow \mathbb{C}/\Lambda_\tau \\ & & [z]_\Lambda & \longmapsto \left[\frac{z}{\omega_2}\right]_{\Lambda_\tau} \end{array} ,$$

dove $\tau := \frac{\omega_1}{\omega_2} \in \mathcal{H}$, è un isomorfismo.

Mostriamo che la scelta di τ non è unica. Sia dunque τ' tale che $\mathbb{C}/\Lambda_{\tau'} \cong \mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_\tau$. Allora, dalla Proposizione 1.2.7, si deduce che $\tau' = \frac{\omega_1'}{\omega_2'}$ dove ω_1' e ω_2' sono tali che

$$\Lambda = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z} \ .$$

Per il Lemma 1.2.4, si ha che esiste f trasformazione di Möbius in $SL_2(\mathbb{Z})$ tale che $\tau = f(\tau')$.

□

Osservazione 1.2.10. Sebbene la rappresentazione di un toro complesso sotto forma di $\mathbb{C}/\Lambda_\tau$ non sia unica, possiamo comunque affermare che *un toro complesso è univocamente determinato da un punto in $\mathcal{H}$ a meno di azioni di $SL_2(\mathbb{Z})$.*

Torneremo su questo aspetto nel capitolo in cui adotteremo un approccio aritmetico.

1.3 Isogenie e loro strumenti fondamentali

A questo punto del discorso, risulta naturale introdurre un nome per queste particolari mappe tra tori complessi. Esse prendono il nome di isogenie. Vedremo che due casi particolarmente semplici hanno un ruolo fondamentale: permettono di descrivere ogni altro tipo di isogenia.

La sezione sarà organizzata nel modo seguente: inizieremo introducendo le definizioni e le proprietà generali delle isogenie, successivamente ci concentreremo sul *sottogruppo di torsione N-esima* dei tori complessi; infine, nell'ultima sottosezione, parleremo di un ulteriore endomorfismo che questi possono ammettere.

Richiamiamo innanzi tutto una nozione di base della teoria dei gruppi di cui faremo uso in seguito.

Definizione 1.3.1. Dato un gruppo G e un sottogruppo $H \leq G$, chiamiamo *indice di H in G* il numero di classi laterali sinistre di H in G, ovvero:

$$[G : H] = \#\{gH \mid g \in G\} \ .$$

1.3.1 Definizioni e proprietà delle isogenie

Iniziamo chiarendo la nozione di isogenia ed enunciandone le proprietà di base, che saranno il punto di partenza per il proseguimento del discorso.

Definizione 1.3.2. Si dice *isogenia* un omomorfismo olomorfo non nullo tra tori complessi.

Osservazione 1.3.1. Ogni isogenia è suriettiva e ha nucleo finito.

Dimostrazione. Un'isogenia $\phi\colon T_1 \longrightarrow T_2$ è in particolare una funzione olomorfa e non costante tra superfici di Riemann compatte, quindi per il Lemma 1.1.11, è suriettiva. Per quanto riguarda il nucleo, questo è finito perché è un discreto (gli zeri di una funzione olomorfa sono isolati) in un compatto (il toro T_1). □

Soffermiamoci ora su due specifici esempi, fondamentali poiché, come vedremo, ogni isogenia può essere espressa come una composizione di essi.

Esempio 1.3.1 (Mappa moltiplicazione per un intero)**.**
Presi $N \in \mathbb{N}^*$ e $\Lambda \subset \mathbb{C}$ reticolo, la funzione

$$[N] : \begin{array}{c} \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda \\ [z]_\Lambda \longmapsto [Nz]_\Lambda \end{array}$$

è un'isogenia perché $N\Lambda \subseteq \Lambda$ e vale il punto 2 del Corollario 1.2.8
Il suo nucleo è detto *insieme dei punti di N-torsione di* $\mathbb{C}/\Lambda$ ed è isomorfo a $\mathbb{Z}_N \times \mathbb{Z}_N$.

Osservazione 1.3.2. Sia $End(\mathbb{C}/\Lambda)$ l'anello degli endomorfismi su $\mathbb{C}/\Lambda$ e consideriamo il sottoanello degli endomorfismi dati dalle mappe moltiplicazioni per un intero:

$$S = \{[N] \mid N \in \mathbb{Z}\} \subset End(\mathbb{C}/\Lambda) \ .$$

Allora S è isomorfo a $\mathbb{Z}$.

Dimostrazione. Consideriamo la funzione naturale

$$\begin{array}{c} \phi\colon \mathbb{Z} \longrightarrow \{[N] \mid N \in \mathbb{Z}\} \\ N \longmapsto [N] \end{array} .$$

Tale mappa è un omomorfismo perché $\phi(N+M) = [N+M] = [N] + [M]$.

Per mostrare l'iniettività, si osservi che, se $N \in \mathbb{Z}$ è tale che $[N]$ è l'endomorfismo nullo, allora per ogni $z \in \mathbb{C}$ si ha che $Nz \in \Lambda$; dunque, se N fosse diverso da 0, questo implicherebbe che, dato che $N\mathbb{C} = \mathbb{C}$, $\mathbb{C} \subseteq \Lambda$ che è assurdo.

Infine, tale mappa è suriettiva perché per ogni $[N] \in \{[N] \mid N \in \mathbb{Z}\}$ si ha che $[N] = \phi(N)$ per $N \in \mathbb{Z}$. □

Esempio 1.3.2 (Mappa quoziente ciclica)**.**
Per $N \in \mathbb{N}^*$, Λ reticolo e $G \leq \ker([N])$ sottogruppo ciclico tale che $G \cong \mathbb{Z}_N$, abbiamo che gli elementi $[g]_\Lambda \in G$ sono tali che $Ng \in \Lambda$. Se consideriamo l'insieme dei rappresentanti:

$$\{g \in \mathbb{C} : Ng \in \Lambda\} \subseteq \mathbb{C}\ ,$$

otteniamo un insieme che genera un reticolo contenente Λ, cioè un *sovra-reticolo* di Λ, che con un piccolo abuso di notazione, chiamiamo ancora G.
La proiezione:

$$\pi\ :\ \begin{array}{c} \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/G \\ [z]_\Lambda \mapsto [z]_G \end{array}$$

è un'isogenia. Inoltre essa ha nucleo $\ker(\pi) = G$.

Osservazione 1.3.3. Ogni isogenia è una composizione delle isogenie appena mostrate.

Per dimostrarlo, abbiamo bisogno dei seguenti risultati di teoria dei gruppi abeliani finitamente generati.

Lemma 1.3.4. *Sia G un gruppo abeliano finitamente generato di rango r e sia $H \leq G$ un sottogruppo di rango s . Allora esiste $\{\gamma_1, ..., \gamma_r\}$ base di G e esistono $t_1, ..., t_s \in \mathbb{Z}$ tali che $\{t_1\gamma_1, ..., t_s\gamma_s\}$ è una base di H.*

Una dimostrazione del Lemma 1.3.4 è disponibile in [Ste03]

Corollario 1.3.5. *Ogni gruppo abeliano finitamente generato si può scrivere*

$$\mathbb{Z}^a \oplus \bigoplus_i \mathbb{Z}_{t_i}$$

per certi $a, t_i \in \mathbb{Z}$.

Dimostrazione (del Corollario 1.3.5). Dalla Definizione 1.1.3 deduciamo che, per il Primo teorema di omomorfismo, un gruppo abeliano finitamente generato può essere visto come quoziente di un gruppo abeliano libero per un suo sottogruppo. Sia quindi G/H un gruppo abeliano finitamente generato, dove G è un gruppo abeliano libero di rango r e $H \leq G$ è di rango s.

Per il Lemma 1.3.4, esistono $t_1, ..., t_s \in \mathbb{Z}$ e esiste un isomorfismo

$$\phi : G \longrightarrow \mathbb{Z}^r$$

tale che $\phi(H)$ ha come base $\{t_1 e_1, ..., t_s e_s\}$, dove con e_i indichiamo l'i-esimo vettore della base canonica di $\mathbb{R}^r$.
Passando al quoziente, otteniamo

$$G/H = \mathbb{Z}^{s-r} \oplus \mathbb{Z}_{t_1} \oplus ... \oplus \mathbb{Z}_{t_s} .$$

□

Corollario 1.3.6. *Sia $N \in \mathbb{N}^*$ e sia K isomorfo a un sottogruppo di $\mathbb{Z}_N \times \mathbb{Z}_N$. Allora esistono $n, n' \in \mathbb{N}^*$ tali che*

$$K \cong \mathbb{Z}_n \times \mathbb{Z}_{nn'} .$$

Dimostrazione. Poiché $\mathbb{Z}_N \times \mathbb{Z}_N$ è un gruppo abeliano finitamente generato, anche K lo è. Identifichiamo $\mathbb{Z}_N \times \mathbb{Z}_N$ con $\mathbb{Z}^2/N\mathbb{Z}^2$ tramite la proiezione

$$\pi \colon \mathbb{Z}^2 \longrightarrow \mathbb{Z}_N \times \mathbb{Z}_N .$$

Quindi, chiamando $\tilde{K} = \pi^{-1}(K)$, si ha che $K \cong \tilde{K}/N\mathbb{Z}^2$. Per il Lemma 1.3.4, esistono $t_1, t_2 \in \mathbb{Z}$ tali che

$$\tilde{K} = t_1\mathbb{Z} + t_2\mathbb{Z} .$$

Poiché $N\mathbb{Z}^2 \subseteq \tilde{K}$, t_i divide N e quindi

$$K \cong \frac{t_1\mathbb{Z}}{N\mathbb{Z}} + \frac{t_2\mathbb{Z}}{N\mathbb{Z}} \cong \mathbb{Z}_{N/t_1} + \mathbb{Z}_{N/t_2} .$$

Prendendo n il massimo comun divisore di $\frac{N}{t_1}$ e $\frac{N}{t_2}$ e prendendo n' tale che nn' è il minimo comune multiplo, otteniamo che

$$K \cong \mathbb{Z}_n \times \mathbb{Z}_{nn'} .$$

□

Dimostrazione (dell'Osservazione 1.3.3). Consideriamo un'isogenia arbitraria:

$$\phi : \begin{array}{c} \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda' \\ [z]_\Lambda \mapsto [mz]_{\Lambda'} \end{array}$$

e chiamiamo

$$K = \ker(\phi) = \{[z]_\Lambda \in \mathbb{C}/\Lambda : mz \in \Lambda'\}$$

che, come prima, leggiamo come il sovra-reticolo $K = m^{-1}\Lambda' \subset \mathbb{C}$ di Λ. Sia N l'ordine di K. Allora, per $[z]_\Lambda \in K$, si ha che $[Nz]_\Lambda = [0]_\Lambda$, cioè $K \subset \ker([N]) \cong \mathbb{Z}_N \times \mathbb{Z}_N$.
Quindi, per il Corollario 1.3.6, esistono $n, n' \in \mathbb{N}^*$ tali che $K \cong \mathbb{Z}/n \times \mathbb{Z}/nn'$. Se consideriamo le mappe:

- $[n]$ da $\mathbb{C}/\Lambda$ in se stesso $\to$ porta K in nK,
- $\pi\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/nK \to$ ha nucleo nK,
- $f\colon \mathbb{C}/nK \longrightarrow \mathbb{C}/\Lambda'$ definita da $[z]_{nK} \mapsto \left[\frac{m}{n} \cdot z\right]_{mK=\Lambda'} \to$ è un isomorfismo;

otteniamo che:

$$\phi = f \circ \pi \circ [n]\colon \begin{array}{ccccccc} \mathbb{C}/\Lambda & \xrightarrow{[n]} & \mathbb{C}/\Lambda & \xrightarrow{\pi} & \mathbb{C}/nK & \xrightarrow{f} & \mathbb{C}/\Lambda' \\ [z]_\Lambda & \longmapsto & [nz]_\Lambda & \longmapsto & [nz]_{nK} & \longmapsto & [mz]_{\Lambda'} \end{array}$$

□

Osservazione 1.3.7. Essere isogeni è una relazione di equivalenza.

Per mostrare questo fatto, abbiamo innanzi tutto bisogno della seguente definizione.

Definizione 1.3.3. Data un'isogenia $\phi\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$, la funzione

$$\hat{\phi}\colon \mathbb{C}/\Lambda' \longrightarrow \mathbb{C}/\Lambda$$

si dice *isogenia duale* di ϕ se vale:

$$\hat{\phi} \circ \phi = [deg(\phi)]$$

dove $deg(\phi) := \#\ker(\phi)$.

Osservazione 1.3.8. Tale isogenia esiste sempre ed è unica.

Dimostrazione (dell'Osservazione 1.3.8). Consideriamo come prima un'isogenia arbitraria

$$\begin{array}{rccc} \phi: & \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda' \\ & [z]_\Lambda & \longmapsto & [mz]_{\Lambda'} \end{array}$$

dove $m \neq 0$ e $m\Lambda \subseteq \Lambda'$.

Per il Lemma 1.3.4, esiste una base $\{\omega_1, \omega_2\}$ di Λ' e esistono $n_1, n_2 \in \mathbb{N}^*$ tali che $\{n_1\omega_1, n_2\omega_2\}$ è una base di $m\Lambda$.

Segue che $n_1 n_2 \Lambda' \subseteq m\Lambda$ e quindi

$$\frac{n_1 n_2}{m}\Lambda' \subseteq \Lambda\ .$$

Deduciamo che esiste:

$$\begin{aligned}\hat{\phi}:\ \mathbb{C}/\Lambda' &\longrightarrow \mathbb{C}/\Lambda \\ [z]_{\Lambda'} &\longmapsto \left[\frac{n_1 n_2}{m} z\right]_{\Lambda}\end{aligned}$$

isogenia duale di ϕ e osserviamo che $\hat{\phi} \circ \phi$ risulta essere una *mappa moltiplicazione* (per l'intero $n_1 n_2$), cioè:

$$\hat{\phi} \circ \phi = [n_1 n_2].$$

Poiché ϕ è suriettiva, questa è una condizione che determina univocamente $\hat{\phi}$. □

Osservazione 1.3.9. $n_1 n_2 = deg(\phi)$.

Dimostrazione (dell'Osservazione 1.3.9). $\left\{\frac{\omega_1}{m}, \frac{\omega_2}{m}\right\}$ è una base di $ker(\phi)$ e $\left\{\frac{n_1\omega_1}{m}, \frac{n_2\omega_2}{m}\right\}$ è una base di Λ e questo implica che l'ordine di $\ker(\phi)$ è $n_1 n_2$. □

Dimostrazione (dell'Osservazione 1.3.7). Essere isogeni è una relazione riflessiva perché un toro è sempre isogeno a se stesso tramite l'identità; è simmetrica perché, se un toro $\mathbb{C}/\Lambda$ è isogeno a un toro $\mathbb{C}/\Lambda'$ tramite un'isogenia ϕ, allora il toro $\mathbb{C}/\Lambda'$ è isogeno al toro $\mathbb{C}/\Lambda$ tramite l'isogenia duale $\hat{\phi}$; è transitiva perché la composizione di isogenie è ancora un'isogenia. □

Studiamo ora alcune delle proprietà principali delle isogenie duali.

Proposizione 1.3.10.

1. *$deg(\phi) = deg(\hat{\phi})$.*
2. *L'isogenia duale della mappa moltiplicazione per un intero è se stessa.*
3. *L'isogenia duale della mappa quoziente ciclica*

   $$\pi\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/G\ ,$$

   dove $G \leq \ker([N])$ e $G \cong \mathbb{Z}_N$ per $N \in \mathbb{N}^*$, è anch'essa una mappa quoziente ciclica. In particolare, se chiamiamo $\hat{\pi}$ l'isogenia duale di π, si ha che

   $$\hat{\pi} \circ \pi = [N]\ .$$

4. *L'isogenia duale di un isomorfismo è la sua inversa. Ovvero, se chiamiamo ϕ tale isomorfismo, si ha*

   $$\hat{\phi} = \phi^{-1}$$

5. *L'isogenia duale di una composizione di isogenie è la composizione delle isogenie duali in ordine invertito, cioè:*

$$\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi} \ .$$

6. *Se* $\phi_1, \phi_2 \colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ *sono due isogenie tali che* $\phi_1 + \phi_2$ *è un'isogenia non nulla, allora l'isogenia duale della somma è la somma delle isogenie duali, cioè:* $\widehat{\phi_1 + \phi_2} = \hat{\phi}_1 + \hat{\phi}_2$.

Dimostrazione.

1. La mappa $[deg(\phi)]$ ha grado $(deg(\phi))^2$ e il grado di una composizione è il prodotto dei gradi.

2. Segue direttamente dal fatto che $[N] \circ [N] = [N^2]$ e che $deg([N]) = N^2$.

3. Osserviamo innanzi tutto che

$$deg(\pi) = \#\ker(\pi) = \#G = N \ ,$$

quindi otteniamo che

$$\hat{\pi} \circ \pi = [deg(\pi)] = [N] \ .$$

Consideriamo ora H il complementare di G in $\ker([N])$. Si ha che, $x \in H \subset \ker([N])$, se e solo se

$$(\hat{\pi} \circ \pi)(x) = [N](x) = 0$$

da cui deduciamo che

$$\ker(\hat{\pi}) = \pi(H)$$

che è un sottogruppo ciclico di $\mathbb{C}/G$. Chiamando $G' := \pi(H)$, otteniamo un sovrareticolo di $G \subset \mathbb{C}$ e quindi otteniamo che l'isogenia duale

$$\hat{\pi} \colon \mathbb{C}/G \longrightarrow \mathbb{C}/\Lambda \simeq \mathbb{C}/G' \ ,$$

è ciclica. In altre parole, abbiamo ottenuto che l'isogenia duale di π quozienta il toro di arrivo (il codominio $\mathbb{C}/G$ di π) nella direzione complementare a G in $\ker([N])$.

