lecture XXVII - add 3

ALGEBRAIC CURVES 4 RIEMANN SURFACES

Prof. M. Spera UCSC - Brescia

2.4. IL TEOREMA DI ADDIZIONE

Consideriamo la funzione

$$f(z) := \wp'(z) - a\wp(z) - b.$$

Tale funzione ha nell'origine un polo triplo[9] e deve quindi avere tre zeri. Due di questi zeri sono noti, e sono proprio z_1 e z_2 per costruzione. Ci sarà poi un ultimo zero, diciamo z_3, che per il teorema 2.5 deve essere tale che

$$z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda} \tag{2.13}$$

ovvero la somma dei tre zeri deve stare per forza su un punto del reticolo, cioè deve essere equivalente all'origine. Applicando $\wp$ a destra e a sinistra e ricordando la periodicità e la parità di $\wp$ otteniamo

$$\wp(z_3) = \wp(-z_1 - z_2) = \wp(z_1 + z_2). \tag{2.14}$$

Mettendo insieme le informazioni fornite dalla seconda delle (2.9) e da (2.14), abbiamo che

$$\wp(z_1 + z_2) = \wp(z_3) = -\wp(z_1) - \wp(z_2) + \frac{a^2}{4}. \tag{2.15}$$

Infine possiamo ricavare a in termini di $\wp(z)$ sottraendo tra loro le (2.12) ottenendo la formula di addizione:

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2$$

che è la stessa formula (1.6) ottenuta per via geometrico-algebrica nella sezione dedicata alla legge di gruppo.

Se poi $z := z_1 = z_2$ basterà prendere il limite per $z_1 \to z_2$ dell'espressione precedente, ottenendo la seguente formula di duplicazione

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

La parametrizzazione (2.11) mette in relazione biunivoca i punti del toro $\mathbb{C}/\Lambda$ con i punti della cubica ellittica $\mathcal{C} \in \mathbb{P}^2(\mathbb{C})$. Resta quindi definita una somma sul parallelogramma fondamentale $\mathcal{P}$, ereditata dalla somma geometrica su $\mathcal{C}$, e il modo di sommare due numeri è dato dal procedimento logico seguente: si prendono due numeri complessi $z_1, z_2 \in \mathcal{P}$, si calcola il rispettivo valore di $\wp, \wp'$ nei punti e si arriva tramite la parametrizzazione ai corrispondenti punti P_1, P_2 sulla cubica ellittica $\mathcal{C}$. A questo punto si sommano i punti

[9] Lo si capisce facilmente guardandone lo sviluppo in serie di Laurent.

tramite la legge di gruppo introdotta geometricamente e si ottiene un terzo punto P_3. Riportando indietro su $\mathcal{P}$ quest'ultimo punto otterremo il nostro punto somma $z_3 = z_1 + z_2$.

D'altra parte su $\mathbb{C}$ abbiamo anche un'altra somma: la somma standard tra numeri complessi, che in effetti rende $(\mathbb{C}, +)$ un gruppo commutativo. Queste due somme sono in realtà la stessa somma, e l'idea del motivo è data nella spiegazione che segue.

