Estensioni di Galois e Anelli di Interi Algebrici

Leo Liberti

Novembre 1997

Sommario

Si prova che per ogni campo numerico F esiste un'estensione di Galois E tale che ogni ideale di $\mathcal{O}_F$ esteso in $\mathcal{O}_E$ diventa principale.

Estensioni di Galois e Anelli di Interi Algebrici

1 Introduzione

Lo scopo di questa breve dissertazione è quello di provare che per ogni campo numerico F esiste un'estensione di Galois E/F tale che, se ϕ è l'immersione dall'anello degli interi di F, $\mathcal{O}_F$, in $\mathcal{O}_E$, (i) per ogni ideale I di $\mathcal{O}_F$, l'ideale J_I di $\mathcal{O}_E$ generato da $\phi(I)$ è principale e (ii) $\phi^{-1}(J_I) = I$. A tale fine si utilizzerà la costruzione di E data da [St. & Tall] (9.12) che assicura che E soddisfi le condizioni (i) e (ii) sopra. Si mostrerà poi che l'estensione E non è unica e che la si può sempre scegliere in modo tale che E/F sia di Galois.

Il presente lavoro è suddiviso in cinque parti: questa introduzione, alcuni risultati concernenti la teoria di Galois classica, alcuni concernenti la teoria degli interi algebrici, il "teorema centrale di cui s'è accennato sopra, e, infine, un esempio. Le nozioni minime necessarie per intraprendere la lettura di quanto segue sono: definizioni e teoria basilare dei gruppi, anelli, campi, ideali di un anello, polinomi.

2 Teoria di Galois

La teoria di Galois permette di determinare sotto quali condizioni un polinomio a coefficienti su un campo F sia risolubile per mezzo di radicali. L'idea di Galois fu di esprimere il "grado di ignoranza delle radici per mezzo del gruppo G delle loro permutazioni. Se si conosce solo F l'ignoranza delle radici è totale e quindi G ha il massimo numero di elementi possibile (il che equivale a dire che ogni radice può essere mandata in ogni altra, o più semplicemente che "una vale l'altra). Prendendo via via in considerazione certe espressioni radicali $\{r_i \mid i < \infty\}$ nei coefficienti del polinomio si tolgono da G tutte le permutazioni che non fissano r_i. Se è possibile restringere G soddisfacendo ad alcune condizioni (che servono ad assicurare che r_i siano in effetti espressioni radicali nei coefficienti) fino a che G rimane composto di un solo elemento, l'identità, allora questo significa che possiamo distinguere ogni radice dalle altre, ovvero che conosciamo le radici, e le possiamo esprimere per mezzo delle espressioni r_i.

Emil Artin fu uno dei primi matematici che rese più formale questo concetto, e ancora adesso il suo approccio alla questione (vedi [Artin]) rimane forse il più valido. Un sunto sarebbe qui fuori luogo, e ci limitiamo pertanto a dare due delle definizioni fondamentali e alcuni risultati che saranno di utilità nella prova del "teorema centrale della dissertazione.

Si noti che i campi considerati sotto sono sempre numerici (cioè sottocampi del campo dei numeri complessi).

Definizione 2.1 *Sia F un campo e E un'estensione di F. Il gruppo di Galois di E su F, denotato da $Gal(E/F)$, è il gruppo di automorfismi di E che fissano F. E/F è un'estensione di Galois se E/F è di grado finito e il campo fisso di $Gal(E/F)$ è F.*

Artin usa il termine "estensione normale per "estensione di Galois, ma preferiamo in questa sede usare la terminologia di Clark (vedi [Clark]) e indicare con "estensione normale E di F un'estensione in cui ogni polinomio irriducibile su F con una radice in E si spezza in E. In [Clark] 129α si prova che se E è un'estensione finita di F e $\mathrm{char}(F) = 0$ allora E è di Galois se e solo se E è normale (di qui la apparente confusione di terminologia).

Teorema 2.1 *Se D è un'estensione finita di E e E è un'estensione finita di F allora D è un'estensione finita di F e $[D : F] = [D : E][E : F]$.*

Dimostrazione. Sia $\{\alpha_1, \ldots, \alpha_m\}$ una base di D su E e $\{\beta_1, \ldots, \beta_n\}$ una base di E su F. Allora $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_n\}$ è una base di D su F (le verifiche sono elementari). □

Teorema 2.2 (Teorema dell'Elemento Primitivo) *Se E/F è un'estensione finita, E è un'estensione semplice di F se e solo se c'è un numero finito di campi intermedî tra E e F.*

Dimostrazione. ($\Longrightarrow$): Sia $E = F(\beta)$ e sia K un campo intermedio. Siano $f(x) = \mathrm{mp}_F(\beta)$ e $g(x) = \mathrm{mp}_K(\beta)$ i polinomî minimi di β rispettivamente su F e su K. Sia $f(x) = p_1(x) \cdot \cdots \cdot p_n(x)$ una fattorizzazione di $f(x)$ in $E[x]$. Poiché $g(x)|f(x)$ esistono al massimo 2^n possibilità di scelta di $g(x)$. Supponiamo per assurdo che $g(x)$ determini due campi, K e K'. Sia $g(x) = x^d + \alpha_1 x^{d-1} + \cdots + \alpha_d$ a coefficienti in K. Sia $K' = F(\alpha_1, \ldots, \alpha_d) \subseteq K$. Ma $g(x) \in K'[x]$ e irriducibile implica che $[E : K'] = [E : K] = d$, perciò $[K : K'] = 1$ e quindi $K = K'$. Pertanto le possibilità di scelta per K sono minori o uguali a 2^n.