4. Segue direttamente dal fatto che gli isomorfismi hanno grado 1 e che la mappa identità corrisponde all'isogenia moltiplicazione [1].

5. Date due isogenie $\psi \colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ e $\phi \colon \mathbb{C}/\Lambda' \longrightarrow \mathbb{C}/\Lambda''$, si ha che:

$$(\phi \circ \psi) \circ (\hat{\psi} \circ \hat{\phi}) = \phi \circ [deg(\psi)] \circ \hat{\phi} = [deg(\psi)] \circ \phi \circ \hat{\phi} =$$
$$= [deg(\psi)] \circ [deg(\phi)] = [deg(\psi) \cdot deg(\phi)] = [deg(\phi \circ \psi)]$$

e quindi $\hat{\psi} \circ \hat{\phi} = \widehat{\phi \circ \psi}$.

6. Mostriamolo leggendo le isogenie come moltiplicazioni per matrici a coefficienti interi. Consideriamo un'isogenia arbitraria:

$$\phi : \begin{array}{c} \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda' \\ [z]_\Lambda \longmapsto [mz]_{\Lambda'} \end{array}$$

dove $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ con $\frac{\omega_1}{\omega_2} \in \mathcal{H}$, $\Lambda' = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$ con $\frac{\omega_1'}{\omega_2'} \in \mathcal{H}$ e $m \neq 0$ è tale che $m\Lambda \subset \Lambda'$.

Si ha quindi che esiste $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ tale che

$$\begin{pmatrix} m\omega_1 \\ m\omega_2 \end{pmatrix} = \alpha \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$$

e questo significa che $\omega_1/\omega_2 = \alpha(\omega_1'/\omega_2')$ e quindi $det(\alpha) > 0$, poiché $\Im(\omega_1/\omega_2), \Im(\omega_1'/\omega_2') > 0$.

Osserviamo che:

$$deg(\phi) = \#\ker(\phi) = [m^{-1}\Lambda' : \Lambda] = [\Lambda' : m\Lambda] = det(\alpha)\ ,$$

da cui deduciamo che, date due isogenie ϕ e ψ, la matrice associata alla composizione sarà

$$M(\phi \circ \psi) = M(\phi) \cdot M(\psi)\ .$$

Nel nostro caso quindi, poiché vale la relazione $\phi \circ \hat{\phi} = [deg(\phi)]$, si avrà che:

$$M(\phi) \cdot M(\hat{\phi}) = M([deg(\phi)]) \implies \alpha \cdot \hat{\alpha} = deg(\phi) \cdot I_2 = det(\alpha) \cdot I_2$$

e quindi:

$$M(\hat{\phi}) = \hat{\alpha} = det(\alpha) \cdot \alpha^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Dunque avremo che l'isogenia somma:

$$\phi_1 + \phi_2 \ : \ \begin{array}{ll} \mathbb{C}/\Lambda & \longrightarrow \mathbb{C}/\Lambda' \\ [z]_\Lambda & \mapsto [(m_1 + m_2)z]_{\Lambda'} \end{array}$$

è associata alla matrice:

$$M(\phi_1 + \phi_2) = \alpha_1 + \alpha_2 = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$

e quindi, per il discorso appena fatto, l'isogenia duale $\widehat{\phi_1 + \phi_2}$ sarà associata alla matrice:

$$M(\widehat{\phi_1 + \phi_2}) = \begin{bmatrix} d_1 + d_2 & -b_1 - b_2 \\ -c_1 - c_2 & a_1 + a_2 \end{bmatrix} = \hat{\alpha_1} + \hat{\alpha_2}$$

che prova quanto volevamo dimostrare.

□

1.3.2 Il gruppo di torsione e l'accoppiamento di Weil

Consideriamo ora il gruppo di torsione N-esima, che svolge un ruolo centrale nello studio delle isogenie. In particolare, su di esso introdurremo l'*accoppiamento di Weil*, strumento fondamentale per comprenderne la struttura.

Sia $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ un reticolo e sia $N \in \mathbb{N}^*$. Il sottogruppo di torsione N-esima di $\mathbb{C}/\Lambda$ è

$$\ker([N]) = \{[g]_\Lambda \in \mathbb{C}/\Lambda : [N]([g]_\Lambda) = [0]_\Lambda\} = \langle \left[\tfrac{\omega_1}{N}\right]_\Lambda, \left[\tfrac{\omega_2}{N}\right]_\Lambda \rangle \simeq \mathbb{Z}_N \times \mathbb{Z}_N \ .$$

Esso rappresenta l'analogo bidimensionale del sottogruppo di torsione N-esima di $\mathbb{R}/\mathbb{Z} \simeq \mathbb{S}^1$, ovvero l'insieme delle radici N-esime dell'unità:

$$\left\{z \in \mathbb{C} : z^N = 1\right\} = \langle e^{\frac{2\pi i}{N}} \rangle \cong \mathbb{Z}_N \ .$$

Questa analogia suggerisce l'esistenza di una sorta di prodotto interno

$$\ker([N]) \times \ker([N]) \longrightarrow \mu_N \ ,$$

che introduciamo di seguito.

Definizione 1.3.4. Sia $N \in \mathbb{N}^*$ e consideriamo la mappa $[N]$ da $\mathbb{C}/\Lambda$ in se stesso, dove $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ e $\frac{\omega_1}{\omega_2} \in \mathcal{H}$.
Presi $P, Q \in \ker([N])$, esiste $\alpha \in M_2(\mathbb{Z}_N)$ tale che

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \left[\frac{\omega_1}{N}\right]_\Lambda \\ \left[\frac{\omega_2}{N}\right]_\Lambda \end{pmatrix} \ .$$

Definiamo allora il *l'accoppiamento di Weil su torsione N-esima* come la mappa

$$\begin{aligned} e_N : \ \ker([N]) \times \ker([N]) &\longrightarrow \mu_N \\ (P, Q) &\longmapsto e^{\frac{2\pi i det(\gamma)}{N}} \ . \end{aligned}$$

Questo strumento non è stato introdotto a caso: riapparirà infatti nel capitolo dedicato all'approccio aritmetico, quando parleremo di *curve ellittiche potenziate*.

1.3.3 Introduzione alla moltiplicazione complessa

Alcuni tori complessi ammettono altri endomorfismi oltre all'isogenia $[N]$: in tal caso si dice che sono dotati di *moltiplicazione complessa*.

Per fornire un esempio di questo, abbiamo bisogno della seguente definizione.

Definizione 1.3.5. Un intero positivo $n \in \mathbb{N}^*$ si dice *privo di quadrati* se nella sua fattorizzazione in numeri primi

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... p_s^{r_s}$$

nessun fattore è ripetuto (e quindi $r_1 = ... = r_s = 1$), cioè n non è diviso da nessun quadrato.

Lemma 1.3.11. *Sia* $\Theta = \tau\mathbb{Z} + \mathbb{Z}$, *dove*

$$\tau = \begin{cases} \sqrt{d} \text{ con } d \in \mathbb{Z}^- \text{ privo di quadrati e tale che } d \equiv 2,3 \pmod 4 \\ \text{oppure} \\ \frac{-1+\sqrt{d}}{2} \text{ con } d \in \mathbb{Z}^- \text{ privo di quadrati e tale che } d \equiv 1 \pmod 4 \end{cases} .$$

In entrambi i casi, Θ *è un anello.*

Dimostrazione. La parte meno immediata da mostrare è la chiusura del prodotto. Siano dunque $a + b\tau,\ c + d\tau \in \Theta$ due elementi generici e calcoliamo

$$(a + b\tau)(c + d\tau) = ac + (bc + ad)\tau + bd\tau^2 .$$

Dunque l'obiettivo è mostrare che τ^2 si scrive come combinazione lineare in $\mathbb{Z}$ di 1 e τ. Se $\tau = \sqrt{d}$, allora $\tau^2 = d \in \mathbb{Z}$; se invece $\tau = \frac{-1+\sqrt{d}}{2}$, con $d \in \mathbb{Z}^-$ privo di quadrati e congruo a 2 o 3 modulo 4, chiamando $\sqrt{d} = s$, si ottiene che $s = 2\tau + 1$ e quindi

$$\tau^2 = \frac{1 - 2s + d}{4} = \frac{d - 4\tau - 1}{4} = -\tau + \frac{d-1}{4} \in \Theta$$

perché $\frac{d-1}{4} \in \mathbb{Z}$. □

Consideriamo un ideale $\Lambda \subseteq \Theta$. Allora per un qualsiasi numero complesso $m \in \Theta$, si ha che $m\Lambda \subset \Lambda$ e questa condizione mi garantisce che la moltiplicazione per m data da

$$\begin{aligned} (m)\colon \mathbb{C}/\Lambda &\longrightarrow \mathbb{C}/\Lambda \\ [z]_\Lambda &\longmapsto [mz]_\Lambda \end{aligned}$$

è ben definita perché manda il reticolo nel reticolo. In particolare abbiamo così mostrato che $(m) \in End(\mathbb{C}/\Lambda)$.

Si può dimostrare che $End(\mathbb{C}/\Lambda_i) \cong \Lambda_i$. Per questo risultato, e per ulteriori approfondimenti sulla moltiplicazione complessa, si rinvia a [Sin].

1.4 $\wp$ di Weierstrass

In questa sezione verrà introdotta la funzione $\wp$ di Weierstrass. Mostreremo, non solo che si tratta di una funzione ellittica con proprietà estremamente utili, che la rendono uno strumento fondamentale per lo studio dell'analisi complessa, ma anche che, grazie ad essa, è possibile studiare qualsiasi altra funzione ellittica in maniera più agevole. In particolare, per poter dimostrare tali risultati, sarà necessario parlare dei campi di funzioni ellittiche, che esamineremo in maniera concisa, cercando di renderli il più chiari possibile.

1.4.1 Costruzione $\wp$ di Weierstrass

Il nostro obiettivo è costruire un esempio quanto più semplice possibile di funzione ellittica non costante.
Sappiamo che non esistono funzioni ellittiche non costanti di ordine 1; perciò ci soffermeremo sul caso di ordine 2. In questo caso, la funzione cercata avrà, modulo il reticolo L, o due poli semplici con residui opposti o un polo doppio con residuo nullo.

Proviamo dunque a definire una funzione ellittica di ordine 2 con un solo polo doppio in 0 modulo L, in modo da ottenere che ogni altro polo coincida con un punto del reticolo.

Un primo tentativo di definizione di una tale funzione, prendendo un reticolo $L \subset \mathbb{C}$ arbitrario, potrebbe essere il seguente:

$$f(z) = \sum_{\omega \in L} \frac{1}{(z-\omega)^2} \quad .$$

Questa funzione ha poli doppi nei punti del reticolo L. Tuttavia, non possiamo affermare che f converga assolutamente per qualsiasi scelta di L. Per esempio, se scegliamo $L = \mathbb{Z} + i\mathbb{Z}$, la serie non converge.
Infatti, separando i termini otteniamo

$$f(z) = \frac{1}{z^2} + \sum_{\omega \in L^*} \frac{1}{(z-\omega)^2}$$

e chiamando la sommatoria $g(z)$, per $\omega = m + in$, con $m, n \in \mathbb{Z}$, calcolando $g(0)$, si arriva al termine

$$\frac{1}{|m+in|^2} = \frac{1}{m^2+n^2}$$

che non converge, come mostra il seguente lemma.

Lemma 1.4.1. *La serie:*

$$\sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m^2+n^2)^\alpha}\,, \quad \alpha \in \mathbb{R}$$

converge se e solo se $\alpha > 1$.

Una dimostrazione di questo lemma si può trovare al capitolo V3 di [BF09] o al capitolo 9 di [SS10].

Vediamo un altro risultato di convergenza che ci servirà a definire la funzione desiderata.

Lemma 1.4.2. *Sia* $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$ *reticolo. Allora la serie*

$$\sum_{\omega\in L^*} \frac{1}{|\omega|^s}$$

converge per $s > 2$.

Dimostrazione. $\forall n \in \mathbb{N}^*$ costruiamo

$$P_n \quad \text{parallelogramma di vertici} \quad \pm n\omega_1 \pm n\omega_2$$

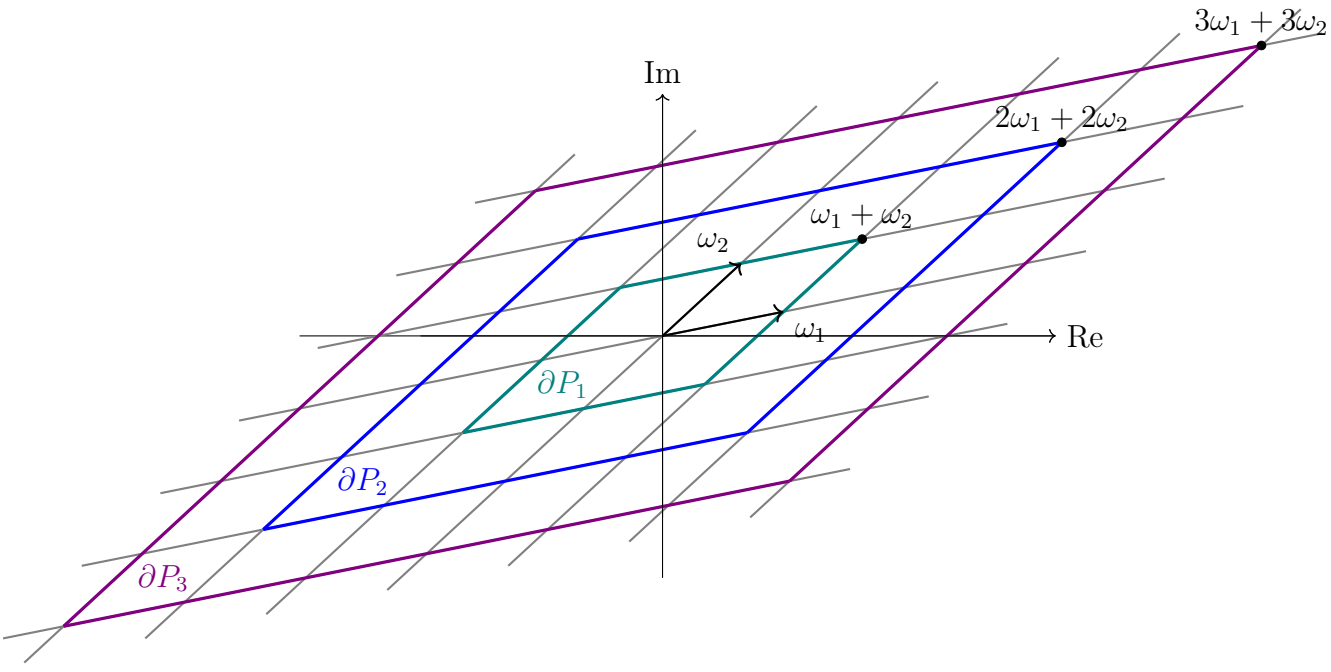


Figura 2: Frontiere dei parallelogrammi P_1, P_2 e P_3

e chiamiamo $L_n = \partial P_n \cap L$ in modo da ottenere

$$L^* = \bigcup_{n \in \mathbb{N}^*} L_n \ .$$

Siano $c_1, c_2 > 0$ tali che per ogni $\omega \in L^*$ si ha

$$n \cdot c_1 \leq |\omega_1| \leq n \cdot c_2 \ .$$

Osservando che

$$\sum_{\omega \in L^*} \frac{1}{|\omega|^s} = \sum_{n=1}^{+\infty} \sum_{\omega \in L_n} \frac{1}{|\omega|^s} \ ,$$

possiamo stimare la somma così:

$$\sum_{n=1}^{+\infty} \frac{8n}{n^s \cdot c_2^s} \leq \sum_{n=1}^{+\infty} \sum_{\omega \in L_n} \frac{1}{|\omega|^s} \leq \sum_{n=1}^{+\infty} \frac{8n}{n^s \cdot c_1^s} \ .$$

La tesi segue direttamente.

□

Definizione 1.4.1. Dato un reticolo L, la funzione definita da

$$\wp(z) = \begin{cases} \dfrac{1}{z^2} + \displaystyle\sum_{\omega \in L \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] \ , & \text{se } z \in \mathbb{C} \setminus L \ , \\ \infty \ , & \text{se } z \in L \ . \end{cases}$$

è chiamata *$\wp$ di Weierstrass associata al reticolo L.*

1.4.2 Proprietà $\wp$ di Weierstrass

In questa sottosezione analizzeremo le proprietà fondamentali della funzione $\wp$ di Weierstrass. Alcune di esse ci permetteranno di verificare che questa è effettivamente una funzione ellittica con poli di ordine 2 nei punti del reticolo. Osserveremo poi che $\wp$ ammette uno sviluppo di Laurent in 0 particolarmente utile per le applicazioni successive.

