Matematica, Cultura e Società

Rivista dell'Unione Matematica Italiana

Ettore Carletti

La risoluzione delle equazioni algebriche di quinto grado mediante funzioni modulari ellittiche

Matematica, Cultura e Società. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **6** (2021), n.2, p. 127–146.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RUMI_2021_1_6_2_127_0>

Matematica, Cultura e Società. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2021.

Matematica, Cultura e Società – Rivista dell'Unione Matematica Italiana
Serie I, Vol. 6, N. 2, agosto 2021, 127-146

La risoluzione delle equazioni algebriche di quinto grado mediante funzioni modulari ellittiche

Ettore Carletti
Università di Genova
E-mail: carletti@dima.unige.it

Sommario: *Lo scopo del presente articolo è quello di presentare il metodo risolutivo dell'equazione algebrica di 5^o grado nella forma di Bring $x^5+5x-a=0$, dove a è un numero complesso non nullo, che compare nel terzo volume della monumentale opera di H. Weber "Lehrbuch der Algebra". Weber trova le soluzioni come funzioni razionali di certi valori di una funzione modulare ellittica, introdotta da Weber stesso per calcolare l'Hilbert class field di un campo quadratico immaginario, in un punto del semipiano superiore complesso la cui dipendenza da a è data esplicitamente.*

Abstract: *The aim of this paper is to present the method of resolution of the algebraic equation of 5^o degree in the Bring's form $x^5+5x-a=0$, where a is a non-zero complex number, which appears in the third volume of monumental work "Lehrbuch der Algebra" by H. Weber. Weber finds the solutions as rational functions of certain values of an elliptic modular function, introduced by Weber himself to compute the Hilbert class field of an imaginary quadratic field, in a point of the complex upper half plane whose dependence on a is explicitly given.*

1. – Introduzione

Notazioni. Premettiamo alcune notazioni. Come è usuale, indicheremo con $\mathbb{N}$, $\mathbb{Z}$. $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ gli insiemi dei numeri naturali, interi, razionali, reali e complessi, rispettivamente. Se $K=\mathbb{Z}$, $\mathbb{Z}_p:=\mathbb{Z}/p\mathbb{Z}$ (p primo), $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ indicheremo con K^* l'insieme $K\setminus\{0\}$ e

$$\begin{aligned}
&\mathrm{GL}_2(K)=\left\{\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}|a,b,c,d\in K,\ \det(\gamma)\neq 0\right\},\\
&\mathrm{GL}_2^+(K)=\{\gamma\in\mathrm{GL}_2(K)\,|\,\det(\gamma)>0\},\ K\neq\mathbb{C},\mathbb{Z}_p,\qquad (1.1)\\
&\mathrm{SL}_2(K)=\{\gamma\in\mathrm{GL}_2(K)\,|\,\det(\gamma)=1\},\\
&\mathrm{D}_2(K)=\left\{\gamma=\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\,|\,\lambda\in K^*\right\}.
\end{aligned}$$

Con $\mathbf{I}$ indicheremo la matrice $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ elemento neutro dei gruppi sopra definiti. Inoltre

$$\mathbb{S}^1=\{z\in\mathbb{C}:|z|=1\},\quad \mathbb{H}=\{z\in\mathbb{C}\,|\,\Im\mathfrak{m}(z)>0\},$$

dove $\Re\mathfrak{e}(z)$ e $\Im\mathfrak{m}(z)$ sono la parte reale e la parte immaginaria di z e $|z|$ è il modulo di z. Se $z\in\mathbb{C}$ allora fissiamo $\arg(z)\in(-\pi,\pi]$; avremo quindi $-1=e^{\pi i}$. Posto $z=|z|e^{\arg(z)i}$, definiamo per $k\in\mathbb{N}$,

$$\sqrt[k]{z}:=\sqrt[k]{|z|}\exp\left(\frac{\arg(z)}{k}i\right),\qquad (1.2)$$

così che $-\frac{\pi}{k}<\arg\left(\sqrt[k]{z}\right)\leq\frac{\pi}{k}$; in particolare avremo $\sqrt{z}>0$ se $z>0$.

Lo scopo del presente articolo è quello di illustrare il ruolo delle funzioni modulari ellittiche nella risoluzione delle equazioni algebriche di 5° grado

Accettato: il 20 giugno 2021.

nello spirito di una celebre frase attribuita al matematico tedesco M. Eichler (1912-1992):

> *Le cinque operazioni elementari in matematica sono la somma, la sottrazione, la moltiplicazione, la divisione e le forme modulari.*

Potremmo parafrasare questa affermazione dicendo che là dove si fermano le quattro operazioni algebriche (somma, sottrazione, moltiplicazione e divisione) e l'operazione inversa dell'estrazione di radici subentrano le forme modulari. Questo è proprio il caso della risoluzione delle equazioni algebriche di 5° grado. È d'uopo ricordare che se $f(X) \in \mathbb{C}[X]$ è un polinomio di grado ≥ 5 e K è il sottocampo di $\mathbb{C}$ generato dai coefficienti di $f(X)$ allora, per il teorema di Abel-Ruffini ([1] e [22]), l'equazione $f(x) = 0$ non possiede, in generale, formule risolutive contenenti solo le operazioni algebriche e l'estrazione di radici, relativamente al campo K. La teoria di Galois dà una risposta definitiva sulla risolubilità per radicali di $f(x) = 0$ (cfr. i Capitoli 4 e 6 di [6]):

> *L'equazione algebrica $f(x) = 0$ è risolubile per radicali se e solo se il gruppo di Galois dell'equazione (ossia il gruppo di Galois dell'estensione L/K dove L è il campo di spezzamento di $f(X)$) è un gruppo risolubile.*

Ad esempio, l'equazione $x^5 - 4x + 2 = 0$ non è risolubile per radicali perché il suo gruppo di Galois è il gruppo simmetrico S_5 che non è risolubile ([6], pag. 246) mentre l'equazione $x^5 - 5x + 12 = 0$ è risolubile per radicali perché il suo gruppo di Galois è il gruppo diedrale D_5 di ordine 10 che è risolubile ([27]). È quindi del tutto naturale che dalla metà del XIX secolo si sia affrontato il problema di esprimere le radici di un'equazione algebrica di grado ≥ 5 utilizzando funzioni trascendenti e, in particolare, funzioni modulari ellittiche di cui si conoscevano le cosiddette "equazioni modulari" di cui parleremo più avanti. Per esattezza storica va segnalato che già F. Viète (1540-1603) determinava le soluzioni di un'equazione cubica irriducibile della forma $x^3 + px + q = 0$ in forma trigonometrica utilizzando la formula di triplicazione del coseno $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$. Il Lettore interessato può consultare ([30]).

È necessario ora fare alcune premesse di carattere generale prima di addentrarci nell'argomento di questo articolo.

Il matematico tedesco E.W. von Tschirnhaus (1651-1708), che fu, tra l'altro, medico e l'inventore della porcellana in Europa, ideò delle trasformazioni, che portano il suo nome, per ricondurre la risoluzione di una generica equazione algebrica di grado n

$$x^n + p_1 x^{n-1} + \ldots + p_{n-1}x + p_n = 0 \tag{1.3}$$

alla risoluzione di un'equazione sempre di grado n ma più semplice da risolvere (cfr. [28]). Tali trasformazioni sono di tipo polinomiale cioè della forma

$$y = a_0 + a_1 x + \ldots + a_r x^r.$$

In effetti von Tschirnhaus pensava di poter risolvere per radicali l'equazione (1.3) eliminandone, mediante certe trasformazioni, tutti i termini intermedi per ricondurla ad un'equazione binomia $y^n + c = 0$. Il suo amico G. W. von Leibniz (1646-1716) obiettò che per risolvere la (1.3) si sarebbe dovuto preliminarmente risolvere un'equazione di grado $(n-1)!$; in particolare, per risolvere un'equazione di 5° grado dovremmo prima risolverne una di grado 24. Grazie alle trasformazioni di von Tschirnhaus il matematico svedese E. S. Bring ([7]) ridusse la generica equazione di 5° grado alla forma (poi detta *forma di Bring*) la cui risoluzione sarà l'oggetto del presente articolo. Nel § 10.2 di [2] il Lettore può trovare la dimostrazione del seguente

TEOREMA 1.1. – *Sia data l'equazione generale di 5° grado*

$$x^5 + p_1 x^4 + p_2 x^3 + p_3 x^2 + p_4 x + p_5 = 0. \tag{1.4}$$

Si possono determinare, risolvendo equazioni di grado ≤ 3, cinque numeri $a_0, a_1, \ldots, a_4$ tali che mediante la sostituzione $y = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$ la (1.4) *si riduca alla* forma di Bring

$$y^5 + P_4 y + P_5 = 0. \tag{1.5}$$

Pertanto, una volta conosciute le radici di (1.5) *possiamo determinare quelle di* (1.4) *risolvendo equazioni di grado ≤ 4.*

La forma di Bring (1.5) (dove $P_4 P_5 \neq 0$) può essere espressa nella forma (Bring-Jerrard)

$$x^5 + 5x - a = 0, \qquad a \neq 0. \tag{1.6}$$

Nel 1858 C. Hermite (1822-1901) pubblica sui *Comptes rendus de l'Académie des Sciences* ([13]) un articolo in cui espone la risoluzione dell'equazione di 5° grado ridotta alla forma di Bring-Jerrard (1.8). Ci sembra opportuno lasciar parlare Hermite:

> *Au lieu de chercher à représenter par une formule radicale à déterminations multiples les système des racines si éntroitement liées entre elles lorsqu'on les considère comme fonctions des coefficients, on peut, ainsi que l'exemple en a été donné dans le troisème degré chercher, en introduisant des variables auxiliaires, à obtenir les racines séparáment exprimées par autant de fonctions distinctes et uniformes relatives à ces nouvelles variables. Dans le cas dont nous venons de parler, où il s'agit de l'équation*
>
> $$x^3 - 3x + 2a = 0,$$
>
> *il suffit, come on sait, de représenter le coefficient a par le sinus d'un arc α pour que le racines se séparent en ces trois fonctions bien déterminées*
>
> $$2\sin\frac{\alpha}{3}, \quad 2\sin\frac{\alpha+2\pi}{3}, \quad 2\sin\frac{\alpha+4\pi}{3}. \tag{1.7}$$
>
> *Or c'est un fait tout semblable que nous avons à exposer relativement à l'équation*
>
> $$x^5 - x - a = 0. \tag{1.8}$$
>
> *Seulement, au lieu des sinus ou cosinus, ce sont les transcendantes elliptiques....*

Hermite ha ben presente che, come le funzioni trigonometriche e iperboliche, anche le funzioni modulari danno luogo a "formule di moltiplicazione" (o "formule di divisione") dell'argomento per un numero intero positivo n, le cosiddette *equazioni modulari di livello n*, e utilizza tali formule per ottenere le soluzioni dell'equazione (1.8). La soluzione di Hermite è basata sulla costruzione di una risolvente di 5° grado dell'equazione modulare di livello 5 della funzione modulare

$$\sqrt[4]{k}(\tau) = \sqrt{2}q^{\frac{1}{8}}\,\frac{\displaystyle\prod_{n=1}^{\infty}(1+q^{2n})}{\displaystyle\prod_{n=1}^{\infty}(1+q^{2n-1})}, \qquad q = e^{\pi i\tau},\ \tau\in\mathbb{H},$$

che è di 6° grado. In generale, siano $f(X)$, $g(X)\in K[X]$ dove K è un campo, diremo che l'equazione $g(x)=0$ è una *risolvente* di un'equazione $f(x)=0$ se tutte le radici di $g(X)$ appartengono al campo di spezzamento di $f(X)$ ossia sono funzioni razionali delle radici di $f(X)$. La funzione

$$k(\tau) = 4q^{\frac{1}{2}}\,\frac{\displaystyle\prod_{n=1}^{\infty}(1+q^{2n})^4}{\displaystyle\prod_{n=1}^{\infty}(1+q^{2n-1})^4}, \qquad q = e^{\pi i\tau},\ \tau\in\mathbb{H},$$

è chiamata *modulo* della funzione ellittica di C. G. J. Jacobi (1804-1851) sn u detta *sinus amplitudinis*. Il Lettore desideroso di approfondire la conoscenza delle funzioni ellittiche di Jacobi e, in particolare, del perché si definisca $k(\tau)$ come modulo di sn u, può proficuamente consultare [8], 99-105. Si deve a Jacobi la determinazione di tale equazione modulare ([14], 29-48). L'equazione modulare (di sesto grado in v) di livello 5 per $\sqrt[4]{k}(\tau)$, che ha tra le sue soluzioni $v = \sqrt[4]{k}(5\tau)$, è

$$v^6 - u^6 + 5u^2v^2(v^2-u^2) + 4uv(u^4v^4-1) = 0, \tag{1.9}$$

dove $u = \sqrt[4]{k}(\tau)$. Una sua risolvente di 5° grado ha equazione che facilmente si riconduce alla forma (1.8)

$$x^5 - x - \left(\frac{2(1+k^2(\tau))}{\sqrt[4]{5^5}\,\sqrt{k(\tau)}\,\sqrt{1-k^2(\tau)}}\right) = 0.$$

E. Galois (1811-1832) espone le sue considerazioni sull'equazione modulare di livello p di $\sqrt[4]{k}(\tau)$, dove p è un primo dispari, nella lettera che scrive ad Auguste Chevalier ([12]), nella notte tra il 29 e il 30 maggio 1832 (il 30 maggio morirà in duello). Galois prova che le equazioni modulari di livello 7 e 11, che hanno grado 8 e 12 rispettivamente, hanno risolventi di grado 7 e 11 ed osserva, senza provarlo, che ciò non accade per le equazioni modulari di livello un numero primo ≥ 13. È stato E. Betti (1823-1892) a dimostrare per primo questo fatto ([4]).

La soluzione di Hermite è stata "tradotta", nel linguaggio della teoria di Galois nel testo di McKean e Moll ([18]), al quale ci siamo ispirati per questo articolo. Il Lettore interessato può consultare anche la più sintetica trattazione di [2] o il classico trattato di L. Bianchi [5]. Ci è parso quindi naturale esporre

la soluzione data da H. Weber (1842-1913) in [32]. Abbiamo seguito, come traccia, sia l'esposizione originale in [32] sia la sua rivisitazione in [19] (si veda anche [2]) ma abbiamo chiarito e motivato i vari passi della dimostrazione di Weber inquadrandoli in modo esplicito nella teoria di Galois, la qual cosa è nascosta nelle esposizioni sopra citate. Abbiamo altresì evidenziato il ruolo delle "molteplici simmetrie", delle funzioni modulari (Proposizione 4.2) come pure quello degli invarianti assoluti nella costruzione delle equazioni modulari e delle loro risolventi (Proposizione 3.12). Abbiamo fornito le dimostrazioni di alcuni risultati fondamentali omettendo quelle più elementari e calcolative.