($\Longleftarrow$): Assumiamo che ci sia un numero finito di campi intermedî fra E e F. Siano $\alpha, \beta \in E$. Troveremo γ tale che $F(\alpha, \beta) = F(\gamma)$. Si considerino tutte le possibili espressioni della forma $\alpha + c\beta$ con $c \in F$. Visto che F è un campo numerico ha infiniti elementi, e dunque esistono infinite espressioni del genere. Ma i campi intermedî sono in numero finito, quindi esistono $c \neq d$ tali che $F(\alpha + c\beta) = F(\alpha + d\beta)$. Sia $\gamma = \alpha + c\beta$. Sappiamo che $\alpha + c\beta, \alpha + d\beta \in F(\gamma)$, perciò $0 \neq (c - d)\beta \in F(\gamma)$ e quindi $\beta = \frac{(c-d)\beta}{c-d} \in F(\gamma)$. Pertanto $c\beta \in F(\gamma) \Rightarrow \alpha = \gamma - c\beta \in F(\gamma)$ sicché $F(\alpha, \beta) \subseteq F(\gamma)$. L'altra inclusione è ovvia. Ora si scelga $\beta \in E$ tale che $[F(\beta) : F]$ sia massimo (ciò è possibile perché esiste un numero finito di campi intermedî) e supponiamo per assurdo che $\alpha \in E \backslash F(\beta)$. Allora esiste γ tale che $F(\gamma) = F(\alpha, \beta)$, ma $[F(\gamma) : F] > [F(\beta) : F]$ contraddicendo la scelta di β. Dunque $E = F(\beta)$. □

Teorema 2.3 *Se E/F è il campo di spezzamento di un polinomio separabile $p(x)$ su F allora $[E : F] = |Gal(E/F)|$.*

Dimostrazione. Per induzione su $[E : F]$. Se $[E : F] = 1$ allora $E = F$ e quindi l'unico automorfismo di E che lascia fisso F è l'identità, dunque $\mathrm{Gal}(E/F) = 1$. Sia ora $[E : F] > 1$, $g(x)$ un fattore irriducibile di $p(x)$ di grado maggiore di 1 (esiste perché altrimenti si avrebbe $[E : F] = 1$) e β una radice di $g(x)$ in E. Sia $\deg g(x) = d > 1$. Poiché $p(x)$ è separabile, tutti i suoi fattori irriducibili hanno radici distinte. Siano $\{\gamma_1, \ldots, \gamma_d\}$ le radici distinte di $g(x)$. Per il Teorema di Estensione dei Monomorfismi (vedi [Artin], teorema 8) esistono d isomorfismi distinti $\phi_i : F(\beta) \longrightarrow F(\gamma_i)$ che estendono l'identità di F. Per ogni $i \leq d$, per ipotesi induttiva, abbiamo $[E : F(\beta)]$ automorfismi (distinti) di E che estendono ϕ_i (e quindi che fissano F). Quindi $|\mathrm{Gal}(E/F)| = [E : F(\beta)] \cdot d = [E : F(\beta)] \deg g(x) = [E : F(\beta)][F(\beta) : F] = [E : F]$. □

Teorema 2.4 *E/F è di Galois se e solo se E è il campo di spezzamento di un polinomio separabile $p(x)$ su F.*

Dimostrazione. ($\Longleftarrow$): per induzione su n, il numero di radici di $p(x)$ in $E\backslash F$. Se tutte le radici di $p(x)$ sono in F allora $E = F$ e l'identità è l'unico automorfismo che lascia F fisso. Supponiamo $n \geq 1$ e sia $p(x) = p_1(x) \cdot p_2(x) \cdot \cdots \cdot p_r(x)$ una fattorizzazione di $p(x)$ in fattori irriducibili. Possiamo supporre $\deg p_1(x) = s > 1$ perché se tutti i $p_i(x)$ avessero grado 1 il polinomio si spezzerebbe in F e n sarebbe uguale a 0. Sia α_1 una radice di $p_1(x)$. Allora $[F(\alpha_1) : F] = \deg p_1(x) = s$. Se consideriamo $F(\alpha_1)$ come il campo su cui $p(x)$ è definito, meno di n radici di $p(x)$ sono in $E\backslash F(\alpha_1)$, inoltre E è il campo di spezzamento di $p(x)$ su $F(\alpha_1)$. Dunque per ipotesi induttiva E è un'estensione di Galois di $F(\alpha_1)$ e quindi ogni elemento in E che non è in $F(\alpha_1)$ è mosso da almeno un automorfismo che fissa $F(\alpha_1)$. Poiché $p(x)$ è separabile, le radici $\alpha_1, \ldots, \alpha_s$ di $p_1(x)$ sono distinte. Per il Teorema di Estensione dei Monomorfismi (vedi [Artin], teorema 8) l'isomorfismo identità $F \longrightarrow F$ si estende ad isomorfismi $\overline{\sigma_1}, \ldots, \overline{\sigma_s}$ da $F(\alpha_1)$ rispettivamente ad $F(\alpha_1), \ldots, F(\alpha_s)$ tali che $\overline{\sigma_i}(\alpha_1) = \alpha_i$. Per il teorema 10 di [Artin] $\overline{\sigma_1}, \ldots, \overline{\sigma_s}$ si possono estendere ad automorfismi $\sigma_1, \ldots, \sigma_s$ di E che fissano F. Sia ora θ un elemento di E che rimane fisso sotto l'azione di tutti gli automorfismi di E che fissano F. Sappiamo che $\theta \in F(\alpha_1)$ perché $E/F(\alpha_1)$ è di Galois, dunque si può scrivere $\theta = c_0 + c_1\alpha_1 + \cdots c_{s-1}\alpha_1^{s-1}$ dove i c_i stanno in F. Applicando σ_i a θ e considerando che $\forall i \leq s$ $(\sigma_i(\theta) = \theta)$ si ottiene che il polinomio $f(x) = c_{s-1}x^{s-1} + \cdots + c_1 x + (c_0 - \theta)$ ha s radici distinte $\alpha_1, \ldots, \alpha_s$ da cui $f(x) = 0$ e quindi $\theta = c_0 \in F$. Dunque E/F è di Galois.