Osservazione 1.4.3. La $\wp$ di Weierstrass associata al reticolo L è pari.

Dimostrazione. Per $z \in \mathbb{C} \setminus L$, si ha

$$\wp(-z) = \frac{1}{z^2} + \sum_{\omega \in L} \left[\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{z^2} + \sum_{\omega \in L} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right] =$$

$$= \frac{1}{z^2} + \sum_{-\omega \in L} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] = \wp(z)$$

□

Proposizione 1.4.4. *La $\wp$ di Weierstrass associata al reticolo L converge assolutamente su $\mathbb{C} \setminus L$ ed è una funzione meromorfa su $\mathbb{C}$ con poli doppi in L.*

Dimostrazione. Fissiamo $z \in \mathbb{C} \setminus L$ e prendiamo R tale che $z \in \mathcal{B}_R(0)$, palla di raggio R centrata in 0.

Spezziamo la somma

$$\wp(z) = \frac{1}{z^2} + \sum_{|\omega| \leq 2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] + \sum_{|\omega| > 2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

e osserviamo che

$$\frac{1}{z^2} + \sum_{|\omega| \leq 2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

è una funzione olomorfa in $\mathbb{C} \setminus (L \cap \overline{\mathcal{B}_{2R}(0)})$ con poli doppi in $L \cap \overline{\mathcal{B}_{2R}(0)}$.
Per quanto riguarda l'altro termine, invece, sfruttando la stima

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{2z\omega + z^2}{(z-\omega)^2 \cdot \omega^2} \right| \leq \left| \frac{2|\omega| \cdot R + R^2}{|\omega|^4 - |\omega|^2 \cdot R^2} \right| ,$$

otteniamo una frazione con ω che ha esponente 1 al numeratore e 4 al denominatore, dunque si deduce che la serie

$$\sum_{|\omega| > 2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

converge in $\mathcal{B}_R(0)$. Ne consegue che $\wp$ è una funzione olomorfa su $\mathbb{C} \setminus L$ con poli doppi in L.

□

Proposizione 1.4.5. *La derivata della $\wp$ di Weierstrass associata al reticolo L ha poli tripli in L, è dispari ed è L-periodica.*

Dimostrazione. Derivando $\wp$ termine a termine, si ottiene

$$\wp'(z) = -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3} \quad .$$

Ragionando come per l'Osservazione 1.4.3, si ottiene

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

per vedere la periodicità, prendiamo $l \in L$ e calcoliamo

$$\wp'(z+l) = -2\sum_{\omega\in L}\frac{1}{(z+l-\omega)^3} = -2\sum_{l-\omega\in L}\frac{1}{(z+l-\omega)^3} = \wp'(z) \ .$$

□

Corollario 1.4.6. *Sia L un reticolo. Allora la $\wp$ di Weierstrass ad esso associata è L-periodica.*

Dimostrazione. Sia $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.

La funzione $\wp$, la funzione $z \mapsto \wp(z+\omega_1)$ e la funzione $z \mapsto \wp(z+\omega_2)$ sono tutte primitive di $\wp'$.
Dunque differiscono di una costante, cioè esistono a e b in $\mathbb{C}$ tali che

$$\wp(z+\omega_1) = \wp(z) + a \quad \text{e} \quad \wp(z+\omega_2) = \wp(z) + b \ .$$

Quindi, poiché $\wp$ è pari, si ha che

$$\wp\left(-\frac{\omega_1}{2}\right) = \wp\left(\frac{\omega_1}{2}\right) = \wp\left(-\frac{\omega_1}{2}\right) + a$$

e analogamente

$$\wp\left(-\frac{\omega_2}{2}\right) = \wp\left(\frac{\omega_2}{2}\right) = \wp\left(-\frac{\omega_2}{2}\right) + b \ .$$

Segue che a e b sono entrambi nulli.

□

Osservazione 1.4.7. Dato il reticolo $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, chiamiamo $\omega_3 = \omega_1 + \omega_2$. Allora per ogni $i = 1, 2, 3$ si ha che ω_i è uno zero di $\wp'$.

Dimostrazione. $\wp'$ è dispari ed è L-periodica. Quindi

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right) \ .$$

□

Notazione 1.4.1. D'ora in avanti, per $i = 1, 2, 3$, indicheremo

$$a_i := \wp\left(\frac{\omega_i}{2}\right) \ .$$

Lemma 1.4.8 (Caratterizzazione invariante degli zeri di $\wp'$)**.** *Sia L un reticolo e consideriamo la $\wp$ di Weierstrass ad esso associata.*
Allora $a \in \mathbb{C}$ è uno zero di $\wp'$ se e solo se

$$a \notin L \quad e \quad 2a \in L \ .$$

In particolare ci sono esattamente 3 zeri di $\wp'$ modulo L.

Dimostrazione. Supponiamo a verifichi la condizione dell'enunciato. Si ha che

$$\wp'(a) = \wp'(a - 2a) = \wp'(-a) = -\wp'(a)$$

quindi $\wp'(a) = 0$. Questo ci dà un'ulteriore prova del fatto che se $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ allora i punti

$$\frac{\omega_1}{2}, \quad \frac{\omega_2}{2} \quad \text{e} \quad \frac{\omega_1 + \omega_2}{2}$$

sono zeri di $\wp'$. Poiché $\wp'$ ha un solo polo triplo modulo L, tali zeri sono gli unici modulo L e sono tutti e tre semplici. □

Proposizione 1.4.9. *Data la $\wp$ di Weierstrass associata al reticolo $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, vale:*

$$(\wp'(z))^2 = 4(\wp(z) - a_1)(\wp(z) - a_2)(\wp(z) - a_3) \ .$$

Dimostrazione. Chiamiamo

$$F(z) = (\wp(z) - a_1)(\wp(z) - a_2)(\wp(z) - a_3)$$

e denotiamo come prima $\omega_3 := \omega_1 + \omega_2$. L'obiettivo è mostrare che $(\wp'(z))^2 = 4 \cdot F(z)$.

Gli unici zeri di F modulo L sono $\frac{\omega_i}{2}$, i quali hanno tutti molteplicità 2. Allo stesso modo, $(\wp')^2$ ha zeri doppi in tali punti (in quanto sono zeri semplici di $\wp'$).
Inoltre F ha, modulo L, un unico polo in 0 di ordine 6 (poiché $\wp$ ha un polo doppio in 0).

Lo stesso vale per $(\wp')^2$ (perché $\wp'$ ha un polo triplo in 0).

Si deduce quindi che la funzione

$$\frac{(\wp')^2}{F}$$

non ha poli ed è L-periodica e quindi, per il Teorema 1.1.1., è costante. Rimane da mostrare che tale costante è 4.

Osserviamo che, vicino a 0, possiamo scrivere

$$\wp(z) = \frac{1}{z^2} + ...$$

quindi

$$\wp'(z) = -\frac{2}{z^3} + ...$$

dove nei puntini ci saranno termini con z di grado più alto. Quindi

$$(\wp'(z))^2 = \frac{4}{z^6} + ...$$

e perciò la costante cercata è proprio 4.

□

Proposizione 1.4.10. *Consideriamo la $\wp$ di Weierstrass associata al reticolo L e due punti $z_1, z_2 \in L$. Allora:*

$$\wp(z_1) = \wp(z_2)$$

se e solo se

$$z_1 \equiv \pm z_2 \pmod{L}\,.$$

Dimostrazione. Fissato z_1 in $\mathbb{C}$, consideriamo la funzione

$$\begin{aligned} f\ :\ \mathbb{C} &\longrightarrow \mathbb{P}^1(\mathbb{C}) \\ z &\longmapsto \wp(z_1) - \wp(z_2) \end{aligned}$$

e osserviamo che

$$f(z) = \frac{1}{z_1^2} - \frac{1}{z_2^2} + \sum_{\omega \in L^*} \left[\frac{1}{(z_1 - \omega)^2} - \frac{1}{(z_2 - \omega)^2} \right]$$

è ellittica e ha zeri nei punti $z_1 \equiv \pm z_2 \pmod{L}$. □

Da questa proposizione deduciamo la seguente conseguenza importante riguardo la ramificazione di $\wp\colon \mathbb{C}/L \longrightarrow \mathbb{P}^1(\mathbb{C})$.

Osservazione 1.4.11. Ci sono 4 punti di biforcazione in $\mathbb{P}^1(\mathbb{C}) : a_1, a_2, a_3, \infty$. Ciascuno di loro ha esattamente una preimmagine con molteplicità 2 in $\mathbb{C}/L$, mentre tutti gli altri punti di $\mathbb{P}^1(\mathbb{C})$ hanno esattamente 2 preimmagini (con molteplicità 1).

Questo risultato geometrico ci ha permesso di comprendere meglio la struttura dei poli di $\wp$, che possiamo analizzare nel dettaglio tramite il suo sviluppo in serie di Laurent in 0.

Osservazione 1.4.12. Lo sviluppo di $\wp$ in serie di Laurent in 0 è

$$\wp(z) = \frac{1}{z^2} + \sum_{n=0}^{+\infty} a_{2n} z^{2n} \, . \tag{1.5}$$

Dimostrazione. Riprendiamo la Definizione 1.4.1 e sviluppiamo i termini della somma

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2}\left(1 - \frac{z}{\omega}\right)^{-2} \, .$$

Sfruttando la serie geometrica generalizzata

$$(1+x)^\alpha = \sum_{k=0}^{+\infty} \binom{\alpha}{x} x^k, \quad \alpha \in \mathbb{R}$$

con $\alpha = -2$, otteniamo

$$\frac{1}{\omega^2}\left(1 - \frac{z}{\omega}\right)^{-2} = \frac{1}{\omega^2}\left(1 + 2\frac{z}{\omega} + 3\frac{z^2}{\omega^2} + 4\frac{z^3}{\omega^3} + ...\right) \, .$$

Quindi si ha

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(2\frac{z}{\omega} + 3\frac{z^2}{\omega^2} + 4\frac{z^3}{\omega^3} + ...\right) = \sum_{k=1}^{+\infty}(k+1)\frac{z^k}{\omega^{k+2}}$$

e di conseguenza

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L^*}\sum_{k=1}^{+\infty}(k+1)\frac{z^k}{\omega^{k+2}} =$$

$$= \frac{1}{z^2} + \sum_{k=1}^{+\infty}(k+1)\left(\sum_{\omega \in L^*}\frac{1}{\omega^{k+2}}z^k\right) = \frac{1}{z^2} + \sum_{k=1}^{+\infty}(k+1)G_{k+2}z^k$$

dove la serie

$$G_n = G_n(L) = \sum_{\omega \in L^*}\frac{1}{\omega^n} \tag{1.6}$$

è detta *serie di Eisenstein*.

Osserviamo che, poiché per ogni $\omega \neq 0$ nel reticolo, si ha che anche $-\omega$ appartiene al reticolo, allora per n dispari si avrà $G_n = 0$. Possiamo quindi riscrivere la somma come

$$\frac{1}{z^2} + \sum_{k=1}^{+\infty}(k+1)G_{k+2}z^k = \frac{1}{z^2} + \sum_{n=1}^{+\infty}(2n+1)G_{2(n+1)}z^{2n} \quad .$$

Chiamando, per $n \geq 1$

$$a_{2n} = (2n+1) \cdot G_{2(n+1)} \ ,$$

otteniamo la scrittura desiderata. □

In alternativa, i coefficienti dello sviluppo in serie di Laurent di $\wp$ si possono ricavare applicando la formula di Taylor alla funzione

$$f(z) := \wp(z) - \frac{1}{z^2} \ .$$

Infatti, calcolando induttivamente le derivate

$$f^{(n)}(z) = (-1)^n(n+1)! \cdot \sum_{\omega \in L^*} \frac{1}{(z-\omega)^{n+2}}$$

si ottiene

$$f^{(2n)}(z) = (2n+1)! \cdot \sum_{\omega \in L^*} \frac{1}{(z-\omega)^{2n+2}} \ .$$

Sostituendo $z = 0$, si conclude:

$$a_{2n} = \frac{f^{(2n)}(0)}{(2n)!} = \frac{(2n+1)!}{(2n)!} \cdot \sum_{\omega \in L^*} \frac{1}{\omega^{2(n+1)}} = (2n+1) \cdot \sum_{\omega \in L^*} \frac{1}{\omega^{2(n+1)}} = (2n+1) \cdot G_{2(n+1)} \ .$$

1.4.3 Equazione differenziale algebrica di $\wp$

L'obiettivo di questa sottosezione è formulare l'equazione differenziale algebrica soddisfatta dalla funzione $\wp$ di Weierstrass, un risultato che permette di comprendere meglio le funzioni ellittiche.

La somma, la differenza e il quoziente (con denominatore non nullo) di funzioni ellittiche è ancora una funzione ellittica. Dunque l'insieme di tutte quelle associate a un certo reticolo L è un campo: lo chiamiamo $K(L)$.

Le funzioni costanti sono funzioni ellittiche quindi la funzione data da

$$\begin{aligned} \mathbb{C} &\longrightarrow K(L) \\ c &\longmapsto \text{funzione ellittica costante uguale a c} \end{aligned}$$

induce un isomorfismo di $\mathbb{C}$ con il sottocampo delle funzioni costanti in $K(L)$.

Per arrivare all'equazione di $\wp$ cercata, è necessario comprendere la struttura del campo $K(L)$ poiché ciò ci permette di dimostrare che ogni funzione ellittica può essere espressa in termini di $\wp$ e della sua derivata $\wp'$.

Sia $f \in K(L)$ una funzione ellittica associata al reticolo L e sia

$$P(w) = a_0 + a_1 w + ... + a_m w^m \in \mathbb{C}[w] \ .$$

Allora la composizione

$$P(f)(z) = a_0 + a_1 f(z) + ... + a_m (f(z))^m$$

è una funzione ellittica. Osserviamo che, per il Lemma 1.1.12, $P(f)$ è non identicamente nulla se e solo se f è non costante e P è non identicamente nulla.

Rivediamo questo discorso più in generale. Indichiamo con:

$$\mathbb{C}(z) = \left\{ f(z) = \frac{p(z)}{q(z)} : p, q \in \mathbb{C}[z] \ \text{ e } \ q \not\equiv 0 \right\}$$

l'insieme delle funzioni razionali e consideriamo $R \in \mathbb{C}(z)$. Questa può quindi essere scritta come quoziente di funzioni polinomiali $R = \frac{P}{Q}$ con Q non identicamente nulla.
La funzione ellittica $R(f) := \frac{P(f)}{Q(f)}$ dipende solo da R e non dalla scelta della rappresentazione in frazione.

Per $f \in K(L)$ definiamo il sottocampo ad essa associato:

$$\mathbb{C}(f) := \{ g \in K(L) : \exists R \in \mathbb{C}(z), \ g = R(f) \} \subseteq K(L) \ .$$

Ora che abbiamo introdotto il campo $\mathbb{C}(f)$, cerchiamo di comprenderne le struttura. Il prossimo lemma mostra che è meno complicata di quanto si possa pensare: dimostreremo, infatti, che questo campo è isomorfo al campo delle funzioni razionali.

Lemma 1.4.13. *Per ogni $f \in K(L)$ non costante si ha:*

$$\mathbb{C}(z) \simeq \mathbb{C}(f) \subseteq K(L) \ .$$

Dimostrazione. Consideriamo la mappa

$$F_f : \begin{array}{c} \mathbb{C}(z) \longrightarrow K(L) \\ R \longmapsto R(f) \ . \end{array}$$

Tale mappa è un omomorfismo perché, per $R, \tilde{R} \in \mathbb{C}(z)$, si ha che

$$F_f(R + \tilde{R}) = (R + \tilde{R})(f) = F_f(R) + F_f(\tilde{R}) \ .$$

Inoltre, per il Lemma 1.1.12, se $R(f) = \tilde{R}(f)$ allora $R = \tilde{R}$. Questo significa che F_f è iniettiva.

Quindi F_f induce un ismorfismo sull'immagine, che è data da $\mathbb{C}(f)$. Segue che

$$\mathbb{C}(z) \simeq \mathbb{C}(f) \ .$$

□

Abbiamo quindi appena caratterizzato i sottocampi di $K(L)$ generati da una funzione ellittica non costante. Quello a cui siamo interessati ora è descrivere l'intera struttura del campo $K(L)$. Vedremo, più avanti in questa sezione, che in realtà sono sufficienti le funzioni $\wp$ e la sua derivata per ottenere tutto $K(L)$: mostreremo, in particolare, che $K(L)$ è un'estensione algebrica finita di grado 2 di un campo razionale.

Cerchiamo per prima cosa di caratterizzare le funzioni ellittiche pari, concentrandoci innanzi tutto su quelle che hanno tutti i poli nel reticolo.

Lemma 1.4.14. *Sia $f \in K(L)$ pari e tale che tutti i suoi poli sono punti del reticolo L. Allora f può essere espressa come polinomio in $\wp$, cioè:*

$$f(z) = a_0 + a_1\wp(z) + ... + a_n(\wp(z))^n, \quad \textit{per certi} \quad a_i \in \mathbb{C}$$

dove il grado di tale polinomio è $n = \frac{Ord(f)}{2}$.