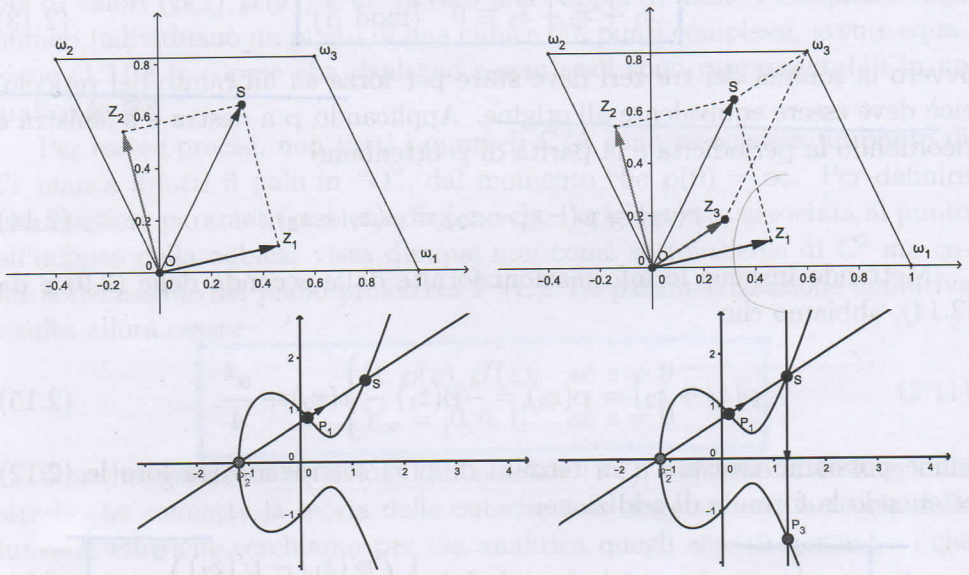

Figura 2.4: Somma di due punti sul toro $\mathcal{P}$ e sulla cubica $\mathcal{C}$.

Sappiamo bene che la somma canonica di $\mathbb{C}$ è caratterizzata dal fatto che per sommare due numeri complessi basta sommare tra loro parti reali e parti immaginarie, e graficamente ciò significa sommare due numeri come fossero due vettori di $\mathbb{R}^2$, cioè usando la regola del parallelogramma. Una volta sommati due numeri "vettorialmente", se il numero ottenuto esce da $\mathcal{P}$ dobbiamo considerare le sue coordinate *modulo* Λ, ovvero riportarle nel toro $\mathcal{P}$ nel modo naturale che siamo abituati a fare dalla Topologia. In questo modo abbiamo ristretto la somma canonica $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ a una funzione $\mathcal{P} \times \mathcal{P} \to \mathcal{P}$.

Dimostriamo ora che anche la somma indotta dalla cubica è fondata sulla regola del parallelogramma.

Iniziamo trovando l'opposto di un punto $z \in \mathcal{P}$. Tramite la parametrizzazione associamo a z il punto $P \in \mathcal{C}$ con $P = (\wp(z), \wp'(z))$. Otteniamo l'opposto cambiando segno alla coordinata y, cioè $-z$ sarà $(\wp(z), -\wp'(z)) = (\wp(-z), \wp'(-z))$, e quindi se ritorniamo in $\mathcal{P}$ con l'inversa della parametriz-

XXVII-add3-2

zazione andiamo proprio nel punto $-z$. Quindi fare l'opposto secondo la somma standard (cioè cambiare segno a parte reale e parte immaginaria) è lo stesso che fare l'opposto secondo la somma indotta dalla cubica.

In generale, prendiamo due numeri complessi $z_1, z_2 \in \mathcal{P}$ e portiamoli in $\mathcal{C}$ tramite la parametrizzazione ottenendo i punti

$$P_1 = (\wp(z_1), \wp'(z_1))$$
$$P_2 = (\wp(z_2), \wp'(z_2)).$$

Se congiungiamo con una retta P_1 e P_2 otteniamo il terzo punto di interezione P_3. Grazie alla (2.13) sappiamo dire subito le coordinate di quest'ultimo: esse saranno infatti forzate ad essere

$$P_3 = (\wp(z_3), \wp'(z_3)) = (\wp(-z_1 - z_2), \wp'(-z_1 - z_2)) = (\wp(z_1 + z_2), -\wp(z_1 + z_2)).$$

Quindi tornando indietro con la parametrizzazione inversa andiamo a finire nel punto $-(z_1 + z_2)$. Ora sul nostro toro abbiamo tre punti: z_1 e z_2 scelti arbitrariamente, e z_3 che ha coordinate $-(z_1 + z_2)$ modulo Λ. Ma siccome la somma dei tre punti deve essere 0 modulo Λ, si capisce che deve valere la regola del parallelogramma. Se così non fosse la somma tra $S = P_1 + P_2$ e P_3 non sarebbe equivalente a 0 (mod Λ) portando a una contraddizione della (2.13). In figura 2.4 è mostrata (in due passi) la somma di punti sul toro il suo corrispondente sulla cubica.