($\Longrightarrow$): sia $\alpha \in E$ e $\mathrm{Gal}(E/F) = \{\sigma_1, \ldots, \sigma_s\}$. Siano $\alpha_1, \ldots, \alpha_r$ le immagini distinte di α sotto gli elementi di $\mathrm{Gal}(E/F)$. Per ogni $i \leq r, j \leq s$ esistono k, m, n tali che $\sigma_j(\alpha_i) = \sigma_j\sigma_k(\alpha) = \sigma_m(\alpha) = \sigma_n$, dunque $\mathrm{Gal}(E/F)$ è un gruppo di permutazioni delle α_i. Sia $f(x) = \prod_{i=1}^{r}(x - \alpha_i)$. Allora $\forall \sigma \in \mathrm{Gal}(E/F)$ $(\sigma(f(x)) = f(x))$ e pertanto i coefficienti di $f(x)$ stanno in F. Sia ora $g(x)$ tale che $g(\alpha) = 0$. Allora applicando gli elementi σ_i di $\mathrm{Gal}(E/F)$ si ottiene che $\forall i \leq r$ $(g(\alpha_i) = 0)$ e quindi $\deg g(x) \geq s$. Dunque $f(x)$ è irriducibile e perciò separabile ($\alpha_1, \ldots, \alpha_r$ sono distinti). Sia ora $[E : F] = n$ e $\{\omega_1, \ldots, \omega_n\}$ una base dello spazio vettoriale E su F. Siano $p_1(x), \ldots, p_n(x)$ i polinomî separabili irriducibili di (rispettivamente) $\omega_1, \ldots, \omega_n$ costruiti come descritto sopra. Sia $p(x) = \prod_{i=1}^{n} p_i(x)$. Allora $p(x)$ è separabile e E è il suo campo di spezzamento. □

Teorema 2.5 *Sia E il campo di spezzamento del polinomio $f(x)$ a coefficienti in F. Allora $Gal(E/F)$ è un gruppo di permutazioni delle radici di $f(x)$.*

Dimostrazione. Sia α una radice di $f(x)$ e sia $\phi \in \mathrm{Gal}(E/F)$. ϕ fissa F, dunque $\phi(f(\alpha)) = f(\phi(\alpha))$ e quindi $\phi(\alpha)$ è una radice di $f(x)$. □

Teorema 2.6 (Teorema Fondamentale della Teoria di Galois) *Sia E/F un'estensione di Galois e B un campo intermedio fra E e F. Allora*

(i) E/B è un'estensione di Galois e $Gal(E/B)$ è un sottogruppo di $Gal(E/F)$.
(ii) B/F è un'estensione di Galois se e solo se $Gal(E/B)$ è un sottogruppo normale di $Gal(E/F)$ nel qual caso $Gal(B/F)$ è isomorfo a $Gal(E/F)/Gal(E/B)$.

Dimostrazione. (i): Per il teorema 2.4 E/F è di Galois $\Rightarrow$ E è il campo di spezzamento di un polinomio separabile $f(x)$ su F. Ma $f(x)$ è separabile su B, sicché ancora per il teorema 2.4 E/B è di Galois. Per il teorema 2.2 $\exists \alpha \in E$ $(B = F(\alpha))$, dunque $\mathrm{Gal}(E/B) \leq \mathrm{Gal}(E/F)$.

(ii): Si noti che (A) $\forall \sigma \in \mathrm{Gal}(B/F)$ $\exists \tilde{\sigma} \in \mathrm{Gal}(E/F)$ $(\tilde{\sigma}|_B = \sigma)$ e che (B) se $N = \{\tilde{\sigma} \in \mathrm{Gal}(E/F) | \tilde{\sigma}(B) = B\}$ e $\Phi : N \longrightarrow \mathrm{Gal}(B/F)$ è data da $\Phi(\tilde{\sigma}) = \tilde{\sigma}|_B$, allora per (A) Φ è suriettiva e $\mathrm{Ker}\ \Phi = \mathrm{Gal}(E/B)$.