H. Weber affronta la risoluzione dell'equazione di 5° grado nella forma di Bring-Jerrard (1.6) utilizzando una funzione modulare, che indicheremo con $\mathfrak{f}$, da lui introdotta allo scopo di determinare l'Hilbert class field di un campo quadratico puramente immaginario (cfr. l'Introduzione 3.1). Il risultato su cui si incentra questa esposizione è il Teorema 5.4 che esprime le soluzioni dell'equazione (1.6) in termini dei valori della funzione $\mathfrak{f}(\tau)$ e delle trasformate di $\mathfrak{f}(5\tau)$ rispetto al gruppo $\mathfrak{G}_{\mathfrak{f}}$ (cfr. la Sezione 4) in un punto del dominio fondamentale $\mathcal{D}_2$ (cfr. l'Esempio 2.6), univocamente determinato dal coefficiente a.

Non possiamo terminare questa introduzione senza suggerire al Lettore di consultare il celebre libro sull'icosaedro ([16]) che F. Klein (1849-1925) scrisse direttamente ispirato dal lavoro di Hermite. Il libro di J. Shurman [26] fornisce una più agevole introduzione alle idee di Klein.

Per completezza d'informazione va infine segnalato che le equazioni di grado ≥ 6 non possono essere risolte, in generale, mediante le equazioni modulari delle funzioni modulari ellittiche come ha provato C. Jordan (Teorema 513 p. 378 di [15]). Jordan ha altresì provato (Teorema 515 p. 380 di [15]) che ciò è invece possibile utilizzando le funzioni iperellittiche. Segnaliamo infine l'articolo di H. Umemura ([29]) dove vengono espresse le soluzioni di una equazione algebrica mediante le forme modulari di Siegel. Va rimarcato che l'approccio di Umemura ha il grande vantaggio di non richiedere che l'equazione sia ridotta mediante le trasformazioni di Tschirnhaus ma di operare direttamente sull'equazione generale di grado n.

In questa esposizione abbiamo cercato di ridurre al minimo i prerequisiti. Le conoscenze di base della teoria delle funzioni olomorfe di una variabile complessa (con alcune nozioni base sui prodotti infiniti e le funzioni ellittiche), l'abc della teoria dei gruppi e dei gruppi di trasformazioni e della teoria di Galois dovrebbero consentire al Lettore una lettura agevole.

2. – Gruppi fuchsiani e funzioni modulari ellittiche

Introduciamo brevemente i concetti di gruppo fuchsiano e di funzione modulare ellittica. La letteratura sulle funzioni (e le forme) modulari è vastissima essendo questo un argomento centrale nella teoria dei numeri. Tra i testi presenti in bibliografia segnaliamo in particolare [24] e [9].

DEFINIZIONE 2.1 (Trasformazioni di Möbius). Chiameremo *sfera di Riemann* la compattificazione di Alexandrov $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}$ di $\mathbb{C}$. Dal punto di vista topologico $\mathbb{C}_\infty$ altro non è che la sfera unitaria $\mathbb{S}^2$ di $\mathbb{R}^3$. Il gruppo $\mathrm{GL}_2(\mathbb{C})$ agisce su $\mathbb{C}_\infty$ mediante la mappa

$$\Phi\colon \mathrm{GL}_2(\mathbb{C}) \times \mathbb{C}_\infty \to \mathbb{C}_\infty, \quad (\gamma, z) \to \gamma z, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

dove

$$\gamma z = \begin{cases} \dfrac{az+b}{cz+d} & \text{se } z \neq \infty,\ z \neq -\dfrac{d}{c},\ c \neq 0 \\ \infty & \text{se } z = \infty, c = 0 \ \text{ oppure se } \ z = -\dfrac{d}{c},\ c \neq 0 \\ \dfrac{a}{c} & \text{se } z = \infty, c \neq 0. \end{cases} \tag{2.1}$$

Tale azione è non effettiva e transitiva e i sottogruppi $\mathrm{GL}_2^+(\mathbb{R})$ e $\mathrm{SL}_2(\mathbb{R})$ di $\mathrm{GL}_2(\mathbb{C})$ agiscono (anch'essi transitivamente ma non effettivamente) su $\mathbb{H}$ e su $\mathbb{R}\cup\{\infty\}$.

Se $\gamma\in\mathrm{GL}_2^+(\mathbb{R})$ la trasformazione $\mathbb{H}\to\mathbb{H}$, $z\to\gamma z$, è detta *trasformazione di Möbius* ed è una mappa biolomorfa (ossia olomorfa con inversa olomorfa) $\mathbb{H}\to\mathbb{H}$ ed ogni mappa biolomorfa $\mathbb{H}\to\mathbb{H}$ è della forma (2.1). Se sul semipiano di Poincaré $\mathbb{H}$ poniamo la metrica iperbolica data dal tensore $\mathbf{g}=\dfrac{1}{y^2}(dx\otimes dx+dy\otimes dy)$ le matrici di $\mathrm{GL}_2^+(\mathbb{R})$ rappresentano tutte e sole le isometrie di $\mathbb{H}$ in sé.

Si dà la seguente classificazione (esaustiva) delle matrici non scalari di $\mathrm{GL}_2^+(\mathbb{R})$ in termini dei loro punti fissi: sia $\alpha\in\mathrm{GL}_2^+(\mathbb{R})$, α non scalare, allora

- α è *parabolica* se ha un solo punto fisso in $\mathbb{R}\cup\{\infty\}$;
- α è *iperbolica* se ha due punti fissi distinti in $\mathbb{R}\cup\{\infty\}$;
- α è *ellittica* se ha un solo punto fisso $z\in\mathbb{H}$ e l'altro punto fisso è il complesso coniugato $\overline{z}$.

Osserviamo infine che, se $\alpha=\gamma^{-1}\beta\gamma$ con $\gamma\in\mathrm{GL}_2^+(\mathbb{R})$, allora α è parabolico (ellittico, iperbolico) se e solo se β è parabolico (ellittico, iperbolico), in altre parole le definizioni date sopra sono invarianti per coniugazione in $\mathrm{GL}_2^+(\mathbb{R})$.

DEFINIZIONE 2.2 (Gruppi fuchsiani). Chiameremo *gruppo fuchsiano* un sottogruppo discreto di $\mathrm{SL}_2(\mathbb{R})$. Per quanto visto sopra, un gruppo fuchsiano Γ agisce su $\mathbb{R}\cup\{\infty\}$ e su $\mathbb{H}$ come gruppo di isometrie rispetto alla metrica iperbolica. Se $w\in\mathbb{H}\cup\mathbb{R}\cup\{\infty\}$ l'orbita Γw è l'insieme $\{\alpha w:\alpha\in\Gamma\}$. Il gruppo fuchsiano "più importante" è il *gruppo modulare* $\mathrm{SL}_2(\mathbb{Z})$. Tale gruppo è generato dalle matrici

$$T=\begin{pmatrix}1&1\\0&1\end{pmatrix}\quad\text{e}\quad S=\begin{pmatrix}0&-1\\1&0\end{pmatrix}. \tag{2.2}$$

I sottogruppi di $\mathrm{SL}_2(\mathbb{Z})$ di indice finito sono detti *sottogruppi modulari*. Tra questi, particolarmente importanti, vi sono i *sottogruppi principali di congruenza di livello* $N\geq 1$

$$\Gamma(N)=\left\{\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}):a\equiv d\equiv 1 \pmod N,\ b\equiv c\equiv 0 \pmod N\right\}.$$

Si ha infatti che

$$[\mathrm{SL}_2(\mathbb{Z}):\Gamma(N)]=N^3\prod_{\substack{p\mid N\\ p\text{ primo}}}\left(1-\frac{1}{p^2}\right),$$

in particolare:

$$[\mathrm{SL}_2(\mathbb{Z}):\Gamma(2)]=6,\quad [\mathrm{SL}_2(\mathbb{Z}):\Gamma(48)]=2^{13}\cdot 3^2. \tag{2.3}$$

Poiché $\mathrm{SL}_2(\mathbb{Z})=\Gamma(1)$, indicheremo $\mathrm{SL}_2(\mathbb{Z})$ per lo più con $\Gamma(1)$. I sottogruppi di $\mathrm{SL}_2(\mathbb{Z})$ che contengono un $\Gamma(N)$ per un N sono detti *sottogruppi di congruenza di livello* N e sono ovviamente sottogruppi modulari. Tra questi dobbiamo menzionare i gruppi

$$\Gamma_0(N)=\left\{\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}):c\equiv 0 \pmod N\right\},$$

$$\Gamma^0(N)=\left\{\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z}):b\equiv 0 \pmod N\right\}.$$

I gruppi $\Gamma_0(N)$ e $\Gamma^0(N)$ sono coniugati in $\Gamma(1)$: $\Gamma_0(N)=S^{-1}\Gamma^0(N)S$; inoltre

$$[\Gamma(1):\Gamma^0(N)]=[\Gamma(1):\Gamma_0(N)]=N\prod_{\substack{p\mid N\\ p\text{ primo}}}\left(1+\frac{1}{p}\right).$$

Terminiamo questa breve serie di esempi con il *gruppo di Hecke* $\mathfrak{G}(2)$ che è generato dalle matrici $T^2=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ e S. Se $P=\begin{pmatrix}0&-1\\1&1\end{pmatrix}$ allora $\mathfrak{G}(2)=P^{-1}\Gamma_0(2)P$. Pertanto il gruppo $\mathfrak{G}(2)$ ha indice 3 in $\Gamma(1)$ e contiene la matrice $-\mathbf{I}$. Dato il ruolo centrale del gruppo $\mathfrak{G}(2)$ in questa esposizione ne diamo due altre caratterizzazioni:

$$\begin{aligned}\mathfrak{G}(2)=\{&\gamma\in\Gamma(1):\gamma\equiv\mathbf{I} \pmod 2\\ &\text{oppure } \gamma\equiv S \pmod 2\},\end{aligned} \tag{2.4}$$

$$=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma(1):a+b-c-d\equiv 0 \pmod 2\right\}. \tag{2.5}$$

(cfr. [20] pag. 29 e p. 33, formula (1.7.4)) dove la congruenza (mod 2) tra matrici significa che le loro entrate di ugual posto sono congruenti (mod 2). Dalla (2.4) si deduce subito che $\mathfrak{G}(2)$ è un sottogruppo di congruenza di livello 2 e che l'indice di $\Gamma(2)$ in $\mathfrak{G}(2)$ è 2.

Diamo ora due definizioni fondamentali. Sia Γ un sottogruppo modulare. Una *cuspide* di Γ è un punto fisso di una matrice parabolica $\alpha \in \Gamma$. Un *punto ellittico* di Γ è un punto fisso di una matrice ellittica $\alpha \in \Gamma$. Per quanto sopra osservato se x è una cuspide (risp. un punto ellittico) di Γ allora l'orbita Γx è costituita di cuspidi (risp. di punti ellittici).

Sia z un punto ellittico di Γ e sia $\Gamma_z = \{\alpha \in \Gamma : \alpha z = z\}$ lo stabilizzatore di z in Γ. Allora Γ_z è un gruppo ciclico finito e l'ordine del gruppo $\Gamma_z/\{\pm\mathbf{I}\}$ è detto *ordine* del punto ellittico z.

La seguente proposizione, di cui la dimostrazione si trova, ad esempio, in [25], cap. 1, dà informazioni sulle cuspidi e sui punti ellittici di un sottogruppo modulare.

PROPOSIZIONE 2.3. – *Sia* Γ *un sottogruppo modulare allora:*

(1) *L'insieme delle cuspidi di* Γ *è* $\mathbb{Q} \cup \{\infty\}$. *Il numero* $\nu_\infty(\Gamma)$ *delle cuspidi inequivalenti è finito.*
(2) *Gli eventuali punti ellittici di* Γ *sono di ordine* 2 *e* 3. *Il numero* $\nu_2(\Gamma)$ *dei punti ellittici di ordine* 2 *inequivalenti e il numero* $\nu_3(\Gamma)$ *dei punti ellittici di ordine* 3 *inequivalenti sono finiti.*

ESEMPIO 2.4 – Il gruppo modulare $\Gamma(1)$ ha una sola cuspide $i\infty$ e due punti ellittici i di ordine 2 e $e^{2\pi i/3}$ di ordine 3. Il gruppo $\mathfrak{G}(2)$ ha due cuspidi $i\infty$ e -1 e un solo punto ellittico i di ordine 2. Il gruppo $\Gamma(2)$ ha 3 cuspidi inequivalenti -1, 0 e $i\infty$ e non ha punti ellittici.

Il concetto di insieme fondamentale, che è naturalmente associato all'azione di un gruppo su un insieme, ha una grande importanza nella fattispecie.

DEFINIZIONE 2.5. Sia Γ un sottogruppo modulare. Un sottinsieme $F \subset \mathbb{H}$ è un *insieme fondamentale per* Γ se ogni orbita Γz di $z \in \mathbb{H}$ interseca F in uno ed un solo punto.

Una *retta iperbolica* di $\mathbb{H}$ è la traccia su $\mathbb{H}$ di una retta parallela all'asse immaginario o di una circonferenza con centro sull'asse reale. Ogni retta iperbolica divide $\mathbb{H}$ in due *semipiani iperbolici*. Un sottinsieme $\overline{P}$ (la chiusura in $\mathbb{P}^1(\mathbb{C})$), dove $P = \bigcap_{i=1}^{n} H_i$, dove H_i sono semipiani iperbolici aperti, si dice *poligono iperbolico generalizzato*. L'aggettivo "generalizzato" sottolinea il fatto che $\overline{P}$ può avere ∞ come vertice e lati giacenti sull'asse reale.

Ogni gruppo fuchsiano Γ finitamente generato possiede un insieme fondamentale la cui chiusura in $\mathbb{P}^1(\mathbb{C})$ è un poligono generalizzato che viene detto *poligono fondamentale di* Γ. Per il Lettore interessato consigliamo i testi [3] o [20]. Qui ci limitiamo a dare alcuni esempi che ci saranno utili nel prosieguo.

ESEMPIO 2.6 – Un poligono fondamentale per $\Gamma(1)$ è dato da $\overline{\mathcal{D}_1}$, la chiusura euclidea del dominio fondamentale

$$\mathcal{D}_1 = \{z \in \mathbb{H} : -\frac{1}{2} \le \Re\mathrm{e}(z) \le 0, \ |z| \ge 1\} \cup \{z \in \mathbb{H} : 0 < \Re\mathrm{e}(z) < \frac{1}{2}, \ |z| > 1\}. \tag{2.6}$$

Un poligono fondamentale per $\mathfrak{G}(2)$ è dato da $\overline{\mathcal{D}_2}$, la chiusura euclidea del dominio fondamentale

$$\mathcal{D}_2 = \{z \in \mathbb{H} : -1 \le \Re\mathrm{e}(z) \le 0, \ |z| \ge 1\} \cup \{z \in \mathbb{H} : 0 < \Re\mathrm{e}(z) < 1, \ |z| > 1\}.$$

Nella Figura 1 indichiamo $e^{2\pi i/3}$ con ρ per cui $e^{\pi i/3} = -\overline{\rho}$.