Dunque la somma definita sulla cubica $\mathcal{C}$ è la stessa somma che troviamo naturalmente su $\mathbb{C}$. Questo permette di dire immediatamente che la somma tra punti sulla cubica è ben definita, senza ricorrere alla dimostrazione geometrica adottata nella sezione relativa alla legge di gruppo.[10] Il toro stesso, dotato dell'operazione indotta, costituisce quello che si chiama un *gruppo di Lie*, ovvero un gruppo munito di una struttura di varietà differenziabile.

this closes the small gap in the purely geometrical proof

2.5 Classi di equivalenza

Dato un reticolo Λ generato da ω_1, ω_2 moltiplichiamo tale reticolo per un numero complesso $c \in \mathbb{C}^*$. Osserviamo che il parallelogramma fondamentale $\mathcal{P}$ viene deformato da tale moltiplicazione: verrà dilatato se $c \in \mathbb{R}$ e verrà inoltre ruotato di un certo angolo nel caso generale in cui $c \in \mathbb{C}$ (si veda l'esempio in figura 2.5).

Abbiamo detto nella scorsa sezione che ad un reticolo Λ viene associata una certa curva ellittica $\mathcal{C}$ tramite la parametrizzazione (2.10); allo stesso

[10] Segue ad esempio l'associatività dell'operazione, che non avevamo dimostrato completamente.

XXVII-add3-3

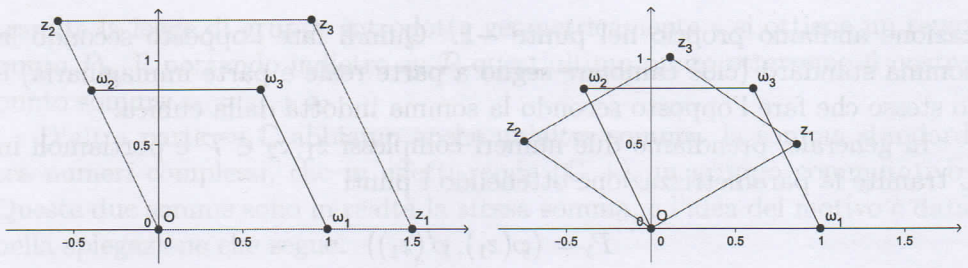

Figura 2.5: Moltiplicazione del parallelogramma fondamentale rispettivamente per $c = \frac{3}{2}$ e $c = \sqrt[3]{i}$

modo al reticolo $c\Lambda$ resterà associata una seconda curva ellittica $\mathcal{C}'$. Vediamo che relazione sussiste tra $\mathcal{C}$ e $\mathcal{C}'$. Premettiamo la seguente proprietà:

Proposizione 2.8. *Le funzioni $\wp$ e $\wp'$ sono soggette alle seguenti leggi di omogeneità:*[11]

$$\begin{cases} \wp(cz, c\Lambda) = c^{-2}\wp(z, \Lambda) \\ \wp'(cz, c\Lambda) = c^{-3}\wp'(z, \Lambda) \end{cases}$$

Dimostrazione. Basta ricorrere alla definizione e raccogliere:

$$\begin{aligned} \wp(cz, c\Lambda) &= \frac{1}{(cz)^2} + \sum_{\omega\in\Lambda^*}\left[\frac{1}{(cz - c\omega)^2} - \frac{1}{(c\omega)^2}\right] \\ &= \frac{1}{c^2}\frac{1}{z^2} + \frac{1}{c^2}\sum_{\omega\in\Lambda^*}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] \\ &= c^{-2}\wp(z, \Lambda) \end{aligned}$$

e analogamente per $\wp'$. □

Esaminiamo come cambia l'equazione della curva ellittica se moltiplichiamo il corrispondente reticolo per c. Sia Λ un reticolo associato alla curva $\mathcal{C}$ di equazione

$$\mathcal{C} : y^2 = 4x^3 - g_2x - g_3. \tag{2.16}$$

Se moltiplichiamo per c, la parametrizzazione diventa

$$z \mapsto (c^{-2}\wp(z), c^{-3}\wp'(z))$$

e quindi $\mathcal{C}'$ avrà equazione

$$\mathcal{C}' : c^{-6}y^2 = 4c^{-6}x^3 - g_2c^{-2}x - g_3$$

[11] Indichiamo esplicitamente la dipendenza di $\wp$ dalla scelta di Λ utilizzando la scrittura $\wp(z, \Lambda) = \wp(z, \omega_1, \omega_2)$