($\Longleftarrow$): Se $\mathrm{Gal}(E/B) \lhd \mathrm{Gal}(E/F)$ allora $\forall \sigma \in \mathrm{Gal}(E/B)$ $\forall \tau \in \mathrm{Gal}(E/F)$ $\exists \sigma_\tau \in \mathrm{Gal}(E/B)$ $(\tau^{-1}\sigma\tau = \sigma_\tau)$. Sia $b \in B$. Poiché E/B è di Galois, B è il campo fisso di $\mathrm{Gal}(E/B)$, dunque $\forall \sigma \in \mathrm{Gal}(E/B)$ $(\sigma\tau(b) = \tau\sigma_\tau(b) = \tau(b))$, quindi $\tau(b) \in B$ e $\tau \in N$. Pertanto si ha che $N = \mathrm{Gal}(E/F)$, sicché $N/\mathrm{Ker}\ \Phi \cong \mathrm{Im}\ \Phi$ da cui $\mathrm{Gal}(B/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/B)$. Ne segue che se F' è il campo fisso di $\mathrm{Gal}(B/F)$ si ha

$$[B : F'] = |\mathrm{Gal}(B/F)| = |\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B)| = [B : F]$$

e quindi $F' = F$ e B/F è di Galois.

($\Longrightarrow$): Se B/F è di Galois allora $[B : F] = \frac{|N|}{[E:B]}$ da cui

$$|N| = [E : B][B : F] = [E : F] = |\mathrm{Gal}(E/F)| \Rightarrow N = \mathrm{Gal}(E/F)$$

Ora $\mathrm{Ker}\ \Phi \lhd N \Rightarrow \mathrm{Gal}(E/B) \lhd \mathrm{Gal}(E/F)$. □

3 Teoria degli Interi Algebrici

Le definizioni e i teoremi di questa sezione, salvo dove indicato diversamente, sono stati presi da [St. & Tall].

Definizione 3.1 *Sia $\mathcal{B}$ l'insieme di tutte le radici di polinomi monici a coefficienti in $\mathcal{Z}$ (cioè a coefficienti interi). Gli elementi di $\mathcal{B}$ sono chiamati interi algebrici. $\mathcal{B}$ è un anello con le solite operazioni di somma e prodotto. Sia F un campo numerico. $\mathcal{O}_F = F \cap \mathcal{B}$ è chiamato l'anello degli interi di F.*

Definizione 3.2 *Sia F un campo e $\mathcal{I}$ l'insieme degli ideali di $\mathcal{O}_F$. Si definisca la relazione d'equivalenza $\sim$ su $\mathcal{I}$ in modo che $\forall I, J \in \mathcal{I}$ $(I \sim J \Longleftrightarrow$ esistono ideali principali $H, L \in \mathcal{I}$ tali che $IH = JL)$. Si indichi con $[I]$ la classe di equivalenza di I. L'insieme di tutte le classi di equivalenza così ottenute con il prodotto $[I][J] = [IJ]$ formano un gruppo che si chiama il gruppo di classe di $\mathcal{O}_F$ e si indica con $GCl(F)$. L'ordine di $GCl(F)$ si chiama il numero di classe.*

Teorema 3.1 *Il gruppo di classe di un campo numerico è un gruppo abeliano finito. Di conseguenza il numero di classe è finito.*

La dimostrazione di questo teorema, nella trattazione di [St. & Tall], segue da alcune considerazioni di teoria dei reticoli, e perciò esula dall'argomento di questa ricerca.

Teorema 3.2 *Sia F un campo numerico con numero di classe h e I un ideale di $\mathcal{O}_F$. Allora I^h è principale.*

Dimostrazione. Per il teorema 3.1 per ogni elemento $[I]$ di $\mathrm{GCl}(F)$ si ha $[I]^h = [\mathcal{O}_F]$, che è l'identità del gruppo di classe; dunque $[I^h] = [\mathcal{O}_F]$ e quindi I^h è principale. □

Teorema 3.3 *Sia F un campo numerico e I un ideale di $\mathcal{O}_F$. Allora esiste un intero algebrico κ tale che, se $\mathcal{O} = \mathcal{O}_{F(\kappa)}$*

(i) $\mathcal{O}\kappa = \mathcal{O}I$
(ii) $(\mathcal{O}\kappa) \cap \mathcal{O}_F = I$
(iii) $(\mathcal{B}\ \kappa) \cap F = I$
(iv) Se $\mathcal{O}'\gamma = \mathcal{O}'I$ *per qualche* $\gamma \in \mathcal{B}$ *e qualsiasi anello* $\mathcal{O}'$ *di interi allora* $\gamma = u\kappa$ *dove* u *è un'unità di* $\mathcal{B}$.

Dimostrazione. (i): Sia h il numero di classe di F. Per il teorema 3.2 si ha che I^h è principale, diciamo $I^h =< \omega >$. Sia $\kappa = \omega^{\frac{1}{h}} \in \mathcal{B}$. Allora $\kappa \in \mathcal{O}$. Inoltre si ha $(\mathcal{O}I)^h = \mathcal{O}(I^h) = \mathcal{O}\omega = \mathcal{O}\kappa^h = (\mathcal{O}\kappa)^h$. Per ([St. & Tall] 4.8) si ha che in $\mathcal{O}$ gli ideali hanno fattorizzazione unica, pertanto $\mathcal{O}I = \mathcal{O}\kappa$.