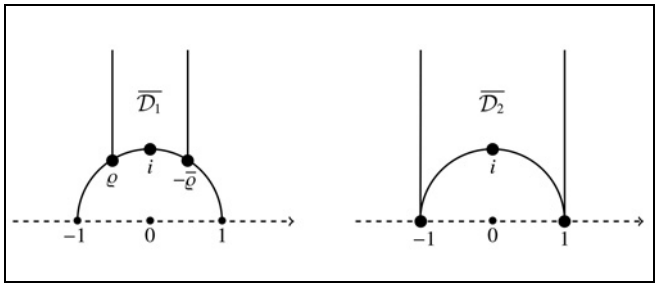

FIGURA 1 – I poligoni fondamentali $\overline{\mathcal{D}_1}$ e $\overline{\mathcal{D}_2}$.

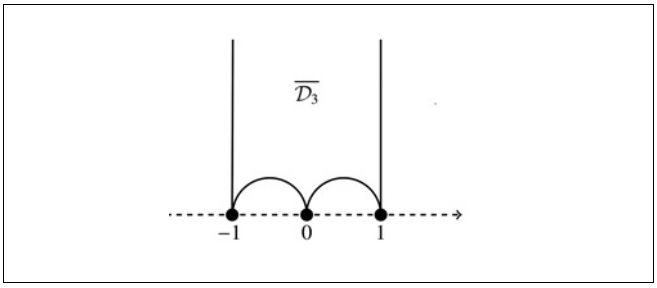

FIGURA 2 – Il poligono fondamentale $\overline{\mathcal{D}_3}$.

ESEMPIO 2.7 – Un poligono fondamentale del gruppo $\Gamma(2)$, che è generato dalle matrici $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ e $\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix}$, è dato da $\overline{\mathcal{D}_3}$ della Figura 2 dove

$$\mathcal{D}_3 = \left\{z \in \mathbb{H} : 0 < \Re\mathrm{e}(z) < 1,\ \left|z - \frac{1}{2}\right| > \frac{1}{2}\right\} \cup$$

$$\cup \left\{z \in \mathbb{H} : -1 \le \Re\mathrm{e}(z) \le 0,\ \left|z + \frac{1}{2}\right| \ge \frac{1}{2}\right\}$$

è un dominio fondamentale.

È necessario ora fare un piccolo cenno alla nozione di curva modulare.

DEFINIZIONE 2.8 (La curva modulare). Sia Γ un sottogruppo modulare. Lo spazio delle orbite $\Gamma\backslash\mathbb{H}$ ha una struttura naturale di superficie di Riemann non compatta e la mappa quoziente $p\colon \mathbb{H} \to \Gamma\backslash\mathbb{H}$ è un rivestimento ramificato nei punti ellittici. "Aggiungendo le $\nu_\infty(\Gamma)$ cuspidi inequivalenti" a $\Gamma\backslash\mathbb{H}$ si ottiene una superficie di Riemann compatta, denotata con $X(\Gamma)$ e detta *curva modulare associata a* Γ, tale che $\Gamma\backslash\mathbb{H}$ è un aperto di $X(\Gamma)$. "Incollando" opportunamente i lati di un poligono fondamentale di Γ (e "aggiungendo" le cuspidi) otteniamo la curva modulare $X(\Gamma)$.

La seguente proposizione individua l'invariante topologico più importante della curva modulare $X(\Gamma)$, il genere, mediante le caratteristiche (algebriche) di Γ.

PROPOSIZIONE 2.9. – *Sia* Γ *un sottogruppo modulare e* $X(\Gamma)$ *la curva modulare associata. Indicato con* $\mathrm{n}(\Gamma)$ *l'indice* $[\mathrm{SL}_2(\mathbb{Z})/\pm(\mathbf{I}) : \Gamma/\pm(\mathbf{I})]$ *e con* $\mathrm{g}(\Gamma)$ *il genere di* $X(\Gamma)$ *si ha*

$$\mathrm{g}(\Gamma) = 1 + \frac{\mathrm{n}(\Gamma)}{12} - \frac{\nu_2(\Gamma)}{4} - \frac{\nu_3(\Gamma)}{3} - \frac{\nu_\infty(\Gamma)}{2}.$$

Dimostrazione. [25], p. 35. □

ESEMPIO 2.10 – Per la Proposizione 2.9 il genere delle curve modulari $X(\Gamma(1))$, $X(G(2))$ e $X(\Gamma(2))$ è 0, infatti

$$\mathrm{g}(\Gamma(1)) = 1 + \frac{1}{12} - \frac{1}{4} - \frac{1}{3} - \frac{1}{2} = 0,$$

$$\mathrm{g}(\mathfrak{G}(2)) = 1 + \frac{3}{12} - \frac{1}{4} - \frac{2}{2} = 0,$$

$$\mathrm{g}(\Gamma(2)) = 1 + \frac{6}{12} - \frac{3}{2} = 0.$$

Pertanto $X(\Gamma(1))$, $X(\mathfrak{G}(2))$ e $X(\Gamma(2))$ sono tutte omeomorfe alla sfera di Riemann $\mathbb{C}_\infty$, ovvero alla sfera $\mathbb{S}^2$ di $\mathbb{R}^3$. Osserviamo però che $\Gamma(1)\backslash\mathbb{H}$ è omeomorfo a $\mathbb{C}$ (Proposizione 2.15), $\mathfrak{G}(2)\backslash\mathbb{H}$ è omeomorfo a $\mathbb{C}$ privato di un punto (Proposizione 3.9) mentre $\Gamma(2)\backslash\mathbb{H}$ è omeomorfo a $\mathbb{C}$ privato di due punti (Proposizione 2.16). La curva modulare $X(\Gamma_0(11))$ ha invece genere 1 (cfr. [25], Prop. 1.43) e quindi è omeomorfa ad un toro.

Introduciamo ora il concetto che sta alla base della "risoluzione trascendente" delle equazioni algebriche di 5° grado.

DEFINIZIONE 2.11 (Funzione modulare). Sia Γ un gruppo modulare e χ un *carattere* di Γ cioè un omomorfismo di gruppi $\chi\colon \Gamma \to \mathbb{S}^1$. Una funzione meromorfa $f\colon \mathbb{H} \to \mathbb{C}$ si dice *funzione modulare di* Γ *con carattere* χ se, per ogni $\gamma \in \Gamma$, si ha

$$f(\gamma z) = \chi(\gamma) f(z), \qquad \text{per ogni } z \in \mathbb{H}. \tag{2.7}$$

Se χ è il carattere banale (cioè $\chi(\gamma) = 1$ per ogni $\gamma \in \Gamma$) diremo semplicemente che f è una *funzione modulare* di Γ.

Definiamo ora il *comportamento nelle cuspidi di* Γ di una funzione modulare di Γ. Dato che i gruppi modulari che tratteremo contengono $-\mathbf{I}$ supponiamo che $-\mathbf{I} \in \Gamma$ per rendere più essenziale la trattazione.

Sia $c \in \mathbb{Q} \cup \{\infty\}$ una cuspide di Γ e sia $\Gamma_c = \{\gamma \in \Gamma : \gamma c = c\}$ lo stabilizzatore di c. Poiché

$$\Gamma(1)_\infty = \left\{\pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^n : n \in \mathbb{Z}\right\}$$

esiste uno ed un solo $h_c \in \mathbb{N}$ tale che

$$\Gamma_\infty = \left\{\pm\begin{pmatrix}1 & h_c\\ 0 & 1\end{pmatrix}^n : n \in \mathbb{Z}\right\}.$$

Allora esiste $\sigma_c \in \mathrm{GL}_2^+(\mathbb{Q})$ tale che $\sigma_c \infty = c$ e $\sigma_c^{-1}\Gamma_c\sigma_c = \Gamma_\infty$. Sia $\gamma_c = \sigma_c\begin{pmatrix}1 & h_c\\ 0 & 1\end{pmatrix}\sigma_c^{-1}$, allora si ha

$$f|_{\sigma_c}(\tau + h_c) = f(\gamma_c\sigma_c\tau) = \chi(\gamma_c) f(\sigma_c\tau) = \chi(\gamma_c) f|_{\sigma_c}(\tau).$$

Esiste uno ed un solo numero reale κ_c, $0 \le \kappa_c < 1$, tale che

$$\chi(\gamma_c) = e^{2\pi i \kappa_c}. \tag{2.8}$$

Posto

$$g(\tau) = \exp\left(-\frac{2\pi\kappa_c i\tau}{h_c}\right) f|_{\sigma_c}(\tau),$$

avremo $g(\tau + h_c) = g(\tau)$ e quindi l'espansione in serie di Fourier

$$f|_{\sigma_c}(\tau) = \sum_{n=n_c}^{+\infty} a_n e^{2\pi(n+\kappa_c)i\tau/h_c}, \quad n_c \geq -\infty,\ a_{n_c} \neq 0. \tag{2.9}$$

Se n_c è un intero negativo diremo che $f(\tau)$ *ha un polo di ordine* $-(\kappa_c + n_c)$ *nella cuspide* c. Se $n_c \geq 0$ diremo che $f(\tau)$ *è olomorfa in* c ed ha in c uno *zero di ordine* $n_c + \kappa_c$; se $n_c + \kappa_c > 0$ diremo che $f(\tau)$ *è cuspidale in* c. È facile verificare che l'intero n_c non dipende dalla scelta di σ_c e se c e c' sono cuspidi equivalenti di γ allora $n_c = n_{c'}$.

Una funzione modulare f (con carattere banale) induce naturalmente una mappa meromorfa $X(\Gamma) \to \mathbb{C}_\infty$, che indicheremo sempre con f. Il comportamento di f nelle cuspidi altro non è che il comportamento di f nei punti di $X(\Gamma)$ che rappresentano le cuspidi.

OSSERVAZIONE 2.12. – Le funzioni modulari sono un caso particolare delle cosiddette forme modulari di peso $k \in \mathbb{R}$ che rivestono un ruolo estremamente importante nella Teoria dei Numeri (e non solo). Sia k un numero reale. Se nella Definizione 2.11 al posto della 2.7 abbiamo che

$$f(\gamma z) = \chi(\gamma)(cz + d)^k f(z), \quad \text{per ogni } z \in \mathbb{H}, \tag{2.10}$$

dove $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ e $\chi\colon \Gamma \to \mathbb{S}^1$ è un *moltiplicatore* allora chiameremo f *forma modulare di* Γ *di peso* k *con moltiplicatore* χ. Rimandiamo ai Capitoli 3 e 4 di [20] per la definizione di moltiplicatore e per le necessarie precisazioni sulla (2.10). Le funzioni modulari altro non sono che le forme di peso 0, perché, in tal caso $(cz + d)^k = 1$ e il moltiplicatore è un carattere. Si verifica molto facilmente che la derivata prima di una funzione modulare con carattere χ è una forma modulare di peso 2 con carattere χ.

DEFINIZIONE 2.13 (Invarianti assoluti). Sia Γ un gruppo modulare. Indicheremo con $\mathcal{M}(\Gamma)$ il campo delle funzioni meromorfe su $X(\Gamma)$ ossia delle funzioni modulari di Γ meromorfe su $\mathbb{H}$ e nelle cuspidi di Γ. Chiameremo *invariante assoluto* di Γ una funzione $f \in \mathcal{M}(\Gamma)$ che possiede un solo polo e questo polo ha ordine 1. L'esistenza di un invariante assoluto porta a stringenti conseguenze.

PROPOSIZIONE 2.14. – *Se un gruppo modulare* Γ *ha un invariante assoluto allora la superficie di Riemann* $X(\Gamma)$ *è isomorfa (come superficie di Riemann) a* $\mathbb{C}_\infty$ *e l'isomorfismo è dato dall'invariante assoluto visto come mappa* $X(\Gamma) \to \mathbb{C}_\infty$. *Pertanto il campo* $\mathcal{M}(\Gamma)$ *coincide con* $\mathbb{C}(f)$ *il campo delle funzioni razionali in* f *a coefficienti in* $\mathbb{C}$. *Se, inoltre,* $g \in \mathcal{M}(\Gamma)$ *è olomorfa su* $\mathbb{H}$ *allora* $g \in \mathbb{C}[f]$ *ossia* g *è un polinomio in* f *a coefficienti in* $\mathbb{C}$.

Dimostrazione. Questo risultato è vero in generale per le superfici di Riemann compatte (cfr [11], p. 45). Poiché il campo delle funzioni meromorfe su $\mathbb{C}_\infty$ coincide con il campo delle funzioni razionali $\mathbb{C}(z)$ si ha subito la tesi. □

Il gruppo modulare $\Gamma(1)$ ha come invariante assoluto la funzione $j(\tau)$ per la cui definizione rimandiamo a [8], Cap. VI, dove è provata la seguente

PROPOSIZIONE 2.15. – *Per ogni* $a \in \mathbb{C}$ *esiste uno ed un solo* $\tau \in \mathcal{D}_1$ *tale che* $j(\tau) = a$. *Ponendo* $j(i\infty) = \infty$, *la mappa* $j\colon X(\Gamma(1)) \to \mathbb{C}_\infty$ *è isomorfismo di superfici di Riemann.*

Come accennato nell'Introduzione Hermite ottiene le soluzioni di (1.8) mediante la funzione $\sqrt[4]{k}(\tau)$.

La funzione $k^2(\tau)$ è invariante assoluto per il gruppo $\Gamma(2)$ ([8], 108-118 dove $k^2(\tau)$ è denotata con $\lambda(\tau)$). Analogamente alla Proposizione 2.15 si ha ([8], p. 118)

PROPOSIZIONE 2.16. – *Per ogni* $a \in \mathbb{C}$, $a \neq 0, 1$, *esiste uno ed un solo* $\tau \in \mathcal{D}_3$ *tale che* $k^2(\tau) = a$. *Mandando opportunamente le tre cuspidi (inequivalenti) di* $\Gamma(2)$ *in* 0, 1 *e* ∞ *otteniamo un isomorfismo di superfici di Riemann* $k^2\colon X(\Gamma(2)) \to \mathbb{C}_\infty$.

Il gruppo $\mathfrak{G}(2)$ (definito in (2.4)) ha come invariante assoluto la funzione di Weber $\mathfrak{f}^{24}(\tau)$ che introdurremo nella Sezione 3 (cfr. il Corollario 3.8).