XXVII-add 3 - 4

che moltiplicando per c^6 diventa

$$y^2 = 4x^3 - c^4 g_2 x - c^6 g_3.$$

Dunque la trasformazione del reticolo Λ comporta il seguente cambio nei coefficienti dell'equazione di $\mathcal{C}$:

$$\begin{cases} g_2 \mapsto c^4 g_2 \\ g_3 \mapsto c^6 g_3. \end{cases} \tag{2.17}$$

Definizione 2.9. *Siano Λ e Λ' due reticoli. Diciamo che essi sono* linearmente equivalenti *se $\Lambda' = c\Lambda$ per un certo $c \in \mathbb{C}^*$.*

Poniamo da qui in avanti

$$\mathcal{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}.$$

Osserviamo che è sempre possibile trasformare il reticolo $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ in $\Lambda' = \mathbb{Z} + \mathbb{Z}\tau$ con $\tau \in \mathcal{H}$, e ciò può essere fatto moltiplicando per il numero complesso $c = \frac{1}{\omega_1}$ e chiamando

$$\tau := \frac{\omega_2}{\omega_1}.$$

Geometricamente ciò significa ruotare e riscalare il parallelogramma $\mathcal{P}$ in modo da far coincidere il lato relativo a ω_1 con l'unità sull'asse reale.

Andiamo ora a ricercare una quantità che risulti essere invariante quando si applica un'equivalenza lineare a una curva ellittica.

Definizione 2.10. *Sia $\mathcal{C}$ una curva ellittica con equazione $y^2 = 4x^3 - g_2 x - g_3$ e sia Λ il corrispondente reticolo. Chiamiamo la seguente quantità*

$$J_{\mathcal{C}} := \frac{g_2^3}{g_2^3 - 27 g_3^2}$$

invariante *J della curva $\mathcal{C}$.*

Si usa chiamare *discriminante ellittico* la quantità $\Delta := g_2^3 - 27 g_3^2$ al denominatore, che ha la proprietà di essere nulla se e solo se la curva considerata è singolare. Infatti la curva di equazione $y^2 = 4x^3 - 3g_3^{2/3} x - g_3$, ottenuta sostituendo $g_2^3 = 27 g_3^2$, ha due radici coincidenti.

Teorema 2.11. *Siano $\mathcal{C}$ e $\mathcal{C}'$ due curve ellittiche, associate rispettivamente ai reticoli Λ e Λ'. Se i due reticoli sono legati dalla relazione $\Lambda' = c\Lambda$ per un certo $c \in \mathbb{C}^*$ allora le due curve $\mathcal{C}$ e $\mathcal{C}'$ sono proiettivamente equivalenti. Viceversa se due curve sono proiettivamente equivalenti, allora esisterà un $c \in \mathbb{C}^*$ che renderà linearmente equivalenti i rispettivi reticoli.*

Dimostrazione. Per la dimostrazione si veda Lang, teorema 6 pagina 14. [3] □

Teorema 2.12. *Due curve ellittiche $\mathcal{C}$ e $\mathcal{C}'$ sono proiettivamente equivalenti se e solo se $J_{\mathcal{C}} = J_{\mathcal{C}'}$.*

Dimostrazione. Supponiamo di avere due curve $\mathcal{C}$ e $\mathcal{C}'$ scritte in forma

$$\mathcal{C} : y^2 = 4x^3 - g_2 x - g_3$$
$$\mathcal{C}' : y^2 = 4x^3 - g_2' x - g_3'$$

e supponiamo che siano proiettivamente equivalenti, ovvero per il teorema 2.11 i coefficienti delle due curve siano legati dalle relazioni (2.17). Allora

$$J_{\mathcal{C}'} = \frac{g_2'^3}{g_2'^3 - 27g_3'^2} = \frac{c^{12}g_2^3}{c^{12}g_2^3 - 27c^{12}g_3^2} = J_{\mathcal{C}}.$$

Viceversa, percorrendo i ragionamenti nel senso inverso, supponiamo $J_{\mathcal{C}} = J_{\mathcal{C}'}$, ovvero

$$\frac{g_2'^3}{g_2'^3 - 27g_3'^2} = \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Due frazioni sono uguali se i due numeratori sono tra loro proporzionali, e i due denominatori anche, e sempre con la stessa costante k. Scegliamo $k = c^{12}$ e otteniamo che deve essere

$$\begin{cases} g_2'^3 = c^{12}g_2^3 \\ g_2'^3 - 27g_3'^2 = c^{12}g_2^3 - 27c^{12}g_3^2 \end{cases} \Rightarrow \begin{cases} g_2' = c^4 g_2 \\ g_2'^3 - 27g_3'^2 = (c^4 g_2)^3 - 27(c^6 g_3)^2, \end{cases}$$

ovvero quello che volevamo.