(ii): (iii) $\Longrightarrow$ (ii).

(iii): Supponiamo $\gamma \in \mathcal{B}\kappa \cap F$. Allora $\exists\lambda \in \mathcal{B}\ (\gamma = \lambda\kappa)$. Si noti che $\gamma \in F$ e $\kappa \in F(\kappa)$ implicano che $\lambda = \gamma\kappa^{-1} \in F(\kappa)$, quindi $\lambda \in \mathcal{O}$, perciò $\gamma^h = \lambda^h\kappa^h = \lambda^h\omega \in \mathcal{B}$, e dunque $\gamma \in B$. Quindi $\gamma \in \mathcal{B}\ \cap F = \mathcal{O}_F$. Inoltre $\lambda^h = \gamma^h\omega^{-1} \in F \Rightarrow \lambda^h \in \mathcal{B}\ \cap F = \mathcal{O}_F$. Dunque si ha

$$\gamma^h = \lambda^h\omega \qquad \text{con } \gamma, \lambda^h, \omega \in \mathcal{O}_F$$

da cui

$$< \gamma >^h = < \lambda^h >< \omega > = < \lambda^h > I^h$$

La fattorizzazione unica degli ideali in $\mathcal{O}_F$ implica che $\exists J$ ideale di $\mathcal{O}_F$ ($< \lambda^h >= J^h$), e quindi $< \gamma >^h = J^hI^h$ da cui ancora $< \gamma >= JI$ e dunque $\gamma \in I$. L'altra inclusione è ovvia.

(iv): Per ([St. & Tall] 5.14) $I =< \alpha, \beta >$ per $\alpha, \beta \in \mathcal{O}_F$, e quindi $\mathcal{O}'\gamma = \mathcal{O}' < \alpha, \beta >$ dunque esistono $\lambda, \mu \in \mathcal{O}'$ tali che $\gamma = \lambda\alpha + \mu\beta$, pertanto, per (i), $\alpha, \beta \in \mathcal{O}\kappa$, sicché $\alpha = \eta\kappa, \beta = \xi\kappa(\eta, \xi \in \mathcal{O} \subseteq \mathcal{B}\ )$. Di qui $\gamma = \lambda\eta\kappa + \mu\xi\kappa$ e $\kappa|\gamma$ in $\mathcal{B}$. Scambiando γ e κ si ottiene $\gamma|\kappa$ e dunque $\gamma = u\kappa$ per qualche unità u di $\mathcal{B}$. □

Per trovare il κ summenzionato si nota come $[I]^h$ deve essere l'identità di $\mathrm{GCl}(F)$. Ma non è detto che per ogni ideale I di $\mathcal{O}_F$ h sia il minimo tale che $[I]^h = [\mathcal{O}_F]$. Supponiamo dunque che I sia tale che esiste $s < h$ tale che $[I]^s = [\mathcal{O}_F]$. Per il teorema di Lagrange, $s|h$. I^s è un ideale principale, diciamo $I^s =< \eta >$, e ovviamente anche I^h è principale, diciamo $I^h =< \omega >$. Allora si ha $< \omega >=< \eta >^{\frac{h}{s}}$. Si può assumere senza perdita di generalità che $\omega = \eta^{\frac{h}{s}}$, e dunque $\omega^{\frac{1}{h}} = \eta^{\frac{1}{s}}$. Nella dimostrazione del teorema 3.3 κ era stato definito come $\omega^{\frac{1}{h}}$, pertanto si vede che κ è indipendente dalla scelta dell'esponente a cui si eleva I per arrivare all'identità di $\mathrm{GCl}(F)$.

Teorema 3.4 *Sia F un campo numerico. Allora esiste un'estensione E di F tale che per ogni ideale I di $\mathcal{O}_F$ si ha (i) $\mathcal{O}_EI$ è principale (ii) $(\mathcal{O}_EI) \cap \mathcal{O}_F = I$.*

Dimostrazione. (i): Sia h il numero di classe di F. Siano $[I_1], \ldots, [I_h]$ gli elementi di $\mathrm{GCl}(F)$ e $\kappa_1, \ldots, \kappa_h$ interi algebrici tali che $\forall i \leq h$ ($\mathcal{O}_{F(\kappa_i)}I_i$ è principale) (i κ_i esistono per il teorema 3.3 (i)). Sia $E = F(\kappa_1, \ldots, \kappa_h)$. Si ha che $\forall i \leq h$ ($\mathcal{O}_EI_i$ è principale). Ma ogni ideale I di $\mathcal{O}_F$ è equivalente a qualche I_i.

(ii): Con la stessa notazione del teorema 3.3, parte (iv), $\alpha = u\kappa$ dove u è un'unità di $\mathcal{B}$. Dunque

$$\begin{aligned}(\mathcal{O}_EI) \cap \mathcal{O}_F &= (\mathcal{O}_E\alpha) \cap \mathcal{O}_F \\ &\subseteq (\mathcal{B}\alpha) \cap F \\ &= (\mathcal{B}\kappa) \cap F \\ &= I\end{aligned}$$

per il teorema 3.3 (iii). L'altra inclusione è ovvia. □

4 Il Teorema Centrale

Si noti che tutti gli indici numerici appartengono ai numeri naturali.