Dimostrazione. Se f è costante, non c'è nulla da dimostrare. Supponiamo dunque che non lo sia. Per il Teorema 1.1.3, f ha almeno un polo (che per ipotesi è un punto del reticolo).

Per la periodicità di f, i poli sono esattamente tutti e soli i punti di L, incluso 0. Lo sviluppo in serie di Laurent di f in 0 conterrà solo termini di grado pari (per la parità di f) tra cui almeno uno di grado negativo:

$$f(z) = a_{-2n}z^{-2n} + a_{-2(n-1)}z^{-2(n-1)} + ..., \quad n \geq 1 \quad .$$

Sfruttando il noto sviluppo in serie di Laurent di $\wp$ (eq. (1.5)) dato da

$$\wp(z) = z^{-2} + ... \quad ,$$

definiamo

$$g(z) = f(z) - a_{-2n} \cdot (\wp(z))^n \ .$$

Osserviamo che g è una funzione ellittica pari con tutti i poli contenuti nel reticolo L. Possiamo dunque induttivamente eliminare tutti i termini con grado negativo dalla parte principale di f così da ottenere una funzione ellittica senza poli che sarà quindi costante. □

Sospendiamo ora l'ipotesi restrittiva secondo la quale i poli sono contenuti nel reticolo.

Proposizione 1.4.15. *Qualsiasi funzione ellittica pari è rappresentabile come funzione razionale in $\wp$.*
In altre parole, il campo delle funzioni ellittiche pari associate a un reticolo L equivale al campo $\mathbb{C}(\wp)$ ed è quindi isomorfo al campo delle funzioni razionali $\mathbb{C}(z)$.

Dimostrazione. Cerchiamo di ricondurci al caso particolare precedentemente affrontato. Sia f una funzione ellittica pari non costante associata al reticolo L. Se a è un polo di f che non appartiene a L, allora $\wp(a)$ è un valore in $\mathbb{C}$ e possiamo definire la funzione ellittica

$$z \mapsto (\wp(z) - \wp(a))^N \cdot f(z)$$

che, se prendiamo N sufficientemente grande, ha una singolarità rimovibile in a .

Denotiamo

$$\{a_1, ..., a_m\}$$

l'insieme dei poli di f, modulo L , non congrui a 0 modulo L.

Induttivamente possiamo considerare $N_1, ..., N_m$ sufficientemente grandi in modo che la funzione ellittica

$$g(z) = f(z) \cdot \prod_{i=1}^{m} (\wp(z) - \wp(a_i))^{N_i}$$

abbia poli solo in L.

Segue che, per il Lemma 1.4.14, la funzione g può essere espressa come polinomio in $\wp$ e dunque concludiamo. □

Studiamo ora le funzioni ellittiche dispari per poi giungere a un risultato generale.

Proposizione 1.4.16. *Ogni funzione ellittica dispari si può scrivere come prodotto di una funzione ellittica pari con $\wp'$*

Dimostrazione. Poiché il quoziente di due funzioni dispari è pari, se consideriamo una funzione ellittica dispari f otteniamo che

$$g = \frac{f}{\wp'}$$

è una funzione ellittica pari. La tesi segue direttamente. □

Ora che abbiamo caratterizzato le funzioni ellittiche, sia pari che dispari, possiamo enunciare il seguente risultato generale.

Teorema 1.4.17. *Sia $f \in K(L)$. Allora esistono funzioni razionali R e S tali che*

$$f = R(\wp) + \wp' \cdot S(\wp) \ ,$$

cioè

$$K(L) = \mathbb{C}(\wp) + \wp' \cdot \mathbb{C}(\wp) = \mathbb{C}[\wp, \wp'] \ .$$

Dunque $K(L)$ è uno spazio vettoriale di dimensione 2 sul campo $\mathbb{C}(\wp)$.

Dimostrazione. Osserviamo che, se $z \mapsto f(z)$ è ellittica, allora anche $z \mapsto f(-z)$ lo è. Quindi ogni funzione si scrive come somma di una funzione ellittica pari e una dispari:

$$f(z) = \frac{1}{2}(f(z) + f(-z)) + \frac{1}{2}(f(z) - f(-z)) \ .$$

Unendo i risultati della Proposizione 1.4.15 e della Proposizione 1.4.16, otteniamo la tesi. □

Questo teorema mostra quindi, come avevamo preannunciato, che le funzioni $\wp$ e $\wp'$ sono sufficienti a generare l'intero campo $K(L)$.

Osservazione 1.4.18. Il campo $K(L)$ è un'estensione di $\mathbb{C}(\wp)$ di grado 2 di un campo razionale.

A questo punto risulta naturale chiedersi quale sia la relazione che lega $\wp$ e $\wp'$. Iniziamo col mostrare come può essere scritta $(\wp')^2$ come polinomio in $\wp$. Vedremo che questo passaggio è proprio ciò che ci permetterà di giungere all'equazione algebrica di $\wp$ cercata.

Esempio 1.4.1 ($(\wp')^2$ **come polinomio in** $\wp$)**.** Sfruttiamo gli stessi ragionamenti delle dimostrazioni precedenti.

$$\wp(z) = z^{-2} + 3 \cdot G_4 \cdot z^2 + 5 \cdot G_6 \cdot z^4 + ... \tag{1.7}$$

$$\Rightarrow \wp'(z) = -2 \cdot z^{-3} + 6 \cdot G_4 \cdot z + 20 \cdot G_6 \cdot z^3 + ... \tag{1.8}$$

$$\Rightarrow (\wp'(z))^2 = 4 \cdot z^{-6} - 24 \cdot G_4 \cdot z^{-2} - 80 \cdot G_6 + ... \tag{1.9}$$

vogliamo quindi eliminare il termine con z^{-6} e quello con z^{-2} dall'eq. (1.9).
Calcoliamo potenze di $\wp$ fino a quando ci servono (grado 3) a partire dall'eq. (1.7):

$$(\wp(z))^2 = z^{-4} + 6 \cdot G_4 + 10 \cdot G_6 \cdot z^2 + ... \tag{1.10}$$

$$\begin{aligned}(\wp(z))^3 &= z^{-6} + (3G_4 + 6G_4) \cdot z^{-2} + (10G_6 + 5G_6) + ... \\ &= z^{-6} + 9 \cdot G_4 \cdot z^{-2} + 15 \cdot G_6 + ...\end{aligned} \tag{1.11}$$

Unendo l'eq. (1.9) e l'eq. (1.11) otteniamo:

$$(\wp'(z))^2 - 4(\wp(z))^3 = -60 \cdot G_4 \cdot z^{-2} - 140 \cdot G_6 + ... \tag{1.12}$$

$$\Rightarrow (\wp'(z))^2 - 4(\wp(z))^3 + 60 \cdot G_4 \cdot \wp(z) = -140 \cdot G_6 + ... \tag{1.13}$$

che è una funzione ellittica senza poli e quindi è costante (in particolare i puntini sono 0).

Abbiamo dunque ottenuto che la scrittura di $(\wp')^2$ come polinomio in $\wp$ è:

$$(\wp')^2 = 4\wp^3 - 60 \cdot G_4 \cdot \wp - 140 \cdot G_6 \ . \tag{1.14}$$

Scriviamolo sotto forma di enunciato.

Teorema 1.4.19 (Equazione differenziale algebrica per $\wp$)**.** *Sia L un reticolo, allora la $\wp$ di Weierstrass ad esso associato verifica la seguente equazione differenziale algebrica*

$$(\wp'(z))^2 = 4 \cdot (\wp(z))^3 - g_2 \cdot \wp(z) - g_3 \tag{1.15}$$

dove

$$g_2 = g_2(L) = 60 \cdot G_4 = 60 \cdot \sum_{\omega \in L^*} \omega^{-4} \quad e \quad g_3 = g_3(L) = 140 \cdot G_6 = 140 \cdot \sum_{\omega \in L^*} \omega^{-6} \ .$$

Concludiamo osservando una proprietà particolarmente comoda dei coefficienti appena definiti, che risulterà molto utile nei capitoli successivi.

Osservazione 1.4.20. Per ogni $m \in \mathbb{C}^*$, si ha che

$$G_n(m\Lambda) = m^{-n} \cdot G_n(\Lambda)$$

e di conseguenza

$$g_2(m\Lambda) = m^{-4} \cdot g_2(\Lambda) \quad \text{e} \quad g_3(m\Lambda) = m^{-6} \cdot g_3(\Lambda) \ .$$

Capitolo 2

Curve ellittiche e tori complessi

In questo capitolo ci concentreremo sulle curve ellittiche e sul loro legame con i tori complessi: mostreremo che, di fatto, questi due oggetti sono intercambiabili. Questo risultato semplifica significativamente lo studio delle curve ellittiche e ci sarà particolarmente utile nel capitolo successivo, quando affronteremo le curve ellittiche da un punto di vista aritmetico.

Nella prima sezione, esibiremo formalmente la definizione di curve ellittiche e mostreremo come queste possano essere ridotte a una forma standard, più facile da trattare.

La seconda sezione, invece, esplora la corrispondenza tra curve ellittiche e tori complessi. Mostreremo, in particolare che è grazie alla funzione $\wp$ di Weierstrass, studiata nel capitolo analitico, che abbiamo la possibilità di associare a una curva ellittica un toro complesso e viceversa.

Adotteremo principalmente gli approcci di [BF09] e [DS05], ma ci serviremo anche di definizioni e risultati presenti in [Hat02], [Smi04] e [Har13].

2.1 Verso la definizione di curva ellittica

In questa sezione, dopo aver richiamato alcune nozioni di base di geometria algebrica, verranno finalmente introdotte le curve ellittiche, protagoniste di questa tesi.

2.1.1 Nozioni preliminari

Definizione 2.1.1. Una *varietà algebrica affine (complessa)* è il luogo degli zeri comuni di una famiglia di polinomi $\{F_i\}_{i\in I}$ in $\mathbb{C}[x_1, ..., x_n]$, ovvero:

$$V = \mathbb{V}(\{F_i\}_{i\in I}) \subset \mathbb{C}^n \ .$$

Definizione 2.1.2. Una *varietà algebrica proiettiva (complessa)* è il luogo degli zeri comuni di una famiglia di polinomi omogenei $\{F_i\}_{i\in I}$ in $\mathbb{C}[x_1, ..., x_{n+1}]$, ovvero:

$$V = \mathbb{V}(\{F_i\}_{i\in I}) \subset \mathbb{P}^n(\mathbb{C}) \ .$$

Definizione 2.1.3. La *dimensione di uno spazio topologico* X è l'estremo superiore di tutti gli interi n tali che esiste una successione $Z_0 \subset Z_1 \subset ... \subset Z_n$ di sottoinsiemi chiusi irriducibili di X, dove con *irriducibili* intendiamo sottoinsiemi che non possono essere espressi come un'unione propria di due sottoinsiemi chiusi.

Definizione 2.1.4. La *dimensione di una varietà algebrica* X è la dimensione di X come spazio topologico.

Definizione 2.1.5. Chiamiamo *curva algebrica* una varietà algebrica di dimensione 1.

Definizione 2.1.6. Diciamo che uno spazio topologico X è una *superficie topologica* se X è di Hausdorff, a base numerabile e tale che ogni punto ammette un intorno omeomorfo a un aperto di $\mathbb{R}^2$.

Definizione 2.1.7. Sia X una superficie topologica compatta e orientabile. Definiamo il *genere di* X come

$$g(X) = \frac{1}{2} rk(H_1(X, \mathbb{Z}))$$

dove, per il concetto di *rango del primo gruppo di omologia di* X *a coefficienti in* $\mathbb{Z}$, seguiamo la terminologia adottata da [Hat02].

Osservazione 2.1.1. La definizione precedente fornisce un intero bene definito. Infatti, per il teorema di Hurewicz, si ha che

$$H_1(X, \mathbb{Z}) \cong \pi_1(X)^{ab} \ ,$$

cioè il primo gruppo di omologia singolare a coefficienti in $\mathbb{Z}$ è isomorfo all'abelianizzato del gruppo fondamentale.

Dalla costruzione standard di una superficie compatta e orientabile si ottiene che X può essere realizzata identificando a coppie i lati di un poligono convesso con $4n$ lati (detto $4n$*-gono*), etichettati

$$a_1, b_1, a_1^{-1}, b_1^{-1} ... a_n, b_n, a_n^{-1}, b_n^{-1} \ .$$

Applicando il teorema di Van Kampen si ottiene che

$$\pi_1(X) = \langle a_1, b_1, ..., a_n, b_n \mid a_1 b_1 a_1^{-1} b_1^{-1} ... a_n b_n a_n^{-1} b_n^{-1} = 1 \rangle$$

e, abelianizzando, si ottiene che $\pi_1(X)^{ab} \cong \mathbb{Z}^{2n}$ e quindi è un gruppo abeliano libero di rango pari. Segue che anche $H_1(X, \mathbb{Z})$ lo è e dunque il genere g della Definizione 2.1.7 è effettivamente un intero e, in particolare, $g = n$.

Per approfondimenti riguardo questo tema rimandiamo alla sezione 2.A di [Hat02].

2.1.2 Definizione e riduzione a una forma standard

Disponiamo ora di tutti gli strumenti necessari per fornire una definizione formale di curva ellittica. In questa sottosezione osserveremo, in particolare, che possiamo concentrarci sullo studio di curve ellittiche viste come cubiche piane descritte da un'equazione specifica e dunque con una forma molto più semplice da studiare. Questo passaggio è fondamentale perché ci permetterà, nella sezione successiva, di sfruttare la $\wp$ di Weierstrass per raggiungere così l'obiettivo che ci eravamo posti all'inizio del capitolo.

Definizione 2.1.8. Una *curva ellittica* è una curva liscia proiettiva di genere 1.

Osservazione 2.1.2. Se guardiamo una curva ellittica X come una superficie topologica, questa è compatta e orientabile di genere $g = 1$. Questo implica, per l'Osservazione 2.1.1, che X è isomorfa a un quadrilatero con i lati identificati a coppie, cioè X è topologicamente un toro.

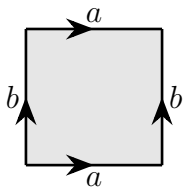


Figura 3: Rappresentazione del toro come quadrato con lati identificati

Proposizione 2.1.3. *Ogni curva ellittica è isomorfa a una cubica piana.*

La dimostrazione di questo risultato segue dal teorema di Riemann-Roch, per il quale si rinvia a [Har13].

Osservazione 2.1.4. Assumendo che X sia una curva ellittica già espressa come cubica piana, con un opportuno cambio di coordinate, ci si può ricondurre a una curva cubica piana della forma:

$$\tilde{X} = \tilde{X}(a_2, a_3) = \left\{[x : y : z] \in \mathbb{P}^2(\mathbb{C}) \mid zy^2 = 4x^3 - a_2z^2x - a_3z^3\right\}$$

per qualche $a_2, a_3 \in \mathbb{C}$.

Osservazione 2.1.5. Il polinomio

$$\tilde{P}(x, y, z) = zy^2 - 4x^3 + a_2z^2x + a_3z^3$$

è l'omogeneizzato di

$$P(x, y) = y^2 - 4x^3 + a_2x + a_3 \ .$$

Denotiamo dunque con

$$X_P = X(a_2, a_3) = \left\{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - a_2x - a_3\right\}$$

la curva affine associata a $\tilde{X}(a_2, a_3)$.

Nel prossimo esempio, cerchiamo di fornirne una visualizzazione in $\mathbb{R}$.

Esempio 2.1.1. Nelle figure seguenti viene rappresentata la curva

$$X(a_2, a_3) \cap \mathbb{R}^2 = \left\{(x, y) \in \mathbb{R}^2 : y^2 = 4x^3 - a_2x - a_3\right\}$$

per due scelte di $a_2, a_3 \in \mathbb{R}$.

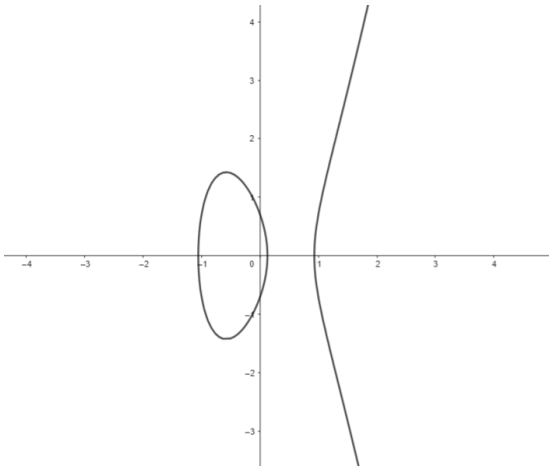


Figura 4: $y^2 = 4x^3 - 4x + 0.5$

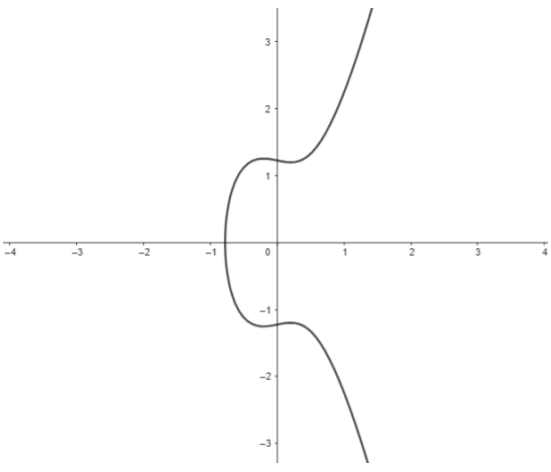


Figura 5: $y^2 = 4x^3 - 0.5x + 1.5$

2.2 Corrispondenza tra tori complessi e curve ellittiche

In questa sezione verrà mostrata concretamente la corrispondenza che c'è tra tori complessi e curve ellittiche, scritte nella forma semplice menzionata nell'Osservazione 2.1.4 e nell'Osservazione 2.1.5.