Ora, grazie al ragionamento fatto nella sezione introduttiva relativa funzioni ellittiche, a g_2, g_3 (tali che $g_2^3 - 27g_3^2 \neq 0$) possiamo associare un reticolo avente periodi pari al valore numerico dell'integrale chiuso calcolato sui cappi incontraibili, e questo conclude la dimostrazione. □

Osserviamo che se cambiamo curva ellittica pur stando nella stessa classe di equivalenza il discriminante ellittico Δ *cambia*, al contrario dell'invariante J.

Dimostriamo ora che l'invariante J sopra definito è lo stesso invariante che abbiamo trovato nella prima parte, definito dalla (1.4), cioè quello che avevamo chiamato *modulo* di una cubica non singolare. La difficoltà nel dimostrare questa corrispondenza sta solo nel fatto che il modulo di una curva ellittica è definito partendo da una cubica in forma (1.1) (forma canonica di Legendre) mentre abbiamo definito l'invariante J a partire da curve in forma (2.16) (forma canonica di Weierstrass). Richiamiamo quindi una proposizione che stabilisca un'equivalenza tra le due forme.

Legendre: $y^2 = x(x-1)(x-c)$
Weierstrass: $y^2 = 4x^3 - g_2 x - g_3$

Proposizione 2.13. *Ogni cubica di equazione in forma canonica di Legendre* (1.1) *è proiettivamente equivalente a una cubica di equazione in forma canonica di Weierstrass* (2.16) *per un'opportuna scelta di coefficienti* g_2, g_3 *in funzione di* c*, e viceversa.*

Dimostrazione. Partendo da (1.1) applichiamo la trasformazione

$$(x, y) \mapsto \left(x + \frac{c+1}{3}, \frac{y}{2}\right).$$

che ha l'effetto di trasformare l'equazione di Legendre nella seguente equazione:

$$y^2 = 4x^3 - \frac{4}{3}(c^2 - c + 1)x - \frac{4}{27}(2c^3 - 3c^2 - 3c + 2).$$

Chiamando

$$\begin{cases} g_2 = \frac{4}{3}(c^2 - c + 1) \\ g_3 = \frac{4}{27}(2c^3 - 3c^2 - 3c + 2) \end{cases} \tag{2.18}$$

otteniamo l'equazione nella forma richiesta. □

Dimostriamo ora che il modulo e l'invariante J associati a una curva ellittica sono il medesimo concetto.

Teorema 2.14. *Il modulo di una curva ellittica in forma di Legendre coincide con l'invariante* J *della stessa curva in forma di Weierstrass.*

Dimostrazione. Usiamo la corrispondenza (2.18) che connette c con g_2, g_3 usata nel precedente risultato per manipolare l'espressione che definisce l'invariante J:

$$J = \frac{g_2^3}{g_2^3 - 27g_3^2} = \frac{\left(\frac{4}{3}(c^2 - c + 1)\right)^3}{\left(\frac{4}{3}(c^2 - c + 1)\right)^3 - 27\left(\frac{4}{27}(2c^3 - 3c^2 - 3c + 2)\right)^2}.$$

Svolgendo i calcoli, si arriva all'espressione

$$\frac{4}{27}\frac{(c^2 - c + 1)^3}{c^2(c-1)^2}$$

che è essenzialmente l'espressione che definisce il modulo. □

Abbiamo dunque trovato l'invariante di una cubica ellittica in due modi: prima per via geometrica, usando il teorema di Salmon e il modulo, poi per via analitica, usando l'equivalenza lineare tra reticoli associati e l'invariante J.

upshot

XXVII - ndd3 - 7