Definizione 4.1 *Sia E un'estensione del campo F e $\beta \in E$. Sia $\alpha \in E$. β è dipendente da α se $\beta \in F(\alpha)$. Sia $S \subseteq E$. β è dipendente da S se $\beta \in D$, dove D è il campo generato da F e S. S è indipendente se non esiste $\gamma \in S$ tale che γ è dipendente da $S \backslash \{\gamma\}$. S è dipendente se non è indipendente.*

Teorema 4.1 *Sia F un campo numerico e $\mathcal{O}_F$ il suo anello degli interi. Allora esiste un'estensione di Galois E di F tale che per ogni ideale I di $\mathcal{O}_F$ si ha che (i) $\mathcal{O}_E I$ è principale e (ii) $(\mathcal{O}_E I) \cap \mathcal{O}_F = I$.*

Dimostrazione. Sia $\mathrm{GCl}(F) = \{[I_1], \ldots, [I_h]\}$ il gruppo di classe di F (di ordine h). Si può assumere che $[I_1]$ sia l'identità $[\mathcal{O}_F]$ e che $I_1 = \mathcal{O}_F =< 1 >$. Sia $\omega_1 = 1$. Per il teorema di Lagrange, $\forall i \leq h$ $([I_i]^h = [\mathcal{O}_F])$ da cui per ogni $i \leq h$ si ha che I_i^h è principale, diciamo $I_i^h =< \omega_i >$ dove $\omega_i \in \mathcal{O}_F$. Ora, per ogni $i \leq h$ sia $p_i(x) = x^h - \omega_i$. Sia $\kappa_1 = \zeta = e^{\frac{2\pi\sqrt{-1}}{h}}$ e per ogni i maggiore di 1 e minore o uguale a h sia κ_i una radice di $p_i(x)$. Sia $E = F(\kappa_1, \ldots, \kappa_h)$. Per costruzione (cfr. dimostrazioni dei teoremi 3.3, 3.4) E è un'estensione di F che soddisfa le condizioni (i) e (ii) della tesi. Rimane da mostrare che E/F è di Galois. Si ha che $\omega_1, \ldots, \omega_h$ sono distinti: supponiamo per assurdo che $\omega_i = \omega_j$ con $i \neq j$. Allora $I_i^h = I_j^h$. Poiché abbiamo la fattorizzazione unica degli ideali si conclude che $I_i = I_j \Rightarrow [I_i] = [I_j]$ e quindi $|GCl(F)| = h - 1$, che è una contraddizione con quanto supposto prima. Ora restringiamo l'insieme $\{\kappa_1, \ldots, \kappa_m\}$ in modo che diventi un insieme indipendente (nel senso della definizione precedente). Rinumerando i κ_i se necessario, esiste $l \leq m$ tale che $\kappa_{l+1}, \ldots, \kappa_m$ sono dipendenti dall'insieme indipendente $\{\kappa_1, \ldots, \kappa_l\}$, dunque $E = F(\kappa_1, \ldots, \kappa_l)$ e

$$\forall i \leq l \ (F(\kappa_1, \ldots, \kappa_{i-1}, \kappa_{i+1}, \ldots, \kappa_l) \text{ è un sottocampo proprio di } E)$$

Sia $p(x) = \prod_{i=1}^{m} p_i(x)$. Poiché $\omega_1, \ldots, \omega_m$ sono distinti, $p(x)$ è separabile. Chiaramente $p(x)$ si spezza in E ma non si spezza in alcun campo B propriamente contenuto in E, dunque E è il campo di spezzamento di un polinomio separabile su F, e pertanto, stante il teorema 2.4, E/F è di Galois. □

4.1 Il gruppo di Galois $\mathbf{Gal}(E/F)$

La struttura particolare di $\mathrm{Gal}(E/F)$ dipende ovviamente da F stesso, e quindi varia caso per caso. È tuttavia possibile fare alcune considerazioni generali sull'ordine di $\mathrm{Gal}(E/F)$. Per il teorema 2.3 $|\mathrm{Gal}(E/F)| = [E : F]$. È possibile formare una catena di campi intermedî fra $E = F(\kappa_1, \ldots, \kappa_l)$ (con $\{\kappa_1, \ldots, \kappa_l\}$ indipendente) e F di lunghezza $l + 1$:

$$E = F(\kappa_1, \ldots, \kappa_l) \supset F(\kappa_1, \ldots, \kappa_{l-1}) \supset \ldots \supset F(\kappa_1) \supset F$$

Per il teorema 2.1 si ha che

$$[E : F] = \prod_{i=1}^{l} [F(\kappa_1, \ldots, \kappa_i) : F(\kappa_1, \ldots, \kappa_{i-1})] = \prod_{i=0}^{l-1} \deg \mathrm{mp}_{F(\kappa_1, \ldots, \kappa_i)}(\kappa_{i+1})$$

dove $\mathrm{mp}_F(\kappa)$ è il polinomio minimo di κ su F. Per l'indipendenza di $\{\kappa_1, \ldots, \kappa_l\}$ abbiamo

$$\forall i \leq l \ (\mathrm{mp}_{F(\kappa_1, \ldots, \kappa_{i-1})}(\kappa_i) = \mathrm{mp}_F(\kappa_i))$$

e dunque

$$|\mathrm{Gal}(E/F)| = \prod_{i=1}^{l} \deg \mathrm{mp}_F(\kappa_i)$$

Evidentemente $\forall i \leq l$ $(\deg \mathrm{mp}_F(\kappa_i) \leq h)$, e inoltre per $\kappa_1 = \zeta$ è noto che $\deg \mathrm{mp}_{\mathcal{Q}}(\zeta) \leq h - 1$, quindi $\deg \mathrm{mp}_F(\kappa_1) \leq h - 1$. A questo punto è possibile effettuare la stima seguente: $|\mathrm{Gal}(E/F)| \leq h^{l-1}(h-1)$. Nel caso in cui si abbia l'eguaglianza e in cui h sia un numero primo si possono applicare i teoremi di Sylow per studiare ulteriormente la struttura di $\mathrm{Gal}(E/F)$.