Per prima cosa, vedremo come costruire, tramite la $\wp$ di Weierstrass, una mappa olomorfa biettiva tra un toro complesso $\mathbb{C}/\Lambda$ e una curva ellittica del tipo $\tilde{X}(a_2, a_3)$, definita nella sezione scorsa.

Successivamente vedremo, non solo che da un toro complesso $\mathbb{C}/\Lambda$ possiamo ottenere una curva ellittica che soddisfa le equazioni

$$y^2 = 4x^3 - a_2x - a_3 \quad a_2 - 27a_3^2 \neq 0 \ , \tag{2.1}$$

ma vedremo anche che vale il viceversa.

2.2.1 Costruzione della biezione

Dall'equazione differenziale algebrica di $\wp$ (eq. (1.15)), deduciamo che per ogni $z \in \mathbb{C} \setminus \Lambda$ si ha che $(\wp(z), \wp'(z)) \in X(g_2, g_3)$, dove $g_2 = g_2(\Lambda)$ e $g_3 = g_3(\Lambda)$.
Questo ci fornisce la seguente mappa olomorfa tra varietà complesse

$$\phi\colon \begin{array}{c} \mathbb{C}/\Lambda \setminus \{[0]_\Lambda\} \longrightarrow X(g_2, g_3) \\ [z]_\Lambda \longmapsto (\wp(z), \wp'(z)) \ . \end{array}$$

Proposizione 2.2.1. *Tale mappa è biunivoca.*

Dimostrazione.

- Suriettività.
  Sia $(u, v) \in X(g_2, g_3)$ e consideriamo la $\wp$ di Weierstrass associata al reticolo Λ

  $$\wp\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{P}^1(\mathbb{C}) \ ,$$

  che è suriettiva per il Lemma 1.1.11. Quindi esiste $[z]_\Lambda \in \mathbb{C}/\Lambda$ tale che $\wp(z) = u$ e si ha:

  $$(u, v) = (\wp(z), v) \in X(g_2, g_3) \ ,$$

  quindi

  $$v^2 = 4 \cdot (\wp(z))^3 - g_2 \cdot \wp(z) - g_3 = (\wp'(z))^2$$
  $$\Rightarrow v^2 - (\wp'(z))^2 = 0 \Rightarrow (v - \wp'(z))(v + \wp'(z)) = 0 \Rightarrow \wp'(z) = \pm v.$$

Si hanno quindi due casi: se $(u, v) = (\wp(z), \wp'(z))$ allora $(u, v) = \phi([z]_\Lambda)$; altrimenti $(u, v) = (\wp(z), -\wp'(z)) = (\wp(-z), \wp'(-z))$, poiché $\wp$ è pari e $\wp'$ è dispari, e quindi $(u, v) = \phi([-z]_\Lambda)$.

- Iniettività.
  Siano $[z]_\Lambda, [w]_\Lambda \in \mathbb{C}/\Lambda \setminus \{[0]_\Lambda\}$ tali che $\phi([z]_\Lambda) = \phi([w]_\Lambda)$ cioè

$$\wp(z) = \wp(w) \quad \text{e} \quad \wp'(z) = \wp'(w).$$

  Per la Proposizione 1.3.4., $z \equiv \pm w \pmod{\Lambda}$, quindi:
  se $z \equiv w \pmod{L}$, allora $[z]_\Lambda = [w]_\Lambda \in \mathbb{C}/\Lambda \setminus \{[0]_\Lambda\}$;
  se invece $z \equiv -w \pmod{L}$, allora

$$\wp'(z) = \wp'(w) = \wp'(-z) = -\wp'(z) \Rightarrow \wp'(z) = 0$$

  e dunque, per il lemma 1.3.5. si ha

$$2z \in L \Rightarrow z \equiv -z \equiv w \pmod{\Lambda} \Rightarrow [z]_\Lambda = [w]_\Lambda \in \mathbb{C}/\Lambda \setminus \{[0]_\Lambda\}.$$

□

Abbiamo così mostrato che la curva affine $X(g_2, g_3)$ è in biezione con il toro privato di un punto $\mathbb{C}/\Lambda \setminus \{[0]_\Lambda\}$.

Osserviamo che possiamo estendere la funzione ϕ della Proposizione 2.2.1 in modo tale da ottenere la biezione tra la curva $\tilde{X}(g_2, g_3)$ e l'intero toro $\mathbb{C}/\Lambda$, menzionata all'inizio di questa sezione. Scriviamolo più precisamente sotto forma di enunciato.

Teorema 2.2.2. *Consideriamo la $\wp$ di Weierstrass associata al reticolo Λ.*
La mappa

$$\mathbb{C}/\Lambda \longrightarrow \tilde{X}(g_2, g_3) \subset \mathbb{P}^2(\mathbb{C})$$
$$[z] \longmapsto \begin{cases} [1 : \wp(z) : \wp'(z)], z \notin \Lambda \\ [0 : 0 : 1], z \in \Lambda \end{cases}$$

è una biezione.

2.2.2 La funzione discriminante

Abbiamo dunque verificato l'esistenza di una mappa olomorfa biettiva tra un toro complesso $\mathbb{C}/\Lambda$ e una curva ellittica del tipo $\tilde{X}(a_2, a_3)$.

Ricordiamo che l'obiettivo di questa sezione è mostrare come sia possibile ottenere, in modo concreto, a partire da un toro complesso $\mathbb{C}/\Lambda$, una curva ellittica che soddisfi le equazioni eq. (2.1), e viceversa. A tal fine, introdurremo, in questa sottosezione, la *funzione discriminante* e ne analizzeremo alcune proprietà, che risulteranno utili per concludere.

Definizione 2.2.1. Chiamiamo *funzione discriminante* la seguente:

$$\Delta : \begin{array}{l} \mathcal{H} \longrightarrow \mathbb{C} \\ \tau \longmapsto (g_2(\tau))^3 - 27 \cdot (g_3(\tau))^2 \ . \end{array}$$

Lemma 2.2.3. *La funzione Δ non è mai nulla in $\mathcal{H}$.*

Per dimostrarlo, abbiamo bisogno di introdurre la definizione di *discriminante di un polinomio di grado n.*

Definizione 2.2.2. Sia

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in \mathbb{C}[x]$$

un polinomio di grado n a coefficienti in $\mathbb{C}$ e siano $x_1, ..., x_n \in \mathbb{C}$ le sue radici. Definiamo il *discriminante di p* come:

$$a_n^{2n-2} \cdot \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \ .$$

Osservazione 2.2.4. Un polinomio di grado n a coefficienti in $\mathbb{C}$ ha radici distinte se e solo se il suo discriminante è non nullo.

Lemma 2.2.5. *Sia*

$$p(x) = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$$

un polinomio di grado 3 a coefficienti in $\mathbb{C}$. Allora il discriminante di p è dato dal numero complesso

$$18abcd - 4b^3 d + b^2 c^2 - 4ac^3 - 27a^2 d^2 \ .$$

Dimostrazione (del Lemma 2.2.5). Siano $x_1, x_2, x_3 \in \mathbb{C}$ le radici di p che riscriviamo come:

$$p(x) = a(x - x_1)(x - x_2)(x - x_3) \ .$$

Otteniamo dunque l'identità

$$ax^3 + bx^x + cx + d = a(x - x_1)(x - x_2)(x - x_3)$$

da cui deduciamo il seguente sistema di equazioni

$$\begin{cases} b = -a(x_1 + x_2 + x_3) \\ c = -a(x_1x_2 + x_1x_3 + x_2x_3) \\ d = -ax_1x_2x_3 \end{cases} \Rightarrow \begin{cases} -\frac{b}{a} = x_1 + x_2 + x_3 := C_1 \\ -\frac{c}{a} = x_1x_2 + x_1x_3 + x_2x_3 := C_2 \\ -\frac{d}{a} = x_1x_2x_3 := C_3 \end{cases} .$$

Dalla Definizione 2.2.2 si deduce che il discriminante di p è dato da

$$a^4(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 . \tag{2.2}$$

Svolgendo i calcoli esplicitamente, si mostra che possiamo riscrivere la quantità

$$k = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

in funzione di C_1, C_2 e C_3 , così da ottenere che

$$a^4k = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 .$$

□

Dimostrazione (del Lemma 2.2.3). Sia $\tau \in \mathcal{H}$ e denotiamo $p_\tau(x) = 4x^3 - g_2(\tau)x - g_3(\tau)$.

Osserviamo che $\Delta(\tau)$ è uguale al discriminante cubico di p_τ a meno di un multiplo scalare. Infatti, per il Lemma 2.2.5, si ha che il discriminante cubico di p_τ è dato da

$$18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 = 16(g_2(\tau))^3 - 16 \cdot 27(g_3(\tau))^2 = 16\Delta(\tau)$$

e quindi Δ si annulla in $\mathcal{H}$ se e solo se p_τ ha discriminante cubico nullo.

Dall'equazione algebrica della $\wp$ di Weierstrass (eq. (1.15)), si deduce che, per la Proposizione 1.4.9, possiamo riscrivere il polinomio p_τ come

$$4(x - a_1)(x - a_2)(x - a_3) .$$

Questo polinomio ha radici distinte (a_1, a_2 e a_3 sono distinti per la Proposizione 1.4.10) e dunque, per l'Osservazione 2.2.4, non può avere discriminante nullo. Segue che $\Delta(\tau) \neq 0$ per ogni $\tau \in \mathcal{H}$. □

2.2.3 Passaggio tra toro e curva ellittica

Abbiamo ora a disposizione tutte le basi per poter proseguire il discorso principale. Esplicitiamo la corrispondenza in entrambe le direzioni: da toro a curva ellittica e viceversa.

Con il seguente corollario, mostriamo come da un toro complesso $\mathbb{C}/\Lambda$ possiamo passare a una curva ellittica data dalle eq. (2.1).

Corollario 2.2.6. *Sia $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ un reticolo. Allora la curva $X = X(a_2, a_3)$ (con $a_2 = g_2(\Lambda)$ e $a_3 = g_3(\Lambda)$) verifica la condizione di liscezza*

$$a_2^3 - 27a_3^2 \neq 0\,.$$

Cioè, dal toro complesso $\mathbb{C}/\Lambda$ possiamo passare a una curva ellittica che verifica le eq. (2.1).

Dimostrazione. Sia $\tau = \frac{\omega_2}{\omega_1}$ e osserviamo che

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \omega_1(\mathbb{Z} + \tau\mathbb{Z}) = \omega_1 \cdot \Lambda_\tau\ .$$

Per l'Osservazione 1.4.20, si ha

$$\begin{aligned} g_2(\Lambda) &= \omega_1^{-4} \cdot g_2(\tau) \\ g_3(\Lambda) &= \omega_1^{-6} \cdot g_3(\tau)\ . \end{aligned}$$

Perciò

$$(g_2(\Lambda))^3 - 27 \cdot (g_3(\Lambda))^2 = \omega_1^{-12} \cdot ((g_2(\tau))^3 - 27 \cdot (g_3(\tau))^2) = \omega_1^{-12} \cdot \Delta(\tau).$$

che è diverso da 0 per il Lemma 2.2.3. □

Osservazione 2.2.7. Abbiamo chiamato

$$a_2^3 - 27a_3^2 \neq 0$$

condizione di liscezza in quanto è proprio grazie ad essa che si può verificare, calcolando le derivate rispetto a x e y del polinomio P definito nell'Osservazione 2.1.5, che la curva $X(a_2, a_3)$ è effettivamente non singolare, cioè liscia.

Definiamo e studiamo ora qualche proprietà di un'altra importante funzione, che ci sarà utile sia nel discorso corrente sia nello studio delle forme modulari nei capitoli successivi.

Definizione 2.2.3. Chiamiamo *funzione modulare* la seguente:

$$\begin{aligned} j\ :\ \mathcal{H} &\longrightarrow \mathbb{C} \\ \tau &\longmapsto 1728 \cdot \frac{(g_2(\tau))^3}{\Delta(\tau)}\ . \end{aligned}$$

Proposizione 2.2.8. *La funzione modulare j:*

1. *È olomorfa.*
2. *È suriettiva.*

Dimostrazione.

1. Segue dal fatto che il Lemma 2.2.3 garantisce che $j(\tau)$ abbia denominatore non nullo per ogni $\tau \in \mathcal{H}$.

2. Si dimostra assumendo per assurdo che esista un elemento $c \in \mathbb{C}$ tale che $j(\tau)$ è diverso da c per ogni $\tau \in \mathcal{H}$.
   Consideriamo
   $$\frac{1}{2\pi i}\int_\gamma \frac{j'(\tau)}{j(\tau)-c}d\tau \ ,$$
   scegliendo γ in modo tale che il Principio dell'argomento garantisca che quell'integrale sia nullo. Sfruttando l'invarianza di j per le trasformazioni $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ e $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ e sfruttando il suo sviluppo
   $$j(\tau) = \frac{1}{q} + ...$$
   (dove $q = e^{2\pi i \tau}$), si arriva a mostrare che tale integrale è non nullo. Questo contraddice quando detto precedentemente.
   Per maggiori dettagli si veda la sezione 1.1. di [DS05].

□

Con la seguente proposizione, mostriamo come passare da una curva ellittica data dalle eq. (2.1) a un toro complesso.

Proposizione 2.2.9. *Sia $X(a_2, a_3)$ una curva che soddisfa la condizione di liscezza*

$$a_2^3 - 27a_3^2 \neq 0 \ .$$

Allora esiste un reticolo Λ tale che $a_2 = g_2(\Lambda)$ e $a_3 = g_3(\Lambda)$.
Cioè, da una curva ellittica che verifica le eq. (2.1) *possiamo passare a un toro complesso* $\mathbb{C}/\Lambda$.

Dimostrazione.

- Caso $a_2 = 0$.
  Consideriamo $\mu_N := e^{\frac{2\pi i}{N}}$ una qualsiasi radice N-esima dell'unità e osserviamo che $\mu_N \Lambda_{\mu_N} = \Lambda_{\mu_N}$. Per semplicità di notazione, chiamiamo $\Lambda_{\mu_N} = L$.
  Abbiamo visto che, per n dispari, $G_n(L)$ è nullo; mentre, per n pari, abbiamo
  $$G_n(L) = \sum_{\lambda \in L^*} \frac{1}{\lambda^n} = \sum_{\lambda \in \mu_N L^*} \frac{1}{\lambda^n} = \sum_{\mu_N \sigma \in \mu_N L^*} \frac{1}{(\mu_N \sigma)^n} = \mu_N^{-n} \sum_{\sigma \in L^*} \frac{1}{\sigma^n} = \mu_N^{-n} \cdot G_n(L) \ ,$$

quindi si ha

$$(1 - \mu_N^{-n}) \cdot G_n(L) = 0 \ .$$

Il reticolo Λ che stiamo cercando deve soddisfare la condizione

$$g_2(\Lambda) = a_2 = 0 \ ,$$

ma per definizione

$$g_2(\Lambda) = 60 \cdot G_4(\Lambda)$$

si annulla se e solo se $G_4(\Lambda)$ si annulla. Per quanto detto in precedenza, avremmo bisogno di un reticolo $\Lambda = \Lambda_{\mu_N}$ tale che $\mu_N^{-4} \neq 1$.

Inoltre, la condizione nelle ipotesi della proposizione

$$a_2^3 - 27a_3^2 \neq 0$$

viene verificata soltanto se $a_3 \neq 0$, quindi il reticolo cercato Λ deve anche essere tale che $g_3(\Lambda)$ non si annulli. Ma per definizione

$$g_3(\Lambda) = 140 \cdot G_6(\Lambda)$$

è non nullo se e solo se $G_6(\Lambda)$ è non nullo. Dunque, sempre per quanto detto in precedenza, ci servirebbe un reticolo $\Lambda = \Lambda_{\mu_N}$ tale che $\mu_N^{-6} = 1$.

Prendendo $N = 3$, si verificano le due condizioni desiderate. Infatti, $\mu_3^{-4} = \mu_3^2 \neq 1$ mentre $\mu_3^{-6} = (\mu_3^3)^2 = 1$. Prendiamo dunque il reticolo

$$\Lambda = m\Lambda_{\mu_3}$$

con m un qualche numero complesso. Si ha che

$$\begin{aligned} g_2(\Lambda) &= m^{-4} g_2(\Lambda_3) = 0 = a_2 \ ; \\ g_3(\Lambda) &= m^{-6} g_3(\Lambda_{\mu_3}) \ . \end{aligned}$$

Scegliendo quindi m tale che

$$m^{-6} = \frac{a_3}{g_3(\Lambda_{\mu_3})} \ ,$$

otteniamo il reticolo cercato.