Poiché la curva modulare di questi gruppi è la sfera di Riemann $\mathbb{C}_\infty$, ognuna di queste funzioni è

esprimibile come funzione razionale delle altre; in particolare si ha (cfr. [10], pp. 235-236)

$$j(\tau)=\frac{(\mathfrak{f}^{24}(\tau)-16)^3}{\mathfrak{f}^{24}(\tau)}. \tag{2.11}$$

3. – Le funzioni di Weber

INTRODUZIONE 3.1. – Sia $q=e^{\pi i\tau}$ con $\tau\in\mathbb{H}$. Le *funzioni di Weber* sono definite dai prodotti infiniti che convergono normalmente su $\mathbb{H}$ (cfr. [21])

$$\begin{aligned}\mathfrak{f}(\tau)&=q^{-\frac{1}{24}}\prod_{k=1}^{\infty}(1+q^{2k-1}),\ \mathfrak{f}_1(\tau)=\\ &=q^{-\frac{1}{24}}\prod_{k=1}^{\infty}(1-q^{2k-1}),\ \mathfrak{f}_2(\tau)=\\ &=\sqrt{2}q^{\frac{1}{12}}\prod_{k=1}^{\infty}(1+q^{2k}).\end{aligned} \tag{3.1}$$

Weber utilizza queste funzioni per calcolare alcuni valori della funzione $j(\tau)$ (cfr. la (2.11)), in particolare quelli che generano l'*Hilbert class field* di un campo quadratico immaginario. Nelle ultime sei pagine di [32] Weber presenta una tabella di valori delle tre funzioni da lui calcolati.

L'Hilbert class field $\mathcal{H}(K)$ di un campo di numeri algebrici K è la più grande estensione abeliana non ramificata (in tutti i primi finiti ed infiniti) di K. Se G è il gruppo di Galois di $\mathcal{H}(K)$ su K e $\mathcal{J}_K$ è il gruppo delle classi di ideali di K allora la mappa di Artin induce un isomorfismo $G\simeq\mathcal{J}_K$. Se con $\mathfrak{h}_K$ indichiamo il "numero delle classi" di K (o "class number" di K), ossia l'ordine del gruppo $\mathcal{J}_K$, si ha subito che $\mathfrak{h}_K=1\iff\mathcal{H}(K)=K$.

Sia ora $K=\mathbb{Q}(\sqrt{d})$ un campo quadratico immaginario e sia O_K il suo anello degli interi. È ben noto che $O_K=\{m+n\tau_K : m,n\in\mathbb{Z}\}$, dove

$$\tau_K=\left(\frac{\delta_K+\sqrt{\delta_K}}{2}\right)\in\mathbb{H} \tag{3.2}$$

e δ_K è il discriminante di K.

Il legame tra l'Hilbert class field di un campo quadratico immaginario e la funzione $j(\tau)$ è dato dal

TEOREMA 3.2. – (H. Weber). *Sia K un campo quadratico immaginario di discriminante δ_K. Se τ_K è come in* (3.2) *allora*

(1) *$j(O_K):=j(\tau_K)$ è un intero algebrico;*
(2) *l'Hilbert class field $\mathcal{H}(K)$ è generato su K da $j(O_K)$ ossia $\mathcal{H}(K)=K(j(O_K))$.*

Grazie alle funzioni $\mathfrak{f}$, $\mathfrak{f}_1$ e $\mathfrak{f}_2$, Weber calcola l'Hilbert class field di $K=\mathbb{Q}(\sqrt{-14})$:

$$\begin{aligned}j(O_K)&=j(\sqrt{-14})=\\ &=2^3\left(323+228\sqrt{2}+\left(231+161\sqrt{2}\right)\sqrt{2\sqrt{2}-1}\right)^3.\end{aligned}$$

Il Lettore interessato può trovare tutti i dettagli in [10] nel capitolo 3, § 12-D. Sempre nel capitolo 3, § 12-E è dimostrato, sempre con l'ausilio delle funzioni di Weber, il seguente importante risultato, congetturato già da Gauss nelle *Disquisitiones Arithmeticae*:

TEOREMA 3.3. – *I campi quadratici immaginari di class number* 1 *sono tutti e soli i campi di discriminante δ_K dove $\delta_K=-3,\ -4,\ -7,\ -8,\ -11,\ -19,\ -43,\ -67,\ -163$.*

Il Teorema 3.2 è una risposta positiva al famoso "Sogno di Gioventù" (Jugendtraum), espressione che L. Kronecker (1823-1891) usa in una lettera del 1880 di R. Dedekind (1831-1916), che consiste nella possibilità di descrivere le estensioni abeliane dei campi quadratici immaginari mediante valori (in opportuni punti) di funzioni modulari ellittiche. D. Hilbert (1862-1943) ne propone, nel suo XII Problema, la generalizzazione alle estensioni abeliane dei campi di numeri algebrici arbitrari. Il primo risultato in questa direzione è il famoso teorema di Kronecker-Weber (formulato da Kronecker ma provato da Weber) che afferma che ogni estensione abeliana di $\mathbb{Q}$ è contenuta in un campo ciclotomico ossia un campo della forma $\mathbb{Q}(\zeta)$ dove $\zeta=e^{\frac{2\pi i}{m}}$ dove m è un intero positivo. Lo Jugendtraum è un importante problema aperto della teoria dei numeri. Ci limitiamo a consigliare al Lettore interessato gli articoli di N. Schappacher [23], di R.P. Langlands [17] e il libro di S. G. Vlăduţ [31] dove può trovare lo stato dell'arte fino alla fine degli anni '80.

Lo studio approfondito delle tre funzioni $\mathfrak{f}(\tau)$, $\mathfrak{f}_1(\tau)$ e $\mathfrak{f}_2(\tau)$ (in particolare lo studio dell'equazione modulare di livello 5 di $\mathfrak{f}(\tau)$) porta Weber ([32]) a

ripercorrere la strada di Hermite utilizzando la funzione $\mathfrak{f}^{24}(\tau)$ per risolvere l'equazione di 5° grado nella forma di Bring-Jerrard (1.6).

Raggruppiamo ora in due proposizioni una serie di relazioni fondamentali che legano tra loro le funzioni di Weber che derivano dai legami di queste con la funzione eta di Dedekind e le costanti theta di C.G.J. Jacobi. Per la dimostrazione il Lettore può consultare il Capitolo 7 di [19] o [2]. L'uguaglianza (3.3) è conseguenza diretta della *"formula memorabilis"* di Jacobi ([2], pag. 84).

PROPOSIZIONE 3.4. – *Le funzioni* $\mathfrak{f}(\tau)$, $\mathfrak{f}_1(\tau)$ *e* $\mathfrak{f}_2(\tau)$ *sono olomorfe e mai nulle su* $\mathbb{H}$ *e soddisfano le seguenti relazioni:*

$$\mathfrak{f}^8(\tau) = \mathfrak{f}_1^8(\tau) + \mathfrak{f}_2^8(\tau), \tag{3.3}$$

$$\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}. \tag{3.4}$$

La seguente proposizione descrive il comportamento della funzione $\mathfrak{f}$ di Weber rispetto alle trasformazioni T e S e

$$U = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \tag{3.5}$$

PROPOSIZIONE 3.5. – *Valgono le seguenti relazioni:*

$$\begin{aligned} \mathfrak{f}(\tau+2) &= e^{-\frac{\pi i}{12}}\,\mathfrak{f}(\tau), \\ \mathfrak{f}\left(-\frac{1}{\tau}\right) &= f(\tau), \\ \mathfrak{f}(\tau)\mathfrak{f}\left(\frac{\tau-1}{\tau+1}\right) &= \sqrt{2}. \end{aligned} \tag{3.6}$$

Le prime due identità della (3.6) esprimono il comportamento di $\mathfrak{f}(\tau)$ rispetto ai generatori del gruppo $\mathfrak{G}(2)$. A questo punto si può ottenere una descrizione dell'azione delle matrici di $\mathfrak{G}(2)$ su $\mathfrak{f}(\tau)$ in funzione delle componenti delle stesse.

PROPOSIZIONE 3.6. – *La funzione di Weber* $\mathfrak{f}(\tau)$ *soddisfa la relazione*

$$\mathfrak{f}(\gamma\tau) = \chi_{\mathfrak{f}}(\gamma)\mathfrak{f}(\tau), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(2), \tag{3.7}$$

dove $\chi_{\mathfrak{f}}\colon \mathfrak{G}(2) \to \mathbb{S}^1$ *è il carattere di* $\mathfrak{G}(2)$ *definito da*

$$\chi_{\mathfrak{f}}(\gamma) = \exp\left(\frac{2\pi n_\gamma}{24} i\right) \tag{3.8}$$

con l'intero n_γ *dato da*

$$n_\gamma = \begin{cases} \dfrac{1}{2}\big[-(a+d)c + bd(c^2-1)\big], & \text{se } \begin{cases} b \equiv c \equiv 1 \pmod 2, \\ a \equiv d \equiv 0 \pmod 2, \end{cases} \\[2ex] \dfrac{1}{2}\big[-(a-2d)c + bd(c^2-1)\big], & \text{se } \begin{cases} a \equiv d \equiv 1 \pmod 2, \\ b \equiv c \equiv 0 \pmod 2. \end{cases} \end{cases} \tag{3.9}$$

L'immagine $\chi_{\mathfrak{f}}(\mathfrak{G}(2))$ *coincide pertanto con il gruppo delle radici 24-esime dell'unità.*

Inoltre $\mathfrak{f}(\tau)$ *ha un polo di ordine* $\dfrac{1}{24}$ *nella cuspide* ∞ *con sviluppo di Fourier*

$$\mathfrak{f}(\tau) = e^{-\frac{\pi i \tau}{24}} + e^{\frac{23\pi i \tau}{24}} + \dots \tag{3.10}$$

e uno zero di ordine $\dfrac{1}{24}$ *nella cuspide* -1 *con sviluppo di Fourier*

$$\mathfrak{f}|_{\sigma_{-1}}(\tau) = \sqrt{2}\, e^{\frac{\pi i \tau}{24}}(1 - e^{\pi i \tau} + \dots) \tag{3.11}$$

dove $\sigma_{-1} = \begin{pmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix}$.

In altre parole la funzione di Weber $\mathfrak{f}(\tau)$ *è una funzione modulare del gruppo* $\mathfrak{G}(2)$ *con carattere* $\chi_{\mathfrak{f}}$ *meromorfa in* ∞ *e cuspidale in* -1. *La funzione di Weber* $\mathfrak{f}(\tau)$ *è altresì una funzione modulare del sottogruppo principale di congruenza* $\Gamma(48)$.

Dimostrazione. Non proveremo la (3.8) ma vogliamo però applicare a questo caso quanto esposto nella Definizione 2.11 a riguardo dell'espansione di Fourier nelle cuspidi. Poiché $\sigma_\infty = \mathbf{I}$, $\gamma_\infty = T^2$, $h_\infty = 2$, $n_\infty = -1$, $\boldsymbol{\chi}(\gamma_\infty) = e^{-\frac{\pi i}{12}} = e^{\frac{23\pi i}{12}}$ per cui $\boldsymbol{\kappa}_\infty = \dfrac{23}{24}$ (cfr. (2.8)), lo sviluppo di $\mathfrak{f}(\tau)$ nella cuspide ∞ assume la forma (3.10)

$$\sum_{n=-1}^{+\infty} e^{2\pi(n+\frac{23}{24})i\tau/2}$$

tenendo conto della prima identità della (3.1). Diremo quindi che $\mathfrak{f}(\tau)$ ha un polo di ordine $\dfrac{1}{24}$ nella cuspide ∞.

Lo stabilizzatore in $\mathfrak{G}(2)$ della cuspide -1 è generato da $\gamma_{-1} = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$ e da $-\mathbf{I}$.

Come trasformazione che manda ∞ nella cuspide -1 utilizzeremo $\sigma_{-1} = \begin{pmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix}$: infatti $\sigma_{-1}^{-1} = U$

e (cfr. Definizione 2.11) $\sigma_{-1}^{-1}\gamma_{-1}\sigma_{-1} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. Poiché $\chi(\gamma_{-1}) = e^{\frac{\pi i}{12}}$ si ha $\kappa_{-1} = \dfrac{1}{24}$ e, per la (2.9),

$$\mathfrak{f}|_{\sigma_{-1}}(\tau) = \sum_{n=n_{-1}}^{\infty} a_n e^{\pi i \tau\left(n+\frac{1}{24}\right)} = \dots$$

$$\dots + a_{-1} e^{-\frac{23\pi i\tau}{24}} + a_0 e^{\frac{\pi i\tau}{24}} + a_1 e^{\frac{25\pi i\tau}{24}} + \dots .$$

Infine si ha

$$\mathfrak{f}|_{\sigma_{-1}}(\tau) = \mathfrak{f}\left(\frac{\tau+1}{-\tau+1}\right) = \mathfrak{f}\left(\frac{\tau-1}{\tau+1}\right) =$$

$$= \frac{\sqrt{2}}{\mathfrak{f}(\tau)} = \frac{\sqrt{2}e^{\frac{\pi i\tau}{24}}}{1+e^{\pi i\tau}+\dots} = \sqrt{2}\; e^{\frac{\pi i\tau}{24}}(1 - e^{\pi i\tau} + \dots).$$

Pertanto $\mathfrak{f}(\tau)$ è olomorfa nella cuspide -1 ed ha in -1 uno zero di ordine $\dfrac{1}{24}$.

Dalla (3.6) si ha immediatamente che $\mathfrak{f}(\tau+48) = \mathfrak{f}(\tau)$, pertanto $\mathfrak{f}(\tau)$ è una funzione modulare per il gruppo $\Gamma(48)$ poiché, per (2.3), $\Gamma(48)$ è un sottogruppo di indice finito di $\mathfrak{G}(2)$ (cfr. [25], p. 31). □

OSSERVAZIONE 3.7. – A p. 134 di [32] H. Weber dà per $\chi_{\mathfrak{f}}$ una forma più compatta utilizzando il simbolo di Kronecker-Jacobi-Legendre.

Abbiamo preferito la (3.8) a questa forma perché più comoda per le successive applicazioni.

COROLLARIO 3.8. – *La funzione $\mathfrak{f}^{24}(\tau)$ è una funzione modulare del gruppo di Hecke $\mathfrak{G}(2)$, ossia soddisfacente alle relazioni*

$$\mathfrak{f}^{24}(\tau+2) = \mathfrak{f}^{24}(\tau), \qquad \mathfrak{f}^{24}\left(-\frac{1}{\tau}\right) = \mathfrak{f}(\tau).$$

Inoltre $\mathfrak{f}^{24}(\tau)$ ha un polo semplice nella cuspide ∞ con sviluppo di Fourier

$$\mathfrak{f}^{24}(\tau) = e^{-\pi i\tau}(1 + 24e^{\pi i\tau} + \dots)$$

e uno zero semplice nella cuspide -1 con sviluppo di Fourier

$$\mathfrak{f}^{24}|_{\sigma_{-1}}(\tau) = 2^{12}e^{\pi i\tau}(1 - 24e^{\pi i\tau} + \dots)$$

dove la matrice σ_{-1} è come nella Proposizione 3.6.