5 L'Analisi di $\mathcal{Q}(\sqrt{-5})$

Prenderemo come esempio illustrativo dell'applicazione del teorema 4.1 il campo $F = \mathcal{Q}(\sqrt{-5})$. La ragione principale di questa scelta è che forse l'esempio più conosciuto di anello non a fattorizzazione unica (e quindi non a ideali principali) è $\mathcal{Z}(\sqrt{-5})$. Proveremo dunque che l'anello degli interi di $\mathcal{Q}(\sqrt{-5})$ è $\mathcal{Z}(\sqrt{-5})$e troveremo un'estensione E di $\mathcal{Q}(\sqrt{-5})$ di Galois che soddisfa a (i) e (ii) dell'enunciato del teorema 4.1.

5.1 Metodi di calcolo dell'anello degli interi di un campo

Le tecniche per calcolare gli anelli di interi $\mathcal{O}_F$ di un campo numerico F sono quelle descritte nella sezione 2.6 di [St. & Tall]: l'idea è di iniziare con un tentativo iniziale approssimato $\mathcal{O}$ (il cui gruppo additivo è un gruppo abeliano libero G di dimensione finita) e calcolare il discriminante Δ_G della base di $\{\alpha_1, \ldots, \alpha_n\}$ di G. Successivamente, per ogni primo p il cui quadrato divide Δ_G controllare quali numeri della forma

$$\frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n) \qquad \text{con } 0 \leq \lambda_i \leq p-1 \text{ e } \lambda_i \in \mathcal{Z}\ \forall i \leq n \tag{1}$$

sono interi algebrici di F. Se si trova qualche nuovo intero β con questo procedimento si deve estendere $\mathcal{O}$ a $\mathcal{O}'$ (con gruppo libero additivo G') in modo che $\beta \in \mathcal{O}'$ e dividere Δ_G per p^2 per ottenere $\Delta_{G'}$ e applicare ricorsivamente questo procedimento fino ad esaurimento dei fattori primi di $\Delta_{G'}$.

Per il caso in cui la base di G sia della forma $\{1, \theta, \ldots, \theta^{n-1}\}$ si può prendere come definizione di Δ_G, ai fini del semplice calcolo numerico, l'espressione

$$\Delta_G = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2 \qquad \text{con } \{\theta_1, \ldots, \theta_n\} \text{ coniugati di } \theta \tag{2}$$

anche se questa non è la definizione usuale del discriminante. Vedi a questo proposito [St. & Tall], pag. 44. Vedi anche le definizioni di traccia e norma in *ibid.*, pag. 54.

Teorema 5.1 *L'anello degli interi di* $\mathcal{Q}(\sqrt{-5})$ *è* $\mathcal{Z}(\sqrt{-5})$.

Dimostrazione. Il campo $\mathcal{Q}(\sqrt{-5})$, preso come spazio vettoriale su $\mathcal{Q}$, ha base $\{1, \sqrt{-5}\}$. Prendiamo come tentativo iniziale $\mathcal{O}$ l'anello generato dal gruppo libero G con base $\{1, \sqrt{-5}\}$. Dunque $\mathcal{O} = \mathcal{Z}(\sqrt{-5})$. Usando l'espressione (2) calcoliamo $\Delta_G = (\sqrt{-5} - (-\sqrt{-5}))^2 = -2^2 \cdot 5$. L'unico primo p il cui quadrato divide Δ_G è $p = 2$, pertanto bisogna controllare tutti i numeri della forma $\alpha = \frac{1}{2}(\lambda_1 + \lambda_2\sqrt{5})$ dove $0 \leq \lambda_1, \lambda_2 \leq 1$ (vedi l'espressione (1)). La traccia di α è $\mathrm{T}(\alpha) = \frac{1}{2}\lambda_1$. Poiché $\mathrm{T}(\alpha) \in \mathcal{Z}$ si ha che $2|\lambda_1$ e quindi $\lambda_1 = 0$. Dunque $\alpha = \frac{\lambda_2\sqrt{-5}}{2}$. La norma di α è $\mathrm{N}(\alpha) = \frac{5\lambda_2}{2}$; poiché $\mathrm{N}(\alpha) \in \mathcal{Z}$ si ottiene che $2|\lambda_2$ e quindi $\lambda_2 = 0$. Di conseguenza l'anello degli interi di $\mathcal{Q}(\sqrt{-5})$ è $\mathcal{Z}(\sqrt{-5})$. □

5.2 Costruzione di E

Seguendo la dimostrazione del teorema 4.1, che è costruttiva, ci proponiamo di trovare un'estensione E di $\mathcal{Q}(\sqrt{-5})$ che sia di Galois e nel cui anello degli interi ogni ideale di $\mathcal{Z}(\sqrt{-5})$ diventi principale, pur "comportandosi bene rispetto all'operazione di estensione e contrazione di ideali.