- Caso $a_3 = 0$.
  Ragionando analogamente si dimostra che il reticolo cercato in questo caso è

$$\Lambda = m\Lambda_{\mu_4} = m\Lambda_i$$

dove m è un numero complesso tale che

$$m^{-4} = \frac{a_2}{g_2(\Lambda_i)} \ .$$

- Caso $a_2, a_3 \neq 0$.
  Poiché la funzione modulare $j\colon \mathcal{H} \longrightarrow \mathbb{C}$ è suriettiva per la Proposizione 2.2.8, si ha che:
  $$\exists\, \tau \in \mathcal{H} : \quad j(\tau) = 1728 \cdot \frac{a_2^3}{a_2^3 - 27a_3^2} \in \mathbb{C}.$$
  Segue che
  $$j(\tau) = 1728 \cdot \frac{(g_2(\tau))^3}{\Delta(\tau)} = 1728 \cdot \frac{(g_2(\tau))^3}{(g_2(\tau))^3 - 27(g_3(\tau))^2} \ ,$$
  e quindi vale l'uguaglianza:
  $$\begin{aligned} 1728 \cdot \frac{a_2^3}{a_2^3 - 27a_3^2} &= 1728 \cdot \frac{(g_2(\tau))^3}{(g_2(\tau))^3 - 27(g_3(\tau))^2} \\ \Rightarrow \frac{a_2^3 - 27a_3^2}{a_2^3} &= \frac{(g_2(\tau))^3 - 27 \cdot (g_3(\tau))^2}{(g_2(\tau))^3} \\ \Rightarrow 1 - 27 \cdot \frac{a_3^2}{a_2^3} &= 1 - 27 \cdot \frac{(g_3(\tau))^2}{(g_2(\tau))^3} \\ \Rightarrow \frac{a_2^3}{(g_2(\tau))^3} &= \frac{a_3^2}{(g_2(\tau))^3} \ . \end{aligned}$$
  Preso $\omega_1 \in \mathbb{C}^*$, chiamiamo $\omega_2 = \tau \cdot \omega_1$ e consideriamo $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \omega_1\Lambda_\tau$.
  Per l'Osservazione 1.4.20, si ha che
  $$g_2(\Lambda) = \omega_1^{-4} g_2(\tau) \quad \text{e} \quad g_3(\Lambda) = \omega_1^{-6} g_3(\tau) \ .$$
  Quindi, scegliendo $\omega_1 \in \mathbb{C}^*$ tale che
  $$\omega_1^{-4} = \frac{a_2}{g_2(\tau)} \ ,$$
  otteniamo che
  $$(\omega_1^{-4})^3 = \frac{a_3^2}{(g_3(\tau))^2} \Rightarrow \omega_1^{-6} = \pm \frac{a_3}{g_2(\tau)} \ .$$
  Dunque, a meno di prendere $i \cdot \omega_1$ invece che ω_1, otteniamo che:
  $$g_2(\Lambda) = a_2 \quad \text{e} \quad g_3(\Lambda) = a_3 \ .$$

□

Possiamo quindi concludere che *i tori complessi (superfici di Riemann, oggetti analitici) e le curve ellittiche (soluzioni di polinomi cubici, oggetti algebrici) sono equivalenti.*

Capitolo 3

Strutture modulari delle curve ellittiche

In questo capitolo adotteremo un approccio di tipo aritmetico allo studio delle curve ellittiche.

Il risultato centrale, da questo punto di vista, è il teorema di modularità, il quale afferma che ad ogni curva ellittica definita su $\mathbb{Q}$ è associata una forma modulare. Come anticipato nell'introduzione, poiché in questa tesi ci occupiamo solo di curve ellittiche definite su $\mathbb{C}$, ci concentreremo su una versione meno forte del teorema. Ne enunceremo dunque la versione complessa: ogni curva ellittica, definita su $\mathbb{C}$, con invariante modulare razionale, proviene da una curva modulare. Sarà quindi necessario chiarire cosa intendiamo con *curva modulare* e con *invariante modulare*.

Per farlo, per prima cosa introdurremo il concetto di *forma modulare*, inizialmente definita rispetto al gruppo modulare $SL_2(\mathbb{Z})$. Osserveremo, però, che questa definizione risulta piuttosto restrittiva e ci chiederemo quindi se sia possibile estenderla a sottogruppi particolari di $SL_2(\mathbb{Z})$. Mostreremo che è effettivamente così e che questi sottogruppi prendono il nome di *sottogruppi di congruenza*.

Una volta introdotti e studiati questi oggetti fondamentali, potremo definire, nella terza sezione, le *curve modulari* come quozienti del semipiano $\mathcal{H}$ rispetto a tali sottogruppi.

Mostreremo poi un risultato fondamentale: le curve modulari sono in corrispondenza biunivoca con gli *spazi di parametri di curve ellittiche potenziate*, di cui forniremo una definizione formale. In termini intuitivi, ciò significa che i punti di una curva modulare parametrizzano curve ellittiche potenziate. Questa corrispondenza ci fornirà l'intuizione chiave per enunciare il teorema di modularità in forma complessa.

Per gran parte della trattazione di questo capitolo seguiremo l'approccio esposto in [DS05].

3.1 Forme modulari

Questa sezione è dedicata allo studio delle forme modulari.

Dopo aver richiamato alcune nozioni preliminari e aver illustrato che cosa significa per una funzione essere debolmente modulare, introdurremo una definizione formale di forma modulare rispetto a $SL_2(\mathbb{Z})$, cercando di motivare in maniera completa perché richiediamo determinate condizioni.

Concluderemo presentando alcuni esempi significativi e alcune osservazioni utili.

Fissiamo una notazione che ricorrerà in questa sezione e nelle prossime.

Notazione 3.1.1. Indichiamo il disco unitario nel piano complesso con

$$\mathbb{D} = \{q \in \mathbb{C} : |q| < 1\} \ .$$

3.1.1 Funzioni debolmente modulari

In questa sottosezione introduciamo il concetto di funzione debolmente modulare, che rappresenterà la prima condizione che richiederemo nella definizione di forma modulare.

Inizieremo richiamando il gruppo modulare $SL_2(\mathbb{Z})$ e descrivendo alcune sue proprietà, che saranno necessarie per le sezioni successive.

Ricordiamo che, per l'Osservazione 1.2.5, gli elementi di $SL_2(\mathbb{Z})$ sono trasformazioni di Möbius.

Osservazione 3.1.1.

- $SL_2(\mathbb{Z})$ è generato dalle trasformazioni

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1 \ , \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : \tau \mapsto -\frac{1}{\tau} \ .$$

- Gli elementi $\pm\alpha \in SL_2(\mathbb{Z})$ corrispondono alla stessa trasformazione. Questo perché se $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, si ha che

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \tau \mapsto \frac{a\tau + b}{c\tau + d} = \frac{-a\tau - b}{-c\tau - d} \hookleftarrow \tau : \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} = -\alpha$$

- Per $\alpha \in SL_2(\mathbb{Z})$ e $\tau \in \mathcal{H}$, vale la formula:

$$\Im(\alpha(\tau)) = \frac{\Im(\tau)}{|c\tau + d|^2} .$$

Definizione 3.1.1. Sia $k \in \mathbb{Z}$. Una funzione meromorfa $f : \mathcal{H} \longrightarrow \mathbb{C}$ si dice *debolmente modulare di peso k* se per ogni $\alpha \in SL_2(\mathbb{Z})$ si ha che per ogni $\tau \in \mathcal{H}$ vale

$$f(\alpha(\tau)) = (c\tau + d)^k \cdot f(\tau) . \tag{3.1}$$

Nelle prossime sezioni, in particolare nel Corollario 3.2.7, mostreremo che, affinché f sia debolmente modulare di peso k, è sufficiente richiedere che:

$$f(\tau + 1) = f(\tau) \quad \text{e} \quad f\left(-\tfrac{1}{\tau}\right) = \tau^k \cdot f(\tau)$$

per ogni $\tau \in \mathcal{H}$.

Osservazione 3.1.2. Se f è una funzione debolmente modulare, allora per ogni $\alpha \in SL_2(\mathbb{Z})$ si ha che $\tau \mapsto f(\tau)$ e $\tau \mapsto f(\alpha(\tau))$ hanno gli stessi zeri e gli stessi poli.

Osservazione 3.1.3. La modularità debole di peso 0 è $SL_2(\mathbb{Z})$-invarianza.

Osservazione 3.1.4.
Sia $f\colon \mathcal{H} \longrightarrow \mathbb{C}$ una funzione meromorfa tale che il differenziale $f(\tau)d\tau$ è $SL_2(\mathbb{Z})$-invariante. Allora f è debolmente modulare di peso 2.

Dimostrazione. L'ipotesi di $SL_2(\mathbb{Z})$-invarianza significa che, per $\tau \in \mathcal{H}$ e $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ vale:

$$f(\tau)d\tau = f(\alpha(\tau))d(\alpha(\tau)) . \tag{3.2}$$

Osserviamo inoltre che

$$d(\alpha(\tau)) = (c\tau + d)^{-2}d\tau . \tag{3.3}$$

Unendo l'eq. (3.3) e l'eq. (3.2), si ottiene che

$$f(\alpha(\tau)) = (c\tau + d)^2 f(\tau) .$$

□

Ci siamo soffermati su funzioni debolmente modulari di peso 2 non a caso: queste sono particolarmente rilevanti in quanto permettono di costruire funzioni debolmente modulari di peso $k > 2$ con k pari anche molto alto.

Infatti, se f e g sono due funzioni debolmente modulari di peso 2, il loro prodotto $f \cdot g$ è debolmente modulare di peso 4 e così via.

A questo punto è naturale chiedersi quale sia il comportamento delle funzioni debolmente modulari di peso dispari.

Osservazione 3.1.5. Se f è una funzione debolmente modulare di peso k e k è dispari, allora f è identicamente nulla.

Dimostrazione. Per definizione, si ha che per ogni $\alpha \in SL_2(\mathbb{Z})$ vale l'eq. (3.1). In particolare vale per $\alpha = -I$ e quindi

$$f = (-1)^k I = -f \ ,$$

da cui segue che $f \equiv 0$. □

Osservazione 3.1.6. Le funzioni debolmente modulari sono $\mathbb{Z}$-periodiche.

Dimostrazione. Segue dal fatto che, applicando l'eq. (3.1) alla traslazione in $SL_2(\mathbb{Z})$ data dalla matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1$, si ottiene che

$$f(\tau + 1) = f(\tau) \ .$$

□

3.1.2 Verso la definizione di forme modulari

Come anticipato, in questa sottosezione forniamo la definizione di forma modulare. Considereremo, innanzi tutto, funzioni debolmente modulari e richiederemo, oltre all'olomorfia su $\mathcal{H}$, la cosiddetta *olomorfia all'* ∞. Spiegheremo subito, nel dettaglio, il significato di questa condizione.

Sia $f \colon \mathcal{H} \longrightarrow \mathbb{C}$ una funzione debolmente modulare di peso $k \in \mathbb{Z}$. Indichiamo $q = e^{2\pi i \tau}$, per $\tau \in \mathcal{H}$.

Osserviamo che, poiché vale

$$|q| = e^{-2\pi \Im(\tau)} \ , \tag{3.4}$$

si ha che $q \in \mathbb{D}^*$.

Consideriamo quindi, associata ad f, la funzione

$$\begin{aligned} g\colon \mathbb{D}^* &\longrightarrow \mathbb{C} \\ q &\longmapsto f\left(\tfrac{log(q)}{2\pi i}\right) \end{aligned} \tag{3.5}$$

che, per la $2\pi i\mathbb{Z}$-periodicità del logaritmo e per l'Osservazione 3.1.6, è ben definita. Quindi, scrivendo f in termini di g, otteniamo che $f(\tau) = g(e^{2\pi i\tau})$.

Si osservi che, se f è olomorfa su $\mathcal{H}$, allora g è olomorfa su $\mathbb{D}^*$. L'eq. (3.4) mostra che, per $\Im(\tau) \to \infty$, si ha che $q \to 0$. Quindi possiamo dare la seguente definizione.

Definizione 3.1.2. Sia $f\colon \mathcal{H} \longrightarrow \mathbb{C}$ una funzione debolmente modulare e sia $g\colon \mathbb{D}^* \longrightarrow \mathbb{C}$ la funzione ad essa associata, come all'eq. (3.5). Supponiamo che ∞ sia un punto lontano sulla retta degli immaginari. Diciamo allora che f *è olomorfa all'* ∞ se g si estende olomorficamente in 0.

Osserviamo dunque che, per determinare l'*olomorfia di* f *all'* ∞, non è necessario calcolare esplicitamente il suo sviluppo in serie, ma è sufficiente mostrare che esiste il $\lim_{\Im(\tau)\to\infty} f(\tau)$ o anche che f è limitata per $\Im(\tau) \to \infty$.

Ora che abbiamo chiarito tutte le condizioni che richiediamo, possiamo fornire la seguente definizione.

Definizione 3.1.3. Sia $k \in \mathbb{Z}$. La funzione $f\colon \mathcal{H} \longrightarrow \mathbb{C}$ è una *forma modulare di peso* k se valgono le seguenti affermazioni:

1. f è olomorfa su $\mathcal{H}$;
2. f è debolmente modulare di peso k;
3. f è olomorfa all'∞.

3.1.3 Esempi e osservazioni

In questa sottosezione presentiamo alcuni esempi di forme modulari: uno semplice e due meno immediati. Mostreremo come da questi esempi segua l'invarianza della funzione modulare j, definita nella Definizione 2.2.3, rispetto alle trasformazioni di $SL_2(\mathbb{Z})$. È per questo motivo che, nelle sezioni successive, la chiameremo talvolta anche *invariante modulare*.

Esempio 3.1.1.

- $f \equiv 0$ è una forma modulare di peso k qualsiasi.
- Per ogni $c \in \mathbb{C}$, la funzione costante $f \equiv c$ è una forma modulare di peso 0.

Esempio 3.1.2.

Richiamiamo la *serie di Eisestein* definita nei capitoli precedenti (si veda l'eq. (1.5)):

$$G_k(\tau) = G_k(\Lambda_\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(c\tau+d)^k}$$

con $k > 2$ pari. Mostriamo che è una forma modulare di peso k.

Per il Lemma 1.4.1, la somma converge assolutamente e converge uniformemente sui compatti di $\mathcal{H}$. Segue che G_k è olomorfa su $\mathcal{H}$ (e quindi vale il punto 1 della Definizione 3.1.3) e possiamo riordinare i coefficienti della sommatoria.

Sia dunque $\alpha = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \in SL_2(\mathbb{Z})$ e calcoliamo:

$$G_k(\alpha(\tau)) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{\left(c\frac{\tilde{a}\tau+\tilde{b}}{\tilde{c}\tau+\tilde{d}} + d\right)^k} = (\tilde{c}\tau+\tilde{d})^k \cdot \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{((c\tilde{a}+d\tilde{c})\tau + c\tilde{b}+d\tilde{d})^k} \quad ;$$

si osservi che α è invertibile quindi

$$(c\tilde{a}+d\tilde{c}, c\tilde{b}+d\tilde{d}) = (c,d)\cdot\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \neq (0,0) \ .$$

Abbiamo perciò ottenuto che

$$G_k(\alpha(\tau)) = (\tilde{c}\tau+\tilde{d})^k \cdot G_k(\tau) \ ,$$

cioè G_k è debolmente modulare di peso k (e quindi vale il punto 2 della Definizione 3.1.3).

Infine, osserviamo che $G_k(\tau)$ è limitata per $\Im(\tau) \to \infty$ (per una motivazione precisa di questo, si veda la sezione 1.1 di [DS05]). Quindi, per il discorso precedente, G_k è olomorfa all'∞ (e quindi vale il punto 3 della Definizione 3.1.3).

Esempio 3.1.3. Mostriamo che la funzione discriminante Δ è una forma modulare di peso 12.

Dall'esempio precedente deduciamo che g_2 e g_3 sono olomorfi su $\mathcal{H}$ e di conseguenza lo

è anche Δ (e quindi vale il punto 1 della Definizione 3.1.3).

Sempre dall'esempio precedente, segue che g_2 è debolmente modulare di peso 4 e g_3 è debolmente modulare di peso 6. Dunque Δ è debolmente modulare di peso 12 (e quindi vale il punto 2 della Definizione 3.1.3).

Infine, guardando lo sviluppo in serie di Fourier di g_2 e g_3 si dimostra che per $\Im(\tau) \to \infty$ si ha che $\Delta(\tau) \to 0$ (e quindi vale vale il punto 3 della Definizione 3.1.3).

Osservazione 3.1.7.

1. La funzione modulare j è $SL_2(\mathbb{Z})$-invariante;
2. La funzione modulare j non è una forma modulare.

Dimostrazione.

1. Segue dal fatto che numeratore e denominatore sono funzioni debolmente modulari entrambe di peso 12 (si veda l'Esempio 3.1.2 e l'Esempio 3.1.3).
2. Segue dal fatto che j non verifica il punto 3 della Definizione 3.1.3 in quanto ha un polo in ∞ (per una dimostrazione formale di questo fatto si veda [DS05]).

□

Osservazione 3.1.8. Non esistono forme modulari non nulle di peso dispari.