Il Corollario 3.8 afferma che la funzione $\mathfrak{f}^{24}(\tau)$ è un invariante assoluto per il gruppo $\mathfrak{G}(2)$. Come casi particolari della Proposizione 2.14 si hanno le seguenti (cfr. le Proposizioni 2.15 e 2.16).

PROPOSIZIONE 3.9. – *Per ogni $a \in \mathbb{C}$, $a \neq 0$ esiste uno ed un solo $\tau \in \mathcal{D}_2$ tale che $\mathfrak{f}^{24}(\tau) = a$. Mandando opportunamente le due cuspidi (inequivalenti) di $\mathfrak{G}(2)$ in 0 e ∞ otteniamo un isomorfismo di superfici di Riemann*

$$\mathfrak{f}^{24}\colon X(\mathfrak{G}(2)) \to \mathbb{P}^1(\mathbb{C}),$$

PROPOSIZIONE 3.10. – *Sia g una funzione modulare meromorfa per $\mathfrak{G}(2)$. Allora*

$$g(\tau) = R(\mathfrak{f}^{24}(\tau))$$

dove R è una funzione razionale. Se $g(\tau)$ è olomorfa su $\mathbb{H}$ e nella cuspide -1 allora R è un polinomio e se è anche olomorfa all'∞ allora R è una costante.

Introduciamo ora la funzione modulare che, grazie alla Proposizione 3.12, sarà cruciale per la deduzione dell'equazione modulare (4.14).

DEFINIZIONE 3.11 La funzione

$$\mathfrak{F}(\tau) = \mathfrak{f}^{24}(\tau) + \frac{2^{12}}{\mathfrak{f}^{24}(\tau)} = q^{-1} + 24 + \dots \tag{3.12}$$

è olomorfa su $\mathbb{H}$ e invariante per le trasformazioni T^2, S e U, per la (3.6). Poiché $\det(U) = 2$ prendiamo $U' = \dfrac{1}{\sqrt{2}}U$, che appartiene a $\mathrm{SL}_2(\mathbb{R})$ ed è un elemento ellittico di ordine finito (poiché $(U')^2 = S$), e consideriamo quindi il sottogruppo $\mathfrak{U}$ di $\mathrm{SL}_2(\mathbb{R})$ generato da T^2, S e U'. Allora $\mathfrak{U}$ è un gruppo fuchsiano (cfr. [3], pp. 200-201) e $\mathfrak{F}(\tau)$ è una funzione modulare per $\mathfrak{U}$. Inoltre dallo sviluppo (3.12) si deduce subito che $\mathfrak{F}(\tau)$ ha polo semplice in ∞. Inoltre $\mathfrak{F}(\tau)$ ha polo semplice in -1 poiché

$$\mathfrak{F}|_{\sigma_{-1}}(\tau) = \mathfrak{F}\left(\frac{\tau+1}{-\tau+1}\right) =$$

$$= \mathfrak{F}\left(\frac{\tau-1}{\tau+1}\right) = \mathfrak{F}(\tau) = e^{-\pi i\tau} + 24 + \dots$$

PROPOSIZIONE 3.12. – *Sia g una funzione modulare meromorfa per $\mathfrak{G}(2)$ tale che*

$$g(U\tau) = g(\tau). \tag{3.13}$$

Allora

$$g(\tau) = G(\mathfrak{F}(\tau))$$

dove G è una funzione razionale e $\mathfrak{F}(\tau)$ è la funzione (3.12). *Se $g(\tau)$ è olomorfa su $\mathbb{H}$ allora G è un polinomio e se è anche olomorfa all'∞ allora G è una costante.*

Dimostrazione. Sia $g(\tau)$ soddisfacente alle ipotesi dell'enunciato. Per la Proposizione 3.10 $g(\tau) = R(\mathfrak{f}^{24}(\tau))$ dove R è una funzione razionale. Per la (3.13) si ha

$$R\left(\mathfrak{f}^{24}\left(\frac{\tau-1}{\tau+1}\right)\right) = R(\mathfrak{f}^{24}(\tau))$$

e quindi, per la (3.6),

$$R\left(\frac{2^{12}}{\mathfrak{f}^{24}(\tau)}\right) = R(\mathfrak{f}^{24}(\tau)).$$

Poniamo $x = \mathfrak{f}^{24}(\tau)$ e $a = 2^{12}$. Poiché è una funzione razionale R ha uno sviluppo del tipo $R(x) = \sum_{k=-\infty}^{+\infty} c_k x^k$. Allora $R\left(\frac{a}{x}\right) = \sum_{k=-\infty}^{+\infty} c_k a^k x^{-k}$ e quindi si ha $c_{-k} = c_k a^k$ così che $R(x) = c_0 + \sum_{k=1}^{+\infty} c_k \left(x^k + \left(\frac{a}{x}\right)^k\right)$. Si può facilmente provare per induzione che, per ogni $k \geq 1$, $x^k + \left(\frac{a}{x}\right)^k = P_k\left(x + \frac{a}{x}\right)$ dove P_k è un polinomio. Pertanto

$$R(x) = c_0 + \sum_{k=1}^{+\infty} c_k P_k\left(x + \frac{a}{x}\right) = G\left(x + \frac{a}{x}\right),$$

dove G è una certa funzione. Ma, essendo le singolarità di R in $\mathbb{C} \cup \{\infty\}$ solo di tipo polare, anche G possiede al più poli in $\mathbb{C} \cup \{\infty\}$ e quindi è una funzione razionale; possiamo quindi supporre che $G(x) = \frac{P(x)}{Q(x)}$ dove $P(x)$ e $Q(x)$ sono polinomi primi tra di loro. Pertanto $g(\tau) = \frac{P(\mathfrak{F}(\tau))}{Q(\mathfrak{F}(\tau))}$. Ma $Q(x)$ ha almeno una radice $x_0 \in \mathbb{C}$ e $P(x_0) \neq 0$. Poiché l'equazione $t^2 - x_0 t + 2^{12} = 0$ ha soluzioni non nulle in $\mathbb{C}$, $\mathfrak{F}(\tau) = x_0$ ha soluzioni $\tau_j \in \mathbb{H}$ per la Proposizione 3.9 e $g(\tau)$ è meromorfa (non olomorfa) in τ_j. Allora se $g(\tau)$ è olomorfa $G(x)$ necessariamente è un polinomio. Infine se $g(\tau)$ è olomorfa in $\mathbb{H}$ e in ∞ allora è costante poiché $\mathfrak{F}(\tau)$ ha un polo in ∞. □

4. – L'equazione modulare di livello 5 per $\mathfrak{f}(\tau)$

Sono ben note le formule di duplicazione (e triplicazione) delle funzioni trigonometriche come pure le corrispondenti formule per le funzioni iperboliche. Per entrambe le classi di funzioni si conoscono le formule di moltiplicazione (e divisione) dell'argomento per un intero positivo qualsiasi n. Assai più complicate da ottenere sono le analoghe relazioni per le forme modulari. Dobbiamo trovare un polinomio irriducibile $H(X, Y) \in \mathbb{C}[X, Y]$ tale che $H(\mathfrak{f}(5\tau), \mathfrak{f}(\tau)) = 0$ per ogni $\tau \in \mathbb{H}$, ossia un polinomio irriducibile $H_{\mathfrak{f}}(X) \in \mathbb{C}(\mathfrak{f}(\tau))[X]$ tale che

$$H_{\mathfrak{f}}(\mathfrak{f}(5\tau)) = 0, \qquad \forall \tau \in \mathbb{H}. \tag{4.1}$$

L'equazione (4.1) viene detta l'*equazione modulare di livello* 5 *per* $\mathfrak{f}(\tau)$. La strategia da seguire per provare che $\mathfrak{f}(5\tau)$ è algebrico su $\mathbb{C}(\mathfrak{f}(\tau))$ è indicata dal seguente (cfr. [6], pag. 126)

TEOREMA 4.1. – (Dedekind-Artin). *Sia G un gruppo finito di automorfismi di un campo L e sia K il suo sottocampo fisso ossia*

$$K = \{x \in L : \sigma(x) = x, \forall \sigma \in G\}.$$

Allora $[L : K] = \#(G)$, L è un'estensione di Galois di K e G è il gruppo di Galois di L su K.

Conviene considerare il gruppo $\mathrm{GL}_2^+(\mathbb{Q})$ che agisce sul campo $\mathcal{M}(\mathbb{H})$ delle funzioni meromorfe $h\colon \mathbb{H} \to \mathbb{C}$ mediante la legge

$$(\gamma h)(\tau) = h\left(\frac{a\tau + b}{c\tau + d}\right), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(2). \tag{4.2}$$

Per la (3.7) l'azione del sottogruppo $\mathfrak{G}(2)$ si restringe al sottocampo $\mathbb{C}(\mathfrak{f}(\tau))$ di $\mathcal{M}(\mathbb{H})$ ossia se $g(\tau) \in \mathbb{C}(\mathfrak{f}(\tau))$ allora $\gamma g \in \mathbb{C}(\mathfrak{f}(\tau))$ per ogni $\gamma \in \mathfrak{G}(2)$. Se $\mathfrak{G}_{\mathfrak{f}}$ è lo stabilizzatore di $\mathfrak{f}(\tau)$ in $\mathfrak{G}(2)$, allora $\mathfrak{G}_{\mathfrak{f}}$ fissa $\mathbb{C}(\mathfrak{f}(\tau))$ punto per punto. Consideriamo ora la $\mathfrak{G}_{\mathfrak{f}}$-orbita $V_{\mathfrak{f}}$ di $\mathfrak{f}(5\tau)$ in $\mathcal{M}(\mathbb{H})$ (cfr. (4.7)). Delineiamo i passi di questa strategia.

(1) Caratterizzeremo il gruppo $\mathfrak{G}_{\mathfrak{f}}$.
(2) Determineremo tutti gli elementi dell'orbita $V_{\mathfrak{f}}$ che risulterà essere un insieme finito su cui agisce transitivamente ma non fedelmente il gruppo $\mathfrak{G}_{\mathfrak{f}}$.
(3) Caratterizzeremo gli stabilizzatori di tutti gli elementi di $V_{\mathfrak{f}}$ in $\mathfrak{G}_{\mathfrak{f}}$ e lo stabilizzatore $\mathfrak{G}_{V_{\mathfrak{f}}} := \{\gamma \in \mathfrak{G}_{\mathfrak{f}} : \gamma h = h, \forall h \in V_{\mathfrak{f}}\}$ dell'intera orbita in $\mathfrak{G}_{\mathfrak{f}}$.
(4) Dedurremo che il gruppo $\mathfrak{G}_{\mathfrak{f}}/\mathfrak{G}_{V_{\mathfrak{f}}}$ è finito e agisce fedelmente (quindi come gruppo di auto-

morfismi) sul campo $\mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ ed ha $\mathbb{C}(\mathfrak{f}(\tau))$ come campo fisso.

(5) Per il Teorema 4.1 concluderemo che $\mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ è un'estensione di Galois di $\mathbb{C}(\mathfrak{f}(\tau))$ di grado $= \#(\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}})$ ed è quindi il campo di spezzamento di un polinomio irriducibile di $H_\mathfrak{f}(X) \in \mathbb{C}(\mathfrak{f}(\tau))[X]$ di grado $= \#V_\mathfrak{f}$ le cui radici sono gli elementi di $V_\mathfrak{f}$.

(6) Determineremo esplicitamente il polinomio $H_\mathfrak{f}(X)$ grazie alla Proposizione 3.12.

Passo 1: il gruppo $\mathfrak{G}_\mathfrak{f}$

Caratterizziamo in modo più esplicito il gruppo $\mathfrak{G}_\mathfrak{f}$. Per la (3.7) lo stabilizzatore $\mathfrak{G}_\mathfrak{f}$ di $\mathfrak{f}(\tau)$ coincide con $\ker\chi_\mathfrak{f}$ ed è quindi un sottogruppo normale di $\mathfrak{G}(2)$. Sia $\gamma \in \mathfrak{G}(2)$ allora $\gamma = S^{n_1}T^{2m_1}\dots S^{n_s}T^{2m_s}$ con n_j e $m_k \in \mathbb{Z}$. Quindi

$$\mathfrak{G}_\mathfrak{f} = \{\gamma \in \mathfrak{G}(2) : \gamma = S^{n_1}T^{2m_1}\dots S^{n_s}T^{2m_s}, \\ m_1 + \dots + m_s \equiv 0 \pmod{24}\}.$$

Poiché l'orbita $\mathfrak{G}(2)\mathfrak{f}$ di $\mathfrak{f}(\tau)$ coincide con l'insieme $= \{uf : u$ radice 24-esima dell'unità, allora si ha $[\mathfrak{G}(2) : \mathfrak{G}_\mathfrak{f}] = 24$. Dobbiamo ora caratterizzare $\mathfrak{G}_\mathfrak{f}$ rispetto alle entrate di $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(2)$. Imponendo $\chi_\mathfrak{f}(\gamma) = 1$ nella (3.8) otteniamo le congruenze

$$\begin{cases} bd(c^2-1) \equiv (a+d)c \pmod{48}, \\ a \equiv d \equiv 0 \pmod 2, \\ b \equiv c \equiv 1 \pmod 2, \end{cases}$$

(4.3)

$$\begin{cases} bd(c^2-1) \equiv (a-2d)c \pmod{48}, \\ a \equiv d \equiv 1 \pmod 2, \\ b \equiv c \equiv 0 \pmod 2. \end{cases}$$

Passi 2 e 3: l'orbita $V_\mathfrak{f}$ e gli stabilizzatori

Studiamo ora l'azione del gruppo $\mathfrak{G}_\mathfrak{f}$ su $\mathfrak{f}(5\tau)$. Si osserva subito che una matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(2)$ fissa $\mathfrak{f}(5\tau)$ se e solo se $\begin{pmatrix} a & 5b \\ \frac{c}{5} & d \end{pmatrix}$ fissa $\mathfrak{f}(\tau)$. Pertanto, affinché $\begin{pmatrix} a & 5b \\ \frac{c}{5} & d \end{pmatrix} \in \Gamma(1)$, dobbiamo avere $c \equiv 0 \pmod 5$. Si verifica facilmente che, utilizzando la (4.3)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}_\mathfrak{f} \iff \begin{pmatrix} a & 5b \\ \frac{c}{5} & d \end{pmatrix} \in \mathfrak{G}_\mathfrak{f}.$$