Il gruppo di classe di $\mathcal{Q}(\sqrt{-5})$ è

$$\mathrm{GCl}(\mathcal{Q}(\sqrt{-5})) = \{[\mathcal{Z}(\sqrt{-5})], [< 2, 1 + \sqrt{-5} >]\} \cong \mathrm{C}_2$$

e $< 2, 1 + \sqrt{-5} >^2 =< 2 >$ (vedi [St. & Tall] pag. 171). Dunque si definiscono $\omega_1 = 1, \omega_2 = 2$, e poiché $h = 2$, $\kappa_1 = -1, \kappa_2 = \sqrt{2}$. ω_1, ω_2 sono distinti, perciò nella notazione della dimostrazione del teorema 4.1 $m = h = 2$. Tuttavia $\kappa_1 = -1 \in F$ mentre κ_2 è indipendente da F, e pertanto $l = 1$ e si ridefinisce $\kappa_1 = \sqrt{2}$. Infine si ha che $E = F(\sqrt{2}) = \mathcal{Q}(\sqrt{2}, \sqrt{-5})$.

5.3 Considerazioni su $E/\mathcal{Q}$

Attiriamo l'attenzione sul fatto che il nostro risultato non prova che $E/\mathcal{Q}$ sia di Galois. In questo caso specifico, tuttavia, è evidente che E è il campo di spezzamento del polinomio separabile $(x^2-2)(x^2+5) = x^4 + 3x^2 - 10$, sicché, stante il teorema 2.4, $E/\mathcal{Q}$ è un'estensione di Galois. Per il teorema 2.2, esiste un elemento θ tale che $E = \mathcal{Q}(\theta)$. Ora, abbiamo che

$$\begin{aligned}
\sqrt{-10} &= \frac{1}{2}[(\sqrt{2} + \sqrt{-5})^2 + 3] \\
\sqrt{-5} &= \frac{1}{3}[5(\sqrt{2} + \sqrt{-5}) - \sqrt{-10}(\sqrt{2} + \sqrt{-5})] \\
\sqrt{2} &= (\sqrt{2} + \sqrt{-5}) - \sqrt{-5}
\end{aligned}$$

Quindi $\mathcal{Q}(\sqrt{2},\sqrt{-5}) \subseteq \mathcal{Q}(\sqrt{2}+\sqrt{-5})$. L'altra inclusione è ovvia, da cui l'uguaglianza. Ora, $\theta = \sqrt{2}+\sqrt{-5}$ ha polinomio minimo x^4+6x^2+49, pertanto

$$|\mathrm{Gal}(E/\mathcal{Q}\ )| = [E : \mathcal{Q}\ ] = [\mathcal{Q}(\theta) : \mathcal{Q}\ ] = 4$$

Per il teorema 2.1 si ha che $4 = [E : \mathcal{Q}\ ] = [E : F][F : \mathcal{Q}\ ] = 2 \cdot 2$, dunque $\mathrm{Gal}(E/F) \cong \mathrm{C}_2$. Il gruppo di Galois di $E/\mathcal{Q}$ ha ordine 4, quindi è C_4 oppure $\mathrm{C}_2 \times \mathrm{C}_2$. Per il teorema 2.5 $\mathrm{Gal}(E/\mathcal{Q}\ ) = \mathrm{Gal}(\mathcal{Q}(\theta)/\mathcal{Q}\ )$ è un gruppo di permutazioni delle radici di x^4+6x^2+49 che sono

$$\begin{aligned}
\theta_1 &= \sqrt{2}+i\sqrt{5} \\
\theta_2 &= \sqrt{2}-i\sqrt{5} \\
\theta_3 &= -\sqrt{2}+i\sqrt{5} \\
\theta_4 &= -\sqrt{2}-i\sqrt{5}
\end{aligned}$$

Sia σ la coniugazione complessa e ρ la mappa indotta da $1 \longrightarrow -1$. Allora

$$\mathrm{Gal}(\mathcal{Q}(\theta)/\mathcal{Q}) \ = < \rho, \sigma \mid \rho^2 = \sigma^2 = e, \rho\sigma = \sigma\rho > \cong \ \mathrm{D}_4 \ \cong \ \mathrm{C}_2 \times \mathrm{C}_2$$

Per il teorema 2.6 si ottiene che $[F : \mathcal{Q}\ ]$ è di Galois e $\mathrm{Gal}(F/\mathcal{Q}\ ) \cong \mathrm{C}_2$.

Riferimenti bibliografici

[Artin] Artin, Emil, *Galois Theory*, Notre Dame University Press, Indiana, 1959 (quarta ed., 1966)

[Clark] Clark, Allan, *Elements of Abstract Algebra*, Dover, New York, 1984

[Pretzel] Pretzel, Oliver, *Galois Theory*, Unpublished lecture notes from lectures held at Imperial College, London, 1994

[St. & Tall] Stewart, Ian, and Tall, David, *Algebraic Number Theory*, Chapman & Hall, London, 1979 (seconda ed., 1987)

[Stewart] Stewart, Ian, *Galois Theory*, Chapman & Hall, London, 1973