Dimostrazione. Diretta conseguenza dell'Osservazione 3.1.5. □

Quanto appena osservato è proprio uno dei motivi per cui limitarsi a studiare forme modulari rispetto a $SL_2(\mathbb{Z})$ costituisce una restrizione piuttosto forte, come anticipato nell'introduzione di questo capitolo.

3.2 Sottogruppi di congruenza

In questa sezione introduciamo i *sottogruppi di congruenza*. Per prima cosa, forniremo la definizione e alcune osservazioni preliminari; successivamente presenteremo una generalizzazione della definizione vista nella sezione precedente, introducendo le *forme modulari rispetto a un sottogruppo di congruenza*. Questo permetterà di chiarire che i sottogruppi di congruenza non sono solamente un mezzo per definire, nella sezione successiva, le *curve modulari* e le *curve ellittiche potenziate*, ma sono anche strumenti utili ad approfondire lo studio delle forme modulari (su cui però non ci soffermeremo, essendo questo al di fuori dell'obiettivo principale della tesi), superando le restrizioni imposte dallo studio delle forme modulari su $SL_2(\mathbb{Z})$.

3.2.1 Definizioni e osservazioni fondamentali

Definizione 3.2.1. Sia $N \in \mathbb{N}^*$. Si dice *sottogruppo di congruenza principale di livello* N:

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\} .$$

Osservazione 3.2.1. $\Gamma(1) = SL_2(\mathbb{Z})$.

Dimostrazione. Per $N = 1$, la relazione

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{1}$$

è banale perché ogni numero è congruo a qualsiasi altro modulo 1. □

Questo caso base appena osservato ci aiuta a comprendere che ogni sottogruppo di congruenza di livello $N > 1$ sarà un sottogruppo proprio di $SL_2(\mathbb{Z})$. In particolare, all'aumentare di N, il sottogruppo si restringe, poiché le matrici devono essere sempre più vicine all'identità modulo N.

Osservazione 3.2.2. Consideriamo l'omomorfismo naturale

$$\begin{aligned} \varphi_1 \colon SL_2(\mathbb{Z}) &\longrightarrow SL_2(\mathbb{Z}_N) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix} \pmod{N} . \end{aligned}$$

Poiché $\Gamma(N) = \ker(\varphi_1)$, si ha che $\Gamma(N) \trianglelefteq SL_2(\mathbb{Z})$.

Inoltre, φ_1 è suriettiva (si veda [DS05]). Quindi, per il primo teorema di omomorfismo, otteniamo che

$$SL_2(\mathbb{Z})/\Gamma(N) \cong SL_2(\mathbb{Z}_N)$$

e quindi $[SL_2(\mathbb{Z}) : \Gamma(N)] < \infty$.

Definizione 3.2.2.
Un sottogruppo $\Gamma \leq SL_2(\mathbb{Z})$ è un *sottogruppo di congruenza (di livello N)* se

$$\Gamma(N) \subseteq \Gamma .$$

Osservazione 3.2.3. Sia $\Gamma \leq SL_2(\mathbb{Z})$ un sottogruppo di congruenza e sia $\alpha \in SL_2(\mathbb{Z})$. Allora $\alpha^{-1}\Gamma\alpha$ è un sottogruppo di congruenza.

Dimostrazione. Per definizione, esiste $N \in \mathbb{N}^*$ tale che $\Gamma(N) \subseteq \Gamma$. Sia dunque $\gamma \in \Gamma(N)$, cioè tale che $\gamma \cong I_2 \pmod N$. Quindi esiste una matrice $X \in M_2(\mathbb{Z})$ tale che $\gamma = I_2 + NX$. Osserviamo che

$$\Gamma \ni \alpha^{-1}\gamma\alpha = \alpha^{-1}I_2\alpha + \alpha^{-1}NX\alpha = I_2 + N(\alpha^{-1}X\alpha) \cong I_2 \pmod N$$

e dunque $\Gamma(N) \subseteq \alpha^{-1}\Gamma\alpha$. □

Definizione 3.2.3. Sia $N \in \mathbb{N}^*$. Oltre al sottogruppo principale, esistono altri due sottogruppi di congruenza di livello N particolarmente rilevanti:

- $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod N \right\}$;
- $\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod N \right\}$.

Vale dunque l'inclusione

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z}) \, .$$

Osservazione 3.2.4. Valgono le seguenti.

1. $\Gamma(N) \trianglelefteq \Gamma_1(N)$ e $\Gamma_1(N)/\Gamma(N) \cong \mathbb{Z}_N$.
2. $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$ e $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}_N)^*$.

Dimostrazione. Consideriamo le mappe

$$\begin{aligned} \varphi_2 \colon \Gamma_1(N) &\longrightarrow \mathbb{Z}_N \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto b \pmod N \end{aligned} \qquad \begin{aligned} \varphi_3 \colon \Gamma_0(N) &\longrightarrow (\mathbb{Z}_N)^* \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto d \pmod N \end{aligned}$$

Queste sono entrambe suriettive. Inoltre, si ha che $\ker(\varphi_2) = \Gamma(N)$ e $\ker(\varphi_3) = \Gamma_1(N)$; il risultato segue dal primo teorema di omomorfismo. Per ulteriori dettagli su questo argomento, si rinvia a [DS05].

□

Definizione 3.2.4. Sia $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ e sia $k \in \mathbb{Z}$.

- Si definisce il *fattore di automorfia* come
$$j(\alpha, \tau) = c\tau + d \in \mathbb{C} \, .$$
- Si definisce l'*operatore di peso k, denotato* $[\alpha]_k$, su una funzione $f \colon \mathcal{H} \longrightarrow \mathbb{C}$ ponendo, per ogni $\tau \in \mathcal{H}$,
$$(f[\alpha]_k)(\tau) = j(\alpha, \tau)^{-k} \, f(\alpha(\tau)) \, .$$

Osservazione 3.2.5. Dato che il fattore di automorfia non è mai nullo o ∞, se f è una funzione meromorfa allora $f[\alpha]_k$ è meromorfa ed ha gli stessi zeri e poli di f.

È quindi opportuno fornire la seguente definizione.

Definizione 3.2.5. Sia $\Gamma \leq SL_2(\mathbb{Z})$ un sottogruppo di congruenza. La funzione $f \colon \mathcal{H} \longrightarrow \mathbb{C}$ si dice *debolmente modulare di peso k rispetto a* Γ se è meromorfa e *invariante di peso k sotto* Γ, cioè se $f[\alpha]_k = f$ per ogni $\alpha \in \Gamma$.

Vediamo ora alcune proprietà di cui godono il fattore di automorfia e l'operatore di peso k, che risulteranno utili in seguito.

Lemma 3.2.6. *Per $\alpha, \alpha' \in SL_2(\mathbb{Z})$ e $\tau \in \mathcal{H}$, valgono le seguenti:*

1. $j(\alpha\alpha', \tau) = j(\alpha, \alpha'(\tau)) \cdot j(\alpha', \tau)$;
2. $(\alpha\alpha')(\tau) = \alpha(\alpha'(\tau))$;
3. $[\alpha\alpha']_k = [\alpha]_k[\alpha']_k$ *(intesa come uguaglianza di operatori);*
4. $\Im(\alpha(\tau)) = \dfrac{\Im(\tau)}{|j(\alpha.\tau)|^2}$;
5. $\dfrac{d\alpha(\tau)}{d\tau} = \dfrac{1}{j(\alpha, \tau)^2}$.

Per una dimostrazione di questo lemma, si veda [DS05], sezione 1.2.

Corollario 3.2.7. *Sia $f \colon \mathcal{H} \longrightarrow \mathbb{C}$ una funzione meromorfa. Se f verifica l'eq.* (3.1) *per le matrici $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ e $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ allora vale per ogni $\alpha \in SL_2(\mathbb{Z})$, cioè f è debolmente modulare di peso k.*

Dimostrazione. Dal punto 3 del Lemma 3.2.6 deduciamo che se f è debolmente modulare rispetto a un insieme di matrici, lo è anche rispetto al gruppo che esse generano. La tesi segue direttamente dal fatto che, per il primo punto dell'Osservazione 3.1.1, si ha che

$$SL_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle .$$

□

3.2.2 Forme modulari rispetto a sottogruppi di congruenza

Il nostro obiettivo ora è fornire una definizione completa di *forma modulare rispetto a un sottogruppo di congruenza.*

Ribadiamo che trattare queste particolari forme non è strettamente necessario per proseguire nello studio delle *curve modulari* e delle *curve ellittiche potenziate*, che definiremo nella sezione successiva, ma lo includiamo comunque per completezza. Come osservato precedentemente, infatti, limitarsi alle forme modulari per $SL_2(\mathbb{Z})$ risulta piuttosto restrittivo. Considerare invece quelle rispetto ai sottogruppi di congruenza è vantaggioso per diversi motivi: gli spazi associati a sottogruppi di congruenza sono più ricchi (per approfondimenti si veda [DS05]) e, se consideriamo un sottogruppo di congruenza $\Gamma \lneq SL_2(\mathbb{Z})$ con $I_2 \notin \Gamma$, è possibile definire forme modulari anche di peso dispari, cosa non consentita per $SL_2(\mathbb{Z})$ (si veda l'Osservazione 3.1.8).

Risulta naturale, per poter affermare che una funzione $f\colon \mathcal{H} \longrightarrow \mathbb{C}$ *è una forma modulare di peso k rispetto a un sottogruppo di congruenza* $\Gamma \leq SL_2(\mathbb{Z})$, richiedere che f sia olomorfa in $\mathcal{H}$ e debolmente modulare di peso k rispetto a Γ, così da avere coerenza con i punti 1 e 2 della Definizione 3.1.3. Richiederemo, inoltre, che f verifichi una particolare condizione di olomorfia che descriveremo di seguito.

Osserviamo che, dato che $\Gamma \supseteq \Gamma(N)$ per qualche $N \in \mathbb{N}^*$, si ha che Γ contiene necessariamente, per qualche $h \in \mathbb{N}^*$, una traslazione

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + h .$$

Si deduce quindi che, se f è debolmente modulare di peso k rispetto a Γ, allora è $h\mathbb{Z}$-periodica, cioè esiste

$$g\colon \mathbb{D}^* \longrightarrow \mathbb{C}$$

tale che $f(\tau) = g(q_h)$ dove $q_h = e^{\frac{2\pi i \tau}{h}}$.

Come visto nella sezione scorsa, abbiamo che, se f è olomorfa su $\mathcal{H}$, allora g è olomorfa su $\mathbb{D}^*$ e diciamo che f *è olomorfa in* ∞ se g si estende olomorficamente in $q = 0$.

Poiché siamo interessati a dare una definizione formale di forma modulare rispetto a un sottogruppo di congruenza $\Gamma \lneq SL_2(\mathbb{Z})$, è necessario fare particolarmente attenzione: vedremo, infatti, che in questo caso tra i punti limite non ci sarà solamente ∞, a differenza di quando stavamo considerando $\Gamma = SL_2(\mathbb{Z})$.

Per motivare questa affermazione, forniamo innanzi tutto la seguente definizione.

Definizione 3.2.6. Dato $\Gamma \leq SL_2(\mathbb{Z})$ un sottogruppo di congruenza, chiamiamo *cuspide di* Γ una classe di Γ-equivalenza di punti in $\mathbb{Q} \cup \infty$.

Osservazione 3.2.8. $\Gamma = SL_2(\mathbb{Z})$ ha una sola cuspide.

Dimostrazione. Dimostriamo che tutti i punti razionali sono in relazione d'equivalenza con ∞, tramite $SL_2(\mathbb{Z})$. Sia dunque $\frac{p}{q} \in \mathbb{Q}$ generico (assumiamo p e q coprimi).
Si ha che, per il Lemma di Bézout, esistono $s, r \in \mathbb{Z}$ tali che

$$ps - qr = 1$$

e quindi

$$\alpha = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in SL_2(\mathbb{Z}) \ .$$

Segue che

$$\alpha(\infty) = \lim_{y \to \infty} \frac{p(iy) + r}{q(iy) + s} = \frac{p}{q}$$

e quindi ∞ e $\frac{p}{q}$ sono $SL_2(\mathbb{Z})$-equivalenti. □

Quanto appena dimostrato motiva il fatto che, quando abbiamo definito le forme modulari rispetto a $SL_2(\mathbb{Z})$, è stato sufficiente richiedere l'olomorfia soltanto all'∞.

Nel caso preso in considerazione adesso, invece, ci saranno più cuspidi e quindi più punti limite in cui richiedere olomorfia.

Osservazione 3.2.9. Il numero di cuspidi di un sottogruppo di congruenza $\Gamma \lneq SL_2(\mathbb{Z})$ è finito.

Dimostrazione. Nella dimostrazione dell'Osservazione 3.2.8, abbiamo visto che per ogni $m \in \mathbb{Q}$ esiste $\alpha \in SL_2(\mathbb{Z})$ tale che $m = \alpha(\infty)$, quindi il numero di cuspidi di Γ sarà

al massimo pari al numero di classi laterali $\Gamma\alpha$ e cioè un numero finito in quanto, per l'Osservazione 3.2.2, si ha che

$$[SL_2(\mathbb{Z}) : \Gamma] < \infty \ .$$

□

Risulta naturale quindi, definire l'olomorfia in una cuspide $m = \alpha(\infty)$ in termini dell'olomorfia in ∞ dell'operatore $[\alpha]_k$. Questa era proprio la condizione di olomorfia che intendevamo definire all'inizio del discorso.

Tale richiesta ha senso poiché, se assumiamo f olomorfa, per l'Osservazione 3.2.5, anche $f[\alpha]_k$ è olomorfa. Inoltre tale operatore è debolmente modulare rispetto a $\alpha^{-1}\Gamma\alpha$, che è un sottogruppo di congruenza per l'Osservazione 3.2.3. Possiamo quindi finalmente definire le forme modulari rispetto a un sottogruppo di congruenza di $SL_2(\mathbb{Z})$.

Definizione 3.2.7. Sia $\Gamma \leq SL_2(\mathbb{Z})$ un sottogruppo di congruenza e sia $k \in \mathbb{Z}$. Diciamo che la funzione $f\colon \mathcal{H} \longrightarrow \mathbb{C}$ è una *forma modulare di peso k rispetto a* Γ se

1. f è olomorfa su $\mathcal{H}$;
2. f è debolmente modulare di peso k rispetto a Γ ;
3. $f[\alpha]_k$ è olomorfa in ∞ per ogni $\alpha \in SL_2(\mathbb{Z})$.

3.3 Curve ellittiche potenziate e curve modulari

In questa sezione ci concentreremo sulle *curve modulari* e sulle curve ellittiche dotate di una struttura di torsione fissata, che chiameremo *curve ellittiche potenziate*.

Inizieremo fornendo le definizioni precise di curve ellittiche potenziate e introducendo gli insiemi delle loro classi di isomorfismo, che chiameremo *spazi di parametri di curve ellittiche potenziate*. Successivamente, definiremo le *curve modulari* come quozienti di $\mathcal{H}$ per sottogruppi di congruenza, soffermandoci in particolare su quelle ottenute dai tre sottogruppi di congruenza più rilevanti definiti nella sezione precedente.

Nella seconda sottosezione verrà presentato un teorema fondamentale che stabilisce una biezione tra curve modulari e spazi di parametri di curve ellittiche potenziate.

Questo risultato ci consentirà, nell'ultima sottosezione, di enunciare il teorema di modularità in forma complessa.

Per semplificare la trattazione, introduciamo una nuova notazione per indicare gli elementi delle curve ellittiche.

Notazione 3.3.1. Nei capitoli precedenti, indicavamo gli elementi di un toro complesso con

$$[z]_\Lambda \in \mathbb{C}/\Lambda \ ,$$

poiché ancora non avevamo mostrato la corrispondenza che sussiste tra tori complessi e curve ellittiche; ci era quindi utile tenere traccia della classe di equivalenza data dal quoziente per il reticolo Λ. D'ora in avanti, invece, poiché denoteremo con E la curva ellittica che corrisponde al toro $\mathbb{C}/\Lambda$ e con E_τ la curva ellittica che corrisponde al toro $\mathbb{C}/\Lambda_\tau$, indicheremo gli elementi di tali curve (o equivalentemente tori) con

$$[z]_E \in E \quad \text{e} \quad [z]_{E_\tau} \in E_\tau \ .$$

3.3.1 Definizioni e considerazioni iniziali

Definizione 3.3.1. Sia $N \in \mathbb{N}^*$. Una *curva ellittica potenziata per* $\Gamma_0(N)$ è una coppia (E, C) dove E è una curva ellittica (complessa) e C è un sottogruppo ciclico di E di ordine N. Due curve ellittiche $(E, C), (E', C')$ potenziate per $\Gamma_0(N)$ si dicono *equivalenti* se esiste un isomorfismo

$$E \xrightarrow{\sim} E'$$

che manda C in C'. Indichiamo il quoziente per tale relazione con:

$$S_0(N) := \{\text{curve ellittiche potenziate per } \Gamma_0(N)\} / \sim \ ;.$$

Definizione 3.3.2. Sia $N \in \mathbb{N}^*$. Una *curva ellittica potenziata per* $\Gamma_1(N)$ è una coppia (E, Q) dove E è una curva ellittica (complessa) e $Q \in E$ è un *punto di ordine* N, cioè tale che $NQ = 0$ ma $nQ \neq 0$ per ogni $n < N$. L'equivalenza è definita analogamente a prima e, di nuovo, indichiamo il quoziente con:

$$S_1(N) := \{\text{curve ellittiche potenziate per } \Gamma_1(N)\} / \sim \ .$$

Definizione 3.3.3. Sia $N \in \mathbb{N}^*$. Una *curva ellittica potenziata per* $\Gamma(N)$ è una coppia $(E, (P, Q))$ dove E è una curva ellittica (complessa) e (P, Q) è una coppia di punti che genera il sottogruppo di torsione N-esima $\ker([N])$ con accoppiamento di Weil

$$e_N(P, Q) = e^{\frac{2\pi i}{N}} \ .$$

Due curve ellittiche $(E, (P, Q)), (E'(P', Q'))$ potenziate per $\Gamma(N)$ si dicono *equivalenti* se esiste un isomorfismo

$$E \xrightarrow{\sim} E'$$

che manda P in P' e Q in Q' . Denotiamo poi

$$S(N) := \{\text{curve ellittiche potenziate per } \Gamma(N)\} / \sim \quad .$$

Definizione 3.3.4. Chiamiamo $S_0(N)$, $S_1(N)$ e $S(N)$ *spazi di parametri di curve ellittiche potenziate*.