Quindi, se indichiamo con $\mathfrak{G}_\infty$ lo stabilizzatore di $\mathfrak{f}(5\tau)$, abbiamo

$$\mathfrak{G}_\infty = \mathfrak{G}_\mathfrak{f} \cap \Gamma_0(5). \tag{4.4}$$

Sia ora $c \not\equiv 0 \pmod 5$ e $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}_\mathfrak{f}$. Poiché $(48c, 5) = 1$ per ogni d esiste uno ed un solo $q \in \{-2,-1,0,1,2\}$ tale che $d \equiv 48cq \pmod 5$. Allora si ha subito che

$$\mathfrak{f}\left(5\frac{a\tau+b}{c\tau+d}\right) = \mathfrak{f}\left(\frac{5a\left(\frac{\tau+48q}{5}\right)+b-48aq}{c\left(\frac{\tau+48q}{5}\right)+\frac{d-48cq}{5}}\right) = \\ = \mathfrak{f}\left(\frac{\tau+48q}{5}\right), \qquad q = -2,-1,0,1,2,$$

se e solo se

$$\sigma = \begin{pmatrix} 5a & b-48aq \\ c & \frac{d-48cq}{5} \end{pmatrix} \in \mathfrak{G}_\mathfrak{f}, \qquad q = -2,-1,0,1,2.$$

Ma ciò è vero come facilmente si verifica utilizzando ancora la (4.3). Pertanto $\mathfrak{G}_\mathfrak{f}$ agisce su $\mathfrak{f}(5\tau)$ producendo 6 funzioni

$$\mathfrak{f}(5\tau) \quad \text{e} \quad \mathfrak{f}\left(\frac{\tau+48q}{5}\right), \quad q = -2,-1,0,1,2. \tag{4.5}$$

Poiché $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 48q \end{pmatrix} = ST^{48q} \in \mathfrak{G}_\mathfrak{f}$, allora, per la (3.6)

$$\mathfrak{f}(5\gamma\tau) = \mathfrak{f}\left(-\frac{5}{\tau+48q}\right) = \mathfrak{f}\left(\frac{\tau+48q}{5}\right).$$

e le 6 funzioni esistono effettivamente. Vedremo, dal loro comportamento rispetto a certe trasformazioni, che sono tutte distinte tra loro. Utilizzeremo, nel prosieguo, la notazione

$$v_\infty := \mathfrak{f}(5\tau), \\ v_{48q} := \mathfrak{f}\left(\frac{\tau+48q}{5}\right), \tag{4.6}$$
$$q = -2,-1,0,1,2.$$

La scelta di questi indici sarà pienamente giustificata dalla Proposizione 4.2, tenendo presente che $\{0, \pm 48, \pm 96\}$ è un sistema completo di residui (mod 5). Indichiamo con $\mathfrak{C}$ l'insieme $\{0, \pm 48, \pm 96, \infty\}$ e con $\mathfrak{C}_\infty$ l'insieme $\{0, \pm 48, \pm 96\}$.

Concludendo, abbiamo visto che la $\mathfrak{G}_\mathfrak{f}$-orbita di v_∞ in $\mathcal{M}(\mathbb{H})$ è l'insieme

$$V_\mathfrak{f} := \{v_\infty,\ v_0, v_{48}, v_{-48}, v_{96}, v_{-96}\}. \tag{4.7}$$

Indicheremo con $\mathfrak{G}_\mathfrak{c}$ lo stabilizzatore di $v_\mathfrak{c}$ in $\mathfrak{G}_f$ per $\mathfrak{c} \in \mathfrak{C}$ e con $\mathfrak{G}_{V_\mathfrak{f}} = \bigcap_{\mathfrak{c}\in\mathfrak{C}} \mathfrak{G}_\mathfrak{c}$ lo stabilizzatore di tutte le funzioni $v_\mathfrak{c}$.

Si ha quindi che

$$[\mathfrak{G}_\mathfrak{f} : \mathfrak{G}_\mathfrak{c}] = 6. \tag{4.8}$$

Ovviamente il gruppo $\mathfrak{G}_\mathfrak{f}$ agisce transitivamente su $V_\mathfrak{f}$ ma non fedelmente. Dobbiamo determinare lo stabilizzatore dell'orbita $\mathfrak{G}_{V_\mathfrak{f}}$ in modo esplicito.

Iniziamo caratterizzando lo stabilizzatore $\mathfrak{G}_0$. Si osserva subito che una matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(2)$ fissa $\mathfrak{f}\left(\frac{\tau}{5}\right)$ se e solo se $\begin{pmatrix} a & \frac{b}{5} \\ 5c & d \end{pmatrix}$ fissa $\mathfrak{f}(\tau)$. Affinché $\begin{pmatrix} a & \frac{b}{5} \\ 5c & d \end{pmatrix} \in \Gamma(1)$ dobbiamo avere $b \equiv 0 \pmod 5$. Si verifica senza difficoltà (grazie a (4.3)) che

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}_\mathfrak{f} \iff \begin{pmatrix} a & \frac{b}{5} \\ 5c & d \end{pmatrix} \in \mathfrak{G}_\mathfrak{f}.$$

Si conclude quindi che

$$\mathfrak{G}_0 = \mathfrak{G}_\mathfrak{f} \cap \Gamma^0(5). \tag{4.9}$$

Sia ora $\omega \in \{\pm 48, \pm 96\}$. La matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(2)$ fissa $\mathfrak{f}\left(\frac{\tau+\omega}{5}\right)$ se e solo se

$$A_\omega = \begin{pmatrix} a + \omega c & \dfrac{b + \omega d - a\omega - \omega^2 c}{5} \\ 5c & d - c\omega \end{pmatrix}$$

fissa $\mathfrak{f}(\tau)$. Affinché $A_\omega \in \Gamma(1)$ dobbiamo avere $b + \omega d - a\omega - \omega^2 c \equiv 0 \pmod 5$. Tenendo conto che $c(a - b - c) \equiv 0 \pmod 2$ è vera per tutte le matrici di $\mathfrak{G}(2)$ allora (grazie a (4.3))

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}_\mathfrak{f} \iff A_\omega \in \mathfrak{G}_\mathfrak{f}.$$

La condizione $b + \omega d - a\omega - \omega^2 c \equiv 0 \pmod 5$ equivale, per le ipotesi su ω, a $b \pm 48kd \mp 48ka - (48k)^2 c \equiv 0 \pmod 5$ con $k = 1, 2$. Le matrici di $\mathfrak{G}_\mathfrak{f}$ che fissano tutte le (4.6) devono appartenere a $\Gamma_0(5) \cap \Gamma^0(5)$. Pertanto la condizione

$$b \pm 48kd \mp 48ka - (48k)^2 c \equiv 0 \pmod 5, \quad k = 1, 2,$$

equivale a $\pm d \mp a \equiv 0 \pmod 5$ ossia a $a \equiv d \pmod 5$. Poiché $ad - bc = 1$ avremo $ad \equiv 1 \pmod 5$ e quindi $a \equiv d \equiv \pm 1 \pmod 5$. Avremo pertanto

$$\mathfrak{G}_{V_\mathfrak{f}} = \mathfrak{G}_\mathfrak{f} \cap \overline{\Gamma}(5)$$

dove

$$\overline{\Gamma}(5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5 \right\}.$$

Osserviamo che $\overline{\Gamma}(5) \not\subset \mathfrak{G}(2)$ e $\mathfrak{G}(2) \not\subset \Gamma_0(5)$. Poiché $\overline{\Gamma}(5)$ è un sottogruppo normale di $\Gamma(1)$ se $\gamma \in \mathfrak{G}_\mathfrak{f}$ allora

$$\gamma \mathfrak{G}_{V_\mathfrak{f}} \gamma^{-1} = (\gamma \overline{\Gamma}(5) \gamma^{-1}) \cap (\gamma \mathfrak{G}_f \gamma^{-1}) = \overline{\Gamma}(5) \cap \mathfrak{G}_\mathfrak{f} = \mathfrak{G}_{V_\mathfrak{f}}$$

e $\mathfrak{G}_{V_\mathfrak{f}}$ è sottogruppo normale di $\mathfrak{G}_\mathfrak{f}$.

Passi 4 e 5: il gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$

Per quanto visto sopra il gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$, il cui campo fisso è $\mathbb{C}(\mathfrak{f}(\tau))$, agisce fedelmente sul campo $\mathbb{C}(\mathfrak{f}(\tau))(v_\infty, v_0, v_{48}, v_{-48}, v_{96}, v_{-96})$ che abbiamo più brevemente indicato con $\mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$. È noto ([20], pp. 20-21) che $[\Gamma_0(5) : \overline{\Gamma}(5)] = 10$ ed inoltre è facile vedere che

$$[\mathfrak{G}_\infty : \mathfrak{G}_{V_\mathfrak{f}}] = [\mathfrak{G}_\mathfrak{f} \cap \Gamma_0(5) : \mathfrak{G}_\mathfrak{f} \cap \overline{\Gamma}(5)] \leq$$

$$\leq [\Gamma_0(5) : \overline{\Gamma}(5)] = 10. \tag{4.10}$$

In realtà si ha

$$[\mathfrak{G}_\infty : \mathfrak{G}_{V_\mathfrak{f}}] = 10. \tag{4.11}$$

Infatti i dieci elementi di $\mathfrak{G}_\infty$

$$\mathbf{I},\ T^{48}, T^{-48}, T^{96},\ T^{-96},\ \gamma = \begin{pmatrix} 8 & -13 \\ 5 & -8 \end{pmatrix},$$

$$\gamma T^{48},\ \gamma T^{-48},\ \gamma T^{96},\ \gamma T^{-96}, \tag{4.12}$$

non sono tra loro $\mathfrak{G}_{V_\mathfrak{f}}$-equivalenti. Rammentiamo che $T^{240} \in \mathfrak{G}_{V_\mathfrak{f}}$ ed osserviamo che $\gamma^2 = -\mathbf{I} \in \mathfrak{G}_{V_\mathfrak{f}}$ e quindi $\gamma^{-1} = -\gamma$. Vi sono quindi almeno 10 classi

distinte di $\mathfrak{G}_\infty \pmod{\mathfrak{G}_{V_\mathfrak{f}}}$. Dalla (4.10) segue allora la (4.11). Pertanto, per la (4.8) e la (4.11) si ha

$$[\mathfrak{G}_\mathfrak{f} : \mathfrak{G}_{V_\mathfrak{f}}] = [\mathfrak{G}_\mathfrak{f} : \mathfrak{G}_\infty][\mathfrak{G}_\infty : \mathfrak{G}_{V_\mathfrak{f}}] = 6 \cdot 10 = 60. \tag{4.13}$$

Possiamo applicare il Teorema 4.1 con $L = \mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ e $G = \mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$. Allora $\mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ è un'estensione di Galois di $\mathbb{C}(\mathfrak{f}(\tau))$ di grado 60 e, poiché G agisce transitivamente su $V_\mathfrak{f}$, è il campo di spezzamento di un polinomio irriducibile di sesto grado $H_\mathfrak{f}(X) \in \mathbb{C}(\mathfrak{f}(\tau))[X]$ le cui radici sono $v_\mathfrak{c}$, $\mathfrak{c} \in \mathfrak{C}$.

Passo 6: il polinomio $H_\mathfrak{f}(X)$

Per determinare il polinomio $H_\mathfrak{f}(X) \in \mathbb{C}(\mathfrak{f}(\tau))[X]$ dobbiamo studiare il comportamento di $v_\mathfrak{c}$ rispetto a T^2, S e U, per poi utilizzare la Proposizione 3.12. Conosciamo già dalla Proposizione 3.5 il comportamento di $f(\tau)$ rispetto a T^2, S e U. Tale comportamento è descritto dalla seguente

PROPOSIZIONE 4.2. – *Le trasformazioni T^2, S e U operano su $v_\mathfrak{c}$ nel seguente modo: se $v_\mathfrak{c} \longmapsto v_{\mathfrak{c}'}$ si ha*

$$T^2\colon \mathfrak{c} \to \mathfrak{c}' = \mathfrak{c} + 2 \pmod 5,$$

$$S\colon \mathfrak{c} \to \mathfrak{c}' = -\frac{1}{\mathfrak{c}} \pmod 5, \quad U\colon \mathfrak{c} \to \mathfrak{c}' = \frac{\mathfrak{c}-1}{\mathfrak{c}+1} \pmod 5,$$

avendo, per convenzione, $\infty \equiv \infty \pmod 5$, $\infty \equiv -\frac{1}{0} \pmod 5$, $0 \equiv -\frac{1}{\infty} \pmod 5$ *e* $\frac{\infty - 1}{\infty + 1} = 1 \equiv 96 \pmod 5$. *Si ha quindi la tabella*

	u	v_∞	v_0	v_{48}	v_{-48}	v_{96}	v_{-96}
T^2	$e^{-\pi i/12}u$	εv_∞	εv_{-48}	εv_0	εv_{-96}	εv_{48}	εv_{96}
S	u	v_0	v_∞	v_{48}	v_{-48}	v_{-96}	v_{96}
U	$\frac{\sqrt{2}}{u}$	$-\frac{\sqrt{2}}{v_{96}}$	$-\frac{\sqrt{2}}{v_{-96}}$	$-\frac{\sqrt{2}}{v_{48}}$	$-\frac{\sqrt{2}}{v_{-48}}$	$-\frac{\sqrt{2}}{v_0}$	$-\frac{\sqrt{2}}{v_\infty}$

dove $u = \mathfrak{f}(\tau)$ *e* $\varepsilon = e^{-5\pi i/12}$.

La dimostrazione è una verifica del tutto elementare ma lunga e noiosa anche se mette in risalto il ruolo delle "simmetrie" di $\mathfrak{f}(\tau)$. Il Lettore può trovare tutti i dettagli in [19] e [2].

COROLLARIO 4.3. – *Con le notazioni della* Proposizione 4.2, *si ha*

	$uv_\mathfrak{c}$	$\frac{u}{v_\mathfrak{c}}$
T^2	$e^{-\pi i/2}uv_{\mathfrak{c}'}$	$e^{\pi i/3}\frac{u}{v_{\mathfrak{c}'}}$
S	$uv_{\mathfrak{c}'}$	$\frac{u}{v_{\mathfrak{c}'}}$

	$uv_\mathfrak{c}$	$\frac{u}{v_\mathfrak{c}}$
U	$-\frac{2}{uv_{\mathfrak{c}'}}$	$-\frac{v_{\mathfrak{c}'}}{u}$.

La Proposizione 3.12, la Proposizione 4.2 e il Corollario 4.3 sono gli ingredienti fondamentali che ci permettono di dedurre la cosiddetta "equazione modulare".