Osservazione 3.3.1. Gli spazi $S_0(N)$, $S_1(N)$ e $S(N)$ costituiscono un caso elementare di *spazi di moduli*, cioè insiemi che parametrizzano classi di isomorfismo di oggetti di tipo fissato. Infatti, ogni punto di $S_*(N)$ corrisponde a una classe di isomorfismo di curve ellittiche potenziate.

Osservazione 3.3.2.

$$S_0(1) = S_1(1) = S(1) = \{\text{classi di isomorfismo di curve ellittiche (complesse)}\} := \mathcal{S} \quad .$$

Definizione 3.3.5. Sia $\Gamma \leq SL_2(\mathbb{Z})$ un sottogruppo di congruenza che agisce su $\mathcal{H}$ da sinistra. Chiamiamo *curva modulare* lo spazio quoziente per le orbite di Γ:

$$Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau \mid \tau \in \mathcal{H}\} \ .$$

Denotiamo:

$$Y_0(N) = Y(\Gamma_0(N)) \ ; \ \ Y_1(N) = Y(\Gamma_1(N)) \ ; \ \ Y(N) = Y(\Gamma(N)) \ .$$

Osservazione 3.3.3.

$$Y_0(1) = Y_1(1) = Y(1) = SL_2(\mathbb{Z})\backslash\mathcal{H} \ .$$

Come preannunciato nell'Osservazione 1.2.6, vale la seguente identificazione.

Osservazione 3.3.4. La curva modulare $Y(1)$ può essere identificata con l'insieme

$$\mathcal{D} = \left\{\tau \in \mathcal{H} : |\Re(\tau) \leq \tfrac{1}{2}, |\tau| \geq 1\right\} \ .$$

detto *dominio fondamentale*, descritto nella fig. 6.

Dimostrazione. Sia $\tau \in \mathcal{H}$ e mostriamo che è $SL_2(\mathbb{Z})$-equivalente ad un qualche punto in $\mathcal{D}$. Applicando un numero finito di volte la trasformazione

$$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau \pm 1$$

otteniamo un elemento τ' nella striscia

$$\left\{\tau \in \mathcal{H} : |\Re(\tau)| \leq \tfrac{1}{2}\right\} .$$

Se $\tau' \notin \mathcal{D}$ significa che $|\tau'| < 1$ e quindi si ha

$$\Im\left(-\tfrac{1}{\tau'}\right) = \Im\left(-\tfrac{\overline{\tau'}}{|\tau'|^2}\right) = \Im\left(\tfrac{\tau'}{|\tau'|^2}\right) > \Im(\tau') .$$

Consideriamo dunque $-\frac{1}{\tau'} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\tau'$ e ripetiamo il procedimento. Poiché nel disco $\mathbb{D}$ ci sono solo un numero finito di punti appartenenti ad un reticolo, c'è un numero finito di coppie di interi (c, d) tali che $|c\tau' + d| < 1$. Si deduce che, per il punto 4 del Lemma 3.2.6, dopo un numero finito di trasformazioni di τ' otteniamo un elemento τ'' con parte immaginaria maggiore di 1. □

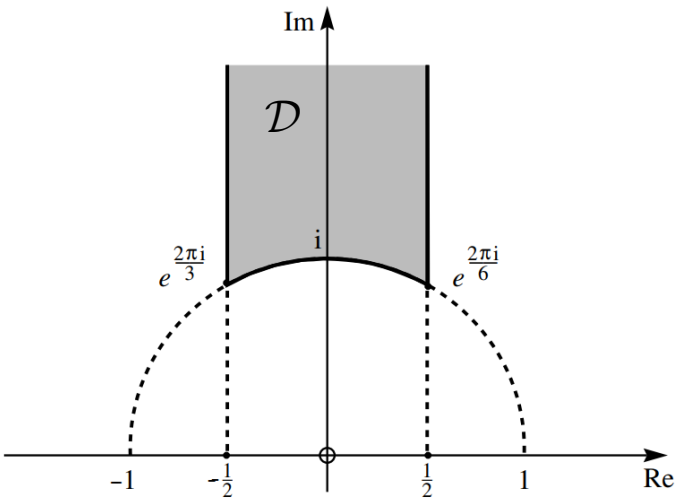


Figura 6: Dominio fondamentale

3.3.2 Corrispondenza tra curve modulari e spazi di parametri di curve ellittiche potenziate

In questa sottosezione vediamo il teorema che stabilisce la corrispondenza tra curve modulari e spazi di parametri di curve ellittiche potenziate. Questo risultato offre un'intuizione non banale: le curve modulari possono essere viste, non più soltanto come quozienti astratti del semipiano $\mathcal{H}$, ma come insiemi di punti corrispondenti a curve ellittiche potenziate.

Teorema 3.3.5. *Sia $N \in \mathbb{N}^*$. Valgono le seguenti affermazioni.*

1. *Lo spazio di parametri di curve ellittiche potenziate per $\Gamma_0(N)$ è dato da*

$$S_0(N) = \left\{ \left[E_\tau, \langle \left[\tfrac{1}{N}\right]_{E_\tau} \rangle \right] : \tau \in \mathcal{H} \right\} .$$

Inoltre, due punti $\left(E_\tau, \langle \left[\tfrac{1}{N}\right]_{E_\tau} \rangle\right)$ e $\left(E_{\tau'}, \langle \left[\tfrac{1}{N}\right]_{E_{\tau'}} \rangle\right)$ sono equivalenti se e solo se

$$\Gamma_0(N)\tau = \Gamma_0(N)\tau' .$$

Quindi c'è una biezione

$$\begin{aligned} \psi_0 \colon S_0(N) &\longrightarrow Y_0(N) \\ \left[E_\tau, \langle \left[\tfrac{1}{N}\right]_{E_\tau} \rangle\right] &\longmapsto \Gamma_0(N)\tau \end{aligned} .$$

2. *Lo spazio di parametri di curve ellittiche potenziate per $\Gamma_1(N)$ è dato da*

$$S_1(N) = \left\{ \left[E_\tau, \left[\tfrac{1}{N}\right]_{E_\tau} \right] : \tau \in \mathcal{H} \right\} .$$

Inoltre, due punti $\left(E_\tau, \left[\tfrac{1}{N}\right]_{E_\tau}\right)$ e $\left(E_{\tau'}, \left[\tfrac{1}{N}\right]_{E_{\tau'}}\right)$ sono equivalenti se e solo se

$$\Gamma_1(N)\tau = \Gamma_1(N)\tau' .$$

Quindi c'è una biezione

$$\begin{aligned} \psi_1 \colon S_1(N) &\longrightarrow Y_1(N) \\ \left[E_\tau, \left[\tfrac{1}{N}\right]_{E_\tau}\right] &\longmapsto \Gamma_1(N)\tau \end{aligned} .$$

3. *Lo spazio di parametri di curve ellittiche potenziate per $\Gamma(N)$ è dato da*

$$S(N) = \left\{ \left[E_\tau, \left(\left[\tfrac{\tau}{N}\right]_{E_\tau}, \left[\tfrac{1}{N}\right]_{E_\tau} \right) \right] : \tau \in \mathcal{H} \right\} .$$

Inoltre, due punti $\left(E_\tau, \left(\left[\tfrac{\tau}{N}\right]_{E_\tau}, \left[\tfrac{1}{N}\right]_{E_\tau} \right)\right)$ e $\left(E_{\tau'}, \left(\left[\tfrac{\tau'}{N}\right]_{E_{\tau'}}, \left[\tfrac{1}{N}\right]_{E_{\tau'}} \right)\right)$ sono equivalenti se e solo se

$$\Gamma(N)\tau = \Gamma(N)\tau' .$$

Quindi c'è una biezione

$$\begin{aligned} \psi \ : \ S(N) &\longrightarrow Y(N) \\ \left[E_\tau, \left(\left[\tfrac{\tau}{N}\right]_{E_\tau}, \left[\tfrac{1}{N}\right]_{E_\tau} \right)\right] &\longmapsto \Gamma(N)\tau \end{aligned} .$$

Dimostrazione. Dimostriamo il punto 1 dell'enunciato.

Sia $[E, C] \in S_0(N)$. Per l'Osservazione 1.2.9, si ha che esiste $\tau \in \mathcal{H}$ tale che $E \cong E_\tau$ tramite un certo isomorfismo ϕ. Chiamando $\tilde{C} = \phi(C)$ si ha che

$$[E, C] = [E_\tau\ , \tilde{C}]\ .$$

Per definizione, $C \leq E$ è un sottogruppo ciclico di ordine N ; di conseguenza, anche $\tilde{C} \leq E_\tau$ è ciclico di ordine N, quindi esiste un elemento $[P]_{E_\tau} \in E_\tau$ tale che $\tilde{C} = \langle [P]_{E_\tau} \rangle$. In particolare, esistono $a, b \in \mathbb{Z}$ primi tra loro tali che

$$[P]_{E_\tau} = \left[\tfrac{a}{N} + \tfrac{b}{N}\tau\right]_{E_\tau}\ .$$

Cerchiamo ora una matrice che ci permetta di cambiare base. Per il lemma di Bézout, esistono $x, y \in \mathbb{Z}$ tali che $ax + by = 1$. Considerando la matrice

$$M = \begin{pmatrix} a & -y \\ b & x \end{pmatrix} \in SL_2(\mathbb{Z})\ ,$$

si ottiene che $M(1, 0) = (a, b)$, quindi possiamo scegliere $\left[\frac{1}{N}\right]_{E_\tau}$ come generatore di $\tilde{C}$. Da ciò segue che

$$S_0(N) = \left\{ \left[E_\tau, \langle\ \left[\tfrac{1}{N}\right]_{E_\tau} \rangle\right] : \tau \in \mathcal{H} \right\}\ .$$

Siano ora

$$\left(E_\tau, \langle \left[\tfrac{1}{N}\right]_{E_\tau} \rangle\right) \sim \left(E_{\tau'}, \langle \left[\tfrac{1}{N}\right]_{E_{\tau'}} \rangle\right)\ .$$

Si ha, cioè, che esiste un isomorfismo tra le curve tale che

$$\langle \left[\tfrac{1}{N}\right]_{E_\tau} \rangle \overset{\cong}{\longmapsto} \langle \left[\tfrac{1}{N}\right]_{E_{\tau'}} \rangle$$

Per la Proposizione 1.2.7 e il Lemma 1.2.4 si ha che $E_\tau \cong E'_\tau$ se e solo se esiste $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ tale che $\tau' = \alpha(\tau)$. La condizione sull'immagine del sottogruppo fa sì che $c \equiv 0 \pmod N$ e quindi $\alpha \in \Gamma_0(N)$, cioè

$$\Gamma_0(N)\tau = \Gamma_0(N)\tau'\ .$$

I punti 2 e 3 si dimostrano con ragionamenti analoghi, per cui si rinvia alla sezione 1.5 di [DS05]. □

Osservazione 3.3.6. Questo teorema, applicato al caso $N = 1$, fornisce un'ulteriore dimostrazione di quanto avevamo già concluso, usando strumenti analitici, nei capitoli precedenti.

Infatti, dal Teorema 3.3.5 si deduce che l'insieme delle classi di isomorfismo di curve ellittiche $\mathcal{S}$ è in biezione con il quoziente $\mathcal{H}/SL_2(\mathbb{Z})$. Ma, per l'Osservazione 1.2.10, ogni toro complesso, o equivalentemente ogni curva ellittica, corrisponde, a meno di isomorfismo, a un elemento del semipiano $\mathcal{H}$, quozientato per l'azione di $SL_2(\mathbb{Z})$.

Per l'Osservazione 3.3.6, ogni classe di isomorfismo di curve ellittiche ha un'orbita $SL_2(\mathbb{Z})\tau \in SL_2(\mathbb{Z})\backslash\mathcal{H}$ ad essa associata e quindi ha un invariante ben definito $j(SL_2(\mathbb{Z})\tau)$.

Poiché tale valore è associato anche a ogni curva ellittica E nella classe di isomorfismo data da τ, possiamo denotarlo $j(E)$.

Dal Teorema 3.3.5 si deduce anche che le mappe tra curve modulari si traducono in mappe tra spazi di parametri di curve ellittiche potenziate.

Vediamo degli esempi per comprendere meglio questo fatto.

Esempio 3.3.1. La mappa

$$\begin{aligned} Y_1(N) &\longrightarrow Y_0(N) \\ \Gamma_1(N)\tau &\longmapsto \Gamma_0(N)\tau \end{aligned}$$

conduce alla mappa

$$\begin{aligned} S_1(N) &\longrightarrow S_0(N) \\ [E, Q] &\longmapsto [E, \langle Q \rangle] \end{aligned}$$

che dimentica il generatore, ricordando soltanto il gruppo che esso genera.

Esempio 3.3.2. Poiché, per l'Osservazione 3.2.4, si ha che $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$, il gruppo quoziente $\Gamma_0(N)/\Gamma_1(N)$ agisce sulla curva modulare $Y_1(N)$. Tale azione si traduce in un'azione sullo spazio di parametri $S_1(N)$ data da:

$$\begin{aligned} [\gamma] : S_1(N) &\longrightarrow S_1(N) \\ [E, Q] &\longmapsto [E, dQ] \ . \end{aligned}$$

dove $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

3.3.3 Teorema di modularità - versione complessa

Giungiamo ora al risultato più rilevante di questo capitolo aritmetico, ovvero il teorema di modularità in forma complessa, secondo cui le curve ellittiche con valori di j razionali provengono da curve modulari.

Prima di fornire l'enunciato preciso, però, è necessaria una puntualizzazione: le curve modulari possono essere compattificate aggiungendo le cuspidi del sottogruppo di congruenza alle quali sono associate.

Se Γ è un sottogruppo di congruenza e $Y(\Gamma)$ è la curva modulare ad esso associata, definiamo

$$X(\Gamma) := Y(\Gamma) \cup \{\text{cuspidi di } \Gamma\} \ .$$

Si ha quindi che la curva modulare compattificata associata al sottogruppo di congruenza Γ è data da

$$X(\Gamma) = Y(\Gamma) \cup \Gamma\backslash(\mathbb{Q} \cup \{\infty\}) = \Gamma\backslash\tilde{\mathcal{H}} \ ,$$

dove $\tilde{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Si può dimostrare che $X(\Gamma)$ è uno spazio effettivamente compatto ed è anche connesso e di Hassdorf, ma per questo si rinvia alla sezione 2.4 di [DS05].

Teorema 3.3.7. *Sia E una curva ellittica (complessa) con invariante modulare razionale, cioè tale che $j(E) \in \mathbb{Q}$. Allora esiste $N \in \mathbb{N}^*$ e esiste una mappa suriettiva olomorfa tra superfici compatte data da*

$$X_0(N) \longrightarrow E \ .$$

Bibliografia

[BF09] Rolf Busam e Eberhard Freitag. *Complex analysis*. Springer, 2009.

[DS05] Fred Diamond e Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[Har13] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002.

[Hus04] Dale Husemöller. *Elliptic curves*. Springer, 2004.

[Mil90] James S Milne. *Modular functions and modular forms*. Course Notes of the University of Michigan, Volume 8. 1990.

[Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces*. Vol. 5. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1995.

[Mod04] Giuseppe Modica. *Funzioni Olomorfe*. Dipartimento di Matematica, Università di Firenze. 2004.

[Neu13] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[Rot12] Joseph J Rotman. *An introduction to the theory of groups*. Vol. 148. Springer Science & Business Media, 2012.

[Sin] Jas Singh. *Complex Multiplication of Elliptic Curves and Class Field Theory*. 2022.

[Smi04] Karen Smith et al. *An invitation to algebraic geometry*. Springer Science & Business Media, 2004.

[SS10] Elias M Stein e Rami Shakarchi. *Complex analysis*. Vol. 2. Princeton University Press, 2010.

[Ste03] William Stein. *Finitely Generated Abelian Groups*. 2003.