TEOREMA 4.4. – (L'equazione modulare). *Assumiamo le notazioni della* Proposizione 4.2. *I numeri complessi $v = v_\mathfrak{c}$, $\mathfrak{c} \in \mathfrak{C}$ soddisfano l'*equazione modulare *a coefficienti in* $\mathbb{C}(u)$

$$H_\mathfrak{f}(X) := X^6 - u^5X^5 + 4uX + u^6 = 0. \tag{4.14}$$

Dimostrazione. Consideriamo le funzioni

$$A_\mathfrak{c} = \left(\frac{u}{v_\mathfrak{c}}\right)^3 + \left(\frac{v_\mathfrak{c}}{u}\right)^3, \qquad B_\mathfrak{c} = (uv_\mathfrak{c})^2 - \left(\frac{4}{uv_\mathfrak{c}}\right)^2.$$

Per il Corollario 4.3 si ha

$$T^2(A_\mathfrak{c}) = U(A_\mathfrak{c}) = -A_{\mathfrak{c}'},$$

$$T^2(B_\mathfrak{c}) = U(B_\mathfrak{c}) = -B_{\mathfrak{c}'},$$

$$S(A_\mathfrak{c}) = A_{\mathfrak{c}'}, \; S(B_\mathfrak{c}) = B_{\mathfrak{c}'}.$$

Allora la funzione $g(\tau) = \prod_{\mathfrak{c}\in\mathfrak{C}} (A_\mathfrak{c} - B_\mathfrak{c})^2$ è olomorfa in $\mathbb{H}$ ed è invariante rispetto alle trasformazioni T^2, S e U perché queste trasformazioni permutano solo i fattori. Avremo

$$A_\infty = \left(\frac{\mathfrak{f}(\tau)}{\mathfrak{f}(5\tau)}\right)^3 + \left(\frac{\mathfrak{f}(5\tau)}{\mathfrak{f}(\tau)}\right)^3 = q^{-\frac{1}{2}}\big[1 - 2q + 9q^2 + \ldots\big],$$

$$B_\infty = (\mathfrak{f}(\tau)\mathfrak{f}(5\tau))^2 - \frac{4}{(\mathfrak{f}(\tau)f(5\tau))^2} = q^{-\frac{1}{2}}\big[1 - 2q + 9q^2 + \ldots\big].$$

Abbiamo ottenuto che $(A_\infty - B_\infty)(\tau) = q^{-\frac{1}{2}} \sum_{n=3}^{\infty} a_n q^n$.

Osserviamo che, essendo $\mathfrak{c} \equiv 0 \pmod{48}$, si ha

$$u(5\tau - \mathfrak{c}) = \mathfrak{f}(5\tau) = v_\infty(\tau)$$

e

$$v_\mathfrak{c}(5\tau - \mathfrak{c}) = \mathfrak{f}\left(\frac{5\tau - \mathfrak{c} + \mathfrak{c}}{5}\right) = \mathfrak{f}(\tau) = u(\tau).$$

Inoltre A e B non cambiano scambiando u con v, quindi

$$A_\mathfrak{c}(5\tau - \mathfrak{c}) = A_\infty(\tau), \qquad B_\mathfrak{c}(5\tau - \mathfrak{c}) = B_\infty(\tau). \tag{4.15}$$

Pertanto

$$(A_\mathfrak{c} - B_\mathfrak{c})(\tau) = (A_\infty - B_\infty)\left(\frac{\tau + \mathfrak{c}}{5}\right) = q^{-\frac{1}{10}} \sum_{n=3}^{\infty} b_n(\mathfrak{c}) q^{\frac{n}{5}}.$$

Quindi si ha

$$g(\tau) = q^{-2}\left(\sum_{n=3}^{\infty} a_n q^n\right)^2 \prod_{\mathfrak{c} \in \mathfrak{C}} \left(\sum_{n=3}^{\infty} b_n(\mathfrak{c}) q^{\frac{n}{5}}\right)^2 = \sum_{n=3}^{\infty} \alpha_n q^n.$$

La funzione $g(\tau)$ soddisfa le ipotesi della Proposizione 3.12 e, essendo cuspidale in ∞, è la funzione nulla. Allora esiste $\mathfrak{c} \in \mathfrak{C}$ tale che $A_\mathfrak{c} - B_\mathfrak{c} = 0$ su un aperto di $\mathbb{H}$ e quindi su tutto $\mathbb{H}$ per l'olomorfia di $A_\mathfrak{c} - B_\mathfrak{c} = 0$. Per la (4.15) $A_\infty - B_\infty = 0$ su $\mathbb{H}$ e $A_\mathfrak{c} - B_\mathfrak{c} = 0$ su $\mathbb{H}$ per ogni $\mathfrak{c} \in \mathfrak{C}$. Pertanto si ha

$$\left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3 = (uv)^2 - \left(\frac{4}{uv}\right)^2$$

cioé $v^6 - u^5 v^5 + 4uv + u^6 = 0$. □

OSSERVAZIONE 4.5. – Dall'equazione modulare otteniamo la "formula di quintuplicazione", della funzione modulare

$$f(\tau): \ \mathfrak{f}(5\tau)^6 - \mathfrak{f}(\tau)^5 \mathfrak{f}(5\tau)^5 + 4\mathfrak{f}(\tau)\mathfrak{f}(5\tau) + \mathfrak{f}(\tau)^6 = 0.$$

5. – L'equazione di 5° grado nella forma di Bring-Jerrard come risolvente dell'equazione modulare

Il passo centrale nel processo di risoluzione dell'equazione di 5° grado nella forma di Bring-Jerrard (1.6) è quello di ottenerla come risolvente della (4.14) ossia come equazione avente per soluzioni delle funzioni razionali delle radici dell'equazione modulare. Come per l'equazione modulare anche in questo caso è fondamentale il ruolo della Proposizione 3.12. L'esistenza in $\mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ di un elemento di grado 5 su $\mathbb{C}(\mathfrak{f}(\tau))$ è essenziale. A questo proposito il seguente risultato è cruciale.

PROPOSIZIONE 5.1. – *Il gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ è isomorfo al gruppo A_5, il gruppo delle isometrie dell'icosaedro.*

Dimostrazione. Consideriamo innanzitutto l'azione di $\mathfrak{G}_\infty$ su $v_\mathfrak{c}$ con $\mathfrak{c} \in \mathfrak{C}_\infty$. Poniamo $\mathfrak{f}_k(\tau) = \mathfrak{f}\left(\frac{\tau + 48k}{5}\right)$, $-2 \le k \le 2$. Se una trasformazione $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}_\infty$ manda $\mathfrak{f}_q(\tau)$ in $\mathfrak{f}_{q'}(\tau)$, dove $-2 \le q < q' \le 2$ allora

$$\sigma \cdot \mathfrak{f}_q(\tau) = \mathfrak{f}_q(\sigma(\tau)) =$$

$$= \mathfrak{f}\left(\frac{\frac{a\tau + b}{c\tau + d} + 48q}{5}\right) = \mathfrak{f}\left(\frac{\tau + 48q'}{5}\right) =$$

$$= \mathfrak{f}\left(\frac{a'\left(\frac{\tau + 48q'}{5}\right) + b'}{c'\left(\frac{\tau + 48q'}{5}\right) + d'}\right)$$

per ogni $\sigma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathfrak{G}_\mathfrak{f}$. Pertanto si ha

$$\mathfrak{f}\left(\frac{(a + 48cq)\tau + b + 48qd}{5c\tau + 5d}\right) = \mathfrak{f}\left(\frac{a'\tau + 48a'q' + 5b'}{c'\tau + 48c'q' + 5d'}\right).$$

Imponendo

$$\begin{pmatrix} a + 48cq & b + 48qd \\ 5c & 5d \end{pmatrix} = \begin{pmatrix} a' & 48a'q' + 5b' \\ c' & 48c'q' + 5d' \end{pmatrix},$$

otteniamo le relazioni

$$a' = a + 48cq, \quad b' = \frac{b + 48qd - 48(a + 48cq)q'}{5}$$

$$c' = 5c, \qquad d' = d - 48cq'.$$

Non è difficile ora verificare che $\sigma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathfrak{G}_\infty$ ossia che $\sigma' \in \Gamma_0(5) \cap \mathfrak{G}_\mathfrak{f}$ per la (4.4). Quindi, mediante $\sigma \in \mathfrak{G}_\infty$, $\mathfrak{f}_q$ viene mandato in $\mathfrak{f}_{q'}$ dove

$$q' \equiv 2bd + d^2 q \pmod{5}. \tag{5.1}$$

Dalla (5.1) si ha subito l'azione delle trasformazioni (4.12) ($\neq \mathbf{I}$) sui $v_\mathfrak{c}$, come permutazioni su $q \pmod 5$ ($q \in \{-2, -1, 0, 1, 2\}$), riassunta dalla Tabella 1.

TABELLA 1 – Azione di $\mathfrak{G}_\infty$ sui $v_\mathfrak{c}$.

	decomposizione in cicli	v_{-96}	v_{-48}	v_0	v_{48}	v_{96}
T^{48}	$(-2\ \ -1\ \ 0\ \ 1\ \ 2)$	v_{-48}	v_0	v_{48}	v_{96}	v_{-96}
T^{-48}	$(-2\ \ 2\ \ 1\ \ 0\ \ -1)$	v_{96}	v_{-96}	v_{-48}	v_0	v_{48}
T^{96}	$(-2\ \ 0\ \ 2\ \ -1\ \ 1)$	v_0	v_{48}	v_{96}	v_{-96}	v_{-48}
T^{-96}	$(-2\ \ 1\ \ -1\ \ 2\ \ 0)$	v_{48}	v_{96}	v_{-96}	v_{-48}	v_0
γ	$(-2\ \ 0)\ \ (1\ \ 2)\ \ (-1)$	v_0	v_{-48}	v_{-96}	v_{96}	v_{48}
γT^{48}	$(-2\ \ 1)\ \ (-1\ \ 0)\ \ (2)$	v_{48}	v_0	v_{-48}	v_{-96}	v_{96}
γT^{-48}	$(-2\ \ -1)\ \ (0\ \ 2)\ \ (1)$	v_{-48}	v_{-96}	v_{96}	v_{48}	v_0
γT^{96}	$(-2\ \ 2)\ \ (-1\ \ 1)\ \ (0)$	v_{96}	v_{48}	v_0	v_{-48}	v_{-96}
γT^{-96}	$(-1\ \ 2)\ \ (0\ \ 1)\ \ (-2)$	v_{-96}	v_{96}	v_{48}	v_0	v_{-48}

Ricordiamo che il segno $\operatorname{sgn}(p)$ di una permutazione p di un insieme di n elementi composta di c cicli disgiunti è dato da $\operatorname{sgn}(p) = (-1)^{n-c}$, pertanto tutte queste permutazioni sono pari.

Per la (4.13) il gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ ha 60 elementi. Certamente $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \subset S_6$ il gruppo delle permutazioni di 6 elementi. Proviamo che $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \subset A_6$. Se $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \not\subset A_6$ allora deve contenere 30 permutazioni pari e 30 permutazioni dispari. Sia $p \in \mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ una permutazione dispari tale che $p(\infty) = i_p \in \{-2,-1,0,1,2\}$. Pertanto $p \notin \mathfrak{G}_\infty$. La permutazione ℓ di $\{\infty,-2,-1,0,1,2\}$ definita da

$$\ell(\infty) = \infty, \quad \ell(i) = T^{48}(i) = i+1 \pmod 5.$$

è pari. Le 6 permutazioni id, p, ℓp, $\ell^2 p$, $\ell^3 p$, $\ell^4 p$ rappresentano le 6 classi di $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \pmod{\mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}}$. Il gruppo $\mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}$, che è lo stabilizzatore di v_∞ in $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$, ha ordine 10, infatti $[\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} : \mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}] = [\mathfrak{G}_\mathfrak{f} : \mathfrak{G}_\infty] = 6$. Le permutazioni p, ℓp, $\ell^2 p$, $\ell^3 p$, $\ell^4 p$ sono dispari mentre quelle di $\mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}$ abbiamo appurato essere pari, pertanto vi sono almeno $5 \cdot \#(\mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}) = 50$ permutazioni dispari in $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ e ciò contrasta l'ipotesi che vi siano esattamente 30 permutazioni dispari. Allora $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \subset A_6$. Pertanto essendo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ un sottogruppo di A_6 di ordine 60 si ha (cfr. [33]) $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \cong A_5$ dove A_5 è il gruppo delle simmetrie dell'icosaedro. □

Poiché $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}} \cong A_5 \supset A_4$ e $[A_5 : A_4] = 60/12 = 5$, per il teorema fondamentale della teoria di Galois esiste un campo intermedio $\mathbb{C}(\mathfrak{f}(\tau)) \subset K_\mathfrak{f} \subset \mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ di grado 5 su $\mathbb{C}(\mathfrak{f}(\tau))$. Per il teorema dell'elemento primitivo esiste quindi un elemento $w_0 \in \mathbb{C}(\mathfrak{f}(\tau))(V_\mathfrak{f})$ di grado 5 su $\mathbb{C}(\mathfrak{f}(\tau))$. Consideriamo l'elemento

$$w_0 = \frac{(v_\infty - v_0)(v_{96} - v_{-96})(v_{-48} - v_{48})}{\sqrt{5}u^3}$$

TABELLA 2 – Azione di $\mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}$ su w_0.

	T^{48}	T^{-48}	T^{96}	T^{-96}	γ	γT^{48}	γT^{-48}	γT^{96}	γT^{-96}
w_0	w_3	w_2	w_1	w_4	w_4	w_2	w_1	w_0	w_3

e dimostriamo che esso viene trasformato dal gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ nei 5 elementi, tra loro distinti,

$$w_k = \frac{(v_\infty - v_k)(v_{k+1} - v_{k-1})(v_{k+2} - v_{k-2})}{\sqrt{5}u^3}, \qquad k = 0,1,2,3,4, \tag{5.2}$$

dove v_j è $v_\mathfrak{c}$ con $\mathfrak{c} \in \mathfrak{S}_\infty$ e $\mathfrak{c} \equiv j \pmod 5$. Dalla Tabella 1 ricaviamo la Tabella 2 che mostra come il sottogruppo $\mathfrak{G}_\infty/\mathfrak{G}_{V_\mathfrak{f}}$ agisce su w_0.

Proviamo ora che il gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ trasforma w_0 nei w_k, $k = 0,1,2,3,4$. Sia ${}^tT^{48}$ la trasposta di T^{48}, allora un conto diretto mostra che

(5.3)

	v_0	v_{48}	v_{-48}	v_{96}	v_{-96}	v_∞
${}^tT^{48}$	v_0	v_∞	v_{96}	v_{-96}	v_{48}	v_{-48}

Quindi ${}^tT^{48}$ agisce su $\{0, \pm 48, \pm 96, \infty\}$ come la permutazione $(0)(\infty\ \ -48\ 96\ \ -96\ 48)$.

Pertanto ${}^tT^{48}$ agisce sui w_i, $i = 0,1,2,3,4$, secondo la tabella

(5.4)

	w_0	w_1	w_2	w_3	w_4
${}^tT^{48}$	w_1	w_3	w_4	w_2	w_0

Poiché $({}^tT^{48})^k \in \mathfrak{G}_\infty$ se e solo se $k \equiv 0 \pmod 5$, le classi (laterali sinistre) (mod $\mathfrak{G}_\infty$) di $\mathbf{I}$, ${}^tT^{48}$, $({}^tT^{48})^2$, $({}^tT^{48})^3$ e di $({}^tT^{48})^4$ sono tutte tra loro distinte. Gli elementi di queste classi sono tutti della forma $({}^tT^{48})^k B$ con $B \in \mathfrak{G}_\infty$ e $k \in \{0,1,2,3,4\}$. Rimane una classe che indicheremo con $[A]$, con $A \in \mathfrak{G}_\mathfrak{f} \setminus \mathfrak{G}_\infty$. Se A non fosse generato da $\mathfrak{G}_\infty$ e da ${}^tT^{48}$ allora la classe dell'elemento $A\,{}^tT^{48}$ sarebbe distinta da tutte le altre contro il fatto che $[\mathfrak{G}_\mathfrak{f} : \mathfrak{G}_\infty] = 6$. Pertanto $\mathfrak{G}_\mathfrak{f}$ è generato da $\mathfrak{G}_\infty$ e da ${}^tT^{48}$. Allora il gruppo $\mathfrak{G}_\mathfrak{f}/\mathfrak{G}_{V_\mathfrak{f}}$ trasforma w_0 negli elementi w_k con $k = 0,1,2,3,4$. Proveremo che tali elementi sono tutti distinti per cui w_0 è un elemento di grado 5 su $\mathbb{C}(\mathfrak{f}(\boldsymbol{\tau}))$ e che il polinomio

$$P_\mathfrak{f}(X) = \prod_{k=0}^{4}(X - w_k) \in \mathbb{C}(\mathfrak{f}(\tau))[X]$$

è il polinomio di spezzamento di w_0. Osserviamo che la scelta dell'elemento w_0 è ispirata dalla Tabella 1, dalla (5.3) e dal fatto che $\mathfrak{G}_\mathfrak{f}$ è generato da $\mathfrak{G}_\infty$ e da ${}^tT^{48}$.

È ora necessario determinare come le trasformazioni T^2, S e U operano sui w_k. Il seguente corollario segue facilmente dalla tabella della Proposizione 4.2.

COROLLARIO 5.2. – *La seguente tabella descrive l'azione delle trasformazioni T^2, S e U sui w_k.*

(5.5)

	w_0	w_1	w_2	w_3	w_4
T^2	$-w_2$	$-w_3$	$-w_4$	$-w_0$	$-w_1$
S	w_0	w_2	w_1	w_4	w_3
U	$-w_0$	$-w_3$	$-w_4$	$-w_2$	$-w_1$

TEOREMA 5.3. – (Una risolvente di 5° grado dell'equazione modulare). *Una risolvente di 5° grado dell'equazione modulare* (4.14) *è l'equazione*

$$X(X^2+5)^2 - \left(\frac{\mathfrak{f}^{24}(\tau) - 64}{\mathfrak{f}^{12}(\tau)}\right) = 0. \tag{5.6}$$

Dimostrazione. Determiniamo la forma esplicita del polinomio monico di 5° grado $P_\mathfrak{f}$ che ha per radici w_k, $k = 0, 1, 2, 3, 4$. Poniamo quindi

$$P_\mathfrak{f}(X) = \prod_{k=0}^{4}(X - w_k) = \tag{5.7}$$

$$= X^5 + A_1X^4 + A_2X^3 + A_3X^2 + A_4X + A_5.$$

Poiché, per $j = 1, \ldots, 5$, si ha $A_j = (-1)^j \sum_{0 \le k_1 < \ldots < k_j \le 4} w_{k_1} \ldots w_{k_j}$, i coefficienti A_j sono olomorfi su $\mathbb{H}$. Per la (5.5) avremo che A_1^2, A_2, A_3^2, A_4 e A_5^2 sono invarianti (come funzioni di τ) rispetto alle trasformazioni T^2, S e U. Pertanto (per la Proposizione 3.12) sono polinomi in

$$u^{24} + \frac{2^{12}}{u^{24}} = \frac{1}{q} + 24 + \ldots.$$

Un tale polinomio è non costante se e solo se la sua espansione in serie di Laurent di q (ossia in $\tau = \infty$) inizia con il termine Kq^r dove $r \le -1$ e $K \neq 0$, così che ha un polo di ordine almeno 1. Siamo condotti a calcolare il primo termine dell'espansione in serie di Laurent di q. A partire dagli sviluppi

$$u^3 = q^{-\frac{1}{8}}(1 + 3q + \ldots), v_\infty = q^{-\frac{5}{24}}(1 + q^5 + \ldots),$$

$$v_\mathfrak{c} = e^{-\frac{\pi i \mathfrak{c}}{120}} q^{-\frac{1}{120}}(1 + q^{\frac{1}{5}} q^{\frac{\mathfrak{c}}{5}} + \ldots),$$

concludiamo che A_1^2, A_2, A_3^2 e A_4 sono costanti rispetto a τ e calcolandole in $\tau = i$ otteniamo $A_1 = 0$, $A_2 = 10$, $A_3 = 0$, $A_4 = 25$. Infine si ha $A_5 = -u^{12} + \dfrac{64}{u^{12}}$, pertanto

$$P_\mathfrak{f}(X) = X(X^2+5)^2 - \left(\frac{\mathfrak{f}^{24}(\tau) - 64}{\mathfrak{f}^{12}(\tau)}\right). \qquad \square$$

TEOREMA 5.4. – *Sia $a \in \mathbb{C}$, $a \neq 0$. Le soluzioni dell'equazione $x^5 + 5x - a = 0$ sono date da*

$$x_k = \frac{a}{w_k^2(\tau_a) + 5}, \qquad k = 0,1,2,3,4, \tag{5.8}$$

dove i $w_k(\tau_a)$ sono come in (5.2) *e τ_a è l'unico numero complesso $\in \mathcal{D}_2$ tale che*

$$\mathfrak{f}^{24}(\tau_a) = \left(\frac{a^2 + \sqrt{a^4 + 256}}{2}\right)^2$$

oppure

$$\mathfrak{f}^{24}(\tau_a) = \left(\frac{a^2 - \sqrt{a^4 + 256}}{2}\right)^2.$$

Dimostrazione. Dobbiamo ridurre l'equazione $P_\mathfrak{f}(w) = 0$ all'equazione di 5° grado nella forma di

Bring-Jerrard (1.6). Per la (3.3) e la (3.4) l'equazione $P_{\mathfrak{f}}(w) = 0$ assume la forma

$$w(w^2+5)^2 = \left(\frac{\mathfrak{f}_1^8(\tau) - \mathfrak{f}_2^8(\tau)}{\mathfrak{f}^2(\tau)}\right)^2. \tag{5.9}$$

Mediante la sostituzione

$$x(\tau) = \frac{\mathfrak{f}_1^8(\tau) - \mathfrak{f}_2^8(\tau)}{\mathfrak{f}^2(\tau)(w^2(\tau)+5)} \tag{5.10}$$

la (5.9) assume la forma

$$x^5 + 5x = \frac{\mathfrak{f}_1^8(\tau) - \mathfrak{f}_2^8(\tau)}{\mathfrak{f}^2(\tau)}. \tag{5.11}$$

Sia $a \neq 0$. Supponiamo di voler risolvere l'equazione (1.6). Dobbiamo allora determinare $\tau \in \mathbb{H}$ tale che $a = \dfrac{\mathfrak{f}_1^8(\tau) - \mathfrak{f}_2^8(\tau)}{\mathfrak{f}^2(\tau)}$. Otteniamo dalle (3.3) e (3.4) l'equazione quadratica in $\mathfrak{f}^{12}(\tau)$

$$\mathfrak{f}^{24}(\tau) - a^2\mathfrak{f}^{12}(\tau) - 64 = 0. \tag{5.12}$$

Avremo quindi

$$\mathfrak{f}^{12}(\tau) = \frac{a^2 \pm \sqrt{a^4+256}}{2}. \tag{5.13}$$

Una delle due radici (5.13) dà la soluzione di $\dfrac{\mathfrak{f}_1^8(\tau) - \mathfrak{f}_2^8(\tau)}{\mathfrak{f}^2(\tau)} = a$ mentre l'altra risolve $\dfrac{\mathfrak{f}_1^8(\tau) - \mathfrak{f}_2^8(\tau)}{\mathfrak{f}^2(\tau)} = -a$. Si osserva subito che il membro a destra della (5.13) è diverso da 0 per ogni $a \in \mathbb{C}$, quindi, per la Proposizione 3.9, esiste uno ed un solo numero complesso $\tau_a \in \mathcal{D}_2$ tale che

$$\mathfrak{f}^{24}(\tau_a) = \left(\frac{a^2 + \sqrt{a^4+256}}{2}\right)^2$$

oppure

$$\mathfrak{f}^{24}(\tau_a) = \left(\frac{a^2 - \sqrt{a^4+256}}{2}\right)^2.$$

Dalla (5.10) otteniamo le soluzioni (5.8) e quindi possiamo esprimere, mediante la (5.2), le radici di (1.6) parametrizzate da $\mathfrak{f}(\tau)$ in $\mathcal{D}_2$. □

RIFERIMENTI BIBLIOGRAFICI

[1] N.H. ABEL: *Beweis der Unmöglichkeit algebraische Gleichungen von höheren Garden als dem vierten allgemeinen aufzulösen*, J. Reine Angel. Math. 1 (1826), pp. 67-84.

[2] J.V. ARMITAGE, W.F. EBERLEIN: *Elliptic Functions*. Cambridge U.P. (2006).

[3] A. BEARDON: *The geometry of discrete groups*. Graduate Texts in Math. 91, Springer (1983).

[4] E. BETTI: *Sopra l'abbassamento delle equazioni modulari delle funzioni ellittiche*, Annali di Scienze matematiche e fisiche, IV, (1853), 81-100, in *Opere Matematiche di Enrico Betti* vol. I, Hoepli, Milano (1903).

[5] L. BIANCHI: *Lezioni sulla Teoria delle Funzioni di Variabile Complessa*, II ed. Spoerri, Pisa (1916).

[6] S. BOSCH: *Algebra*, Springer (2003).

[7] E.S. BRING: *Melemata Quaedam Mathematica circa Transformationem Aequationum Algebricarum*, Lund (1786).

[8] K. CHANDRASEKHARAN: *Elliptic Functions*. Springer (1985).

[9] H. COHEN e F. STRÖMBERG: *Modular Forms. A Classical Approach.* Graduate Studies in Mathematics **179**, American Mathematical Society (2017).

[10] D.A. Cox: *Primes of the Form $x^2 + ny^2$*, II ed., John Wiley & Sons (2013).

[11] S. DONALDSON: *Riemann Surfaces*, Oxford U.P. (2011).

[12] E. GALOIS: *The Testamentary Letter of 29 May 1832* in P. M. Neumann: *The mathematical writings of Évariste Galois*, European Math. Soc. (2011), 83-96.

[13] C. HERMITE: *Sur la résolution de l'équation du cinquième degré*. Comptes rendus de l'Académie des Sciences, XLVI, (1858) (I), 508-515.

[14] C.G.J. JACOBI: *Gesammelte Werke*, 7 voll. Reimer, Berlin. Ristampato da Chelsea, New York (1969).

[15] C. JORDAN: *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris (1870).

[16] F. KLEIN: *Lectures on the Icosahedron and The Solution of Equations of the Fifth Degree*, Dover (1956).

[17] R.P. LANGLAND: *Some Contemporary Problems with Origins in Jugendtraum*. Proceedings Symposia in Pure Mathematics vol. 28 (1976), 401-418.

[18] H. MCKEAN, V. MOLL: *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge U.P. (1999).

[19] V. PRASOLOV, Y. SOLOVYEV: *Elliptic Functions and Elliptic Integrals*, Am. Math. Soc. (1997).

[20] R.A. RANKIN: *Modular forms and functions*. - Cambridge U.P. (1997).

[21] R. REMMERT: *Classical Topics in Complex Function Theory*. Graduate Texts in Math. Springer (1998).

[22] P. RUFFINI: *Teoria generale delle equazioni in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto*, Stamperia di S. Tommaso d'Aquino, Bologna (1799).

[23] N. SCHAPPACHER: *On the history of Hilbert's twelfth problem: a comedy of errors*. Matériaux pour l'histoire des mathématiques au XXe siècle (Nice, 1996). Sèmin. Congr. 3. Paris: Société Mathématique de France. pp. 243-273.

[24] J.P. SERRE: *A Course in Arithmetic*. Graduate Texts in Math. Springer (1973).

[25] G. SHIMURA: *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton U.P. (1971).

[26] J. SHURMAN: *Geometry of the Quintic*, Wiley Interscience (1997).

[27] B.K. SPEARMAN, K.S. WILLIAMS: *Characterization of Solvable Quintics* $x^5 + ax + b = 0$, Amer. Math. Monthly **101** (1994), 986-982.

[28] E.W. VON TSCHIRNHAUS: *Nova methodus auferendi omnes terminos intermedios ex data aequatione*, Acta eruditorum (1683), 204-207.

[29] H. UMEMURA: *Resolution of Algebraic Equations by Theta Constants*, in D.Mumford, ed. *Tata Lectures on Theta*, vol. II, pp. 3.261-3.272, Birkhäuser, (1984).

[30] F. VIÈTE: *Analytic Art* (traduzione di T. R. Witmer). Kent, OH: Kent State University Press, (1983).

[31] S. G. VLĂDUȚ: *Kronecker's Jugendtraum and modular functions*. Studies in the Development of Modern Mathematics. 2. New York: Gordon and Breach Science Publishers. (1991).

[32] H. WEBER: *Lehrbuch der Algebra*, vol. III, 2° ed. Vieweg (1908).

[33] R.A. WILSON: *The Finite Simple Groups*, Graduate Texts in Math. 251, Springer (2009).

Ettore Carletti

E. Carletti è stato ricercatore confermato presso il Dipartimento di Matematica dell'Università di Genova. Si è occupato di funzioni L *in teoria dei numeri e geometria spettrale. È stato coautore (con M. Beltrametti, D. Gallarati e G. Monti Bragadin) di due volumi di geometria proiettiva per i tipi della Casa Editrice Boringhieri e di un volume di geometria algebrica pubblicato dall'European Mathematical Society.*