Introduzione alla Teoria di Galois

Andrea Previtali

Sabato, 15 Settembre 2001

1 Nozioni preliminari

Lo scopo del corso è di descrivere la Teoria di Galois, ossia come usare la teoria dei gruppi nello studio della struttura dei campi. Abbiamo preliminarmente bisogno di introdurre alcuni concetti relativi alla divisibilità negli anelli, l'esempio più importante per noi restando quello dei polinomi o delle funzioni razionali.

1.1 Divisibilità

Nel resto di questa sezione indicheremo con A un anello commutativo dotato di identità che denoteremo con 1 o 1_A. Nostra intenzione è definire un concetto di divisibilità in A che ricordi l'analoga nozione sugli interi $\mathbb{Z}$. Benché esista una teoria della divisibilità nel caso non commutativo, noi ci limiteremo al caso commutativo per semplicità.

Definizione 1.1. *Dati $a, b \in A$, diremo che a divide b, $a \mid b$, se esiste $c \in A$ tale che $b = ac$.*

Esercizio 1.2. *Mostrare che ogni elemento di A divide 0.*

Definizione 1.3. *Se $u \in A$ divide 1, diremo che u è un'***unità** *o un elemento invertibile di A. Indicheremo l'insieme delle* *unità di A con $A^{\#}$ (riservando ad A^* il significato di $A \setminus \{0\}$).*

Ad esempio $\mathbb{Z}^{\#} = \{\pm 1\}$.

Esercizio 1.4. *Provare che $A^{\#}$ è un gruppo rispetto al prodotto definito in A.*

Definizione 1.5. *Due elementi a, b di A si dicono* **associati***, $a \approx b$, se $a = ub$, con $u \in A^{\#}$.*

Esercizio 1.6. *Mostrare che $\approx$ definisce una relazione di equivalenza su A.*

Definizione 1.7. *Un anello commutativo A viene detto un* **dominio** *se $ab = 0$ implica che a o b è nullo.*

Esercizio 1.8. *Dimostrare che se D è un dominio di integrità finito, allora $|D| = 1 + k|D^{\#}|$, per qualche intero k o, in notazione modulare, $|D| \equiv_{|D^{\#}|} 1$.*

In realtà k risulta essere sempre 1.

Esercizio 1.9. *(Difficile) Provare che $k = 1$. Cosa afferma questo risultato sulla struttura dei domini di integrità finiti?*

Nel seguito restringeremo ulteriormente il nostro universo considerando solo domini di integrità che denoteremo generalmente con D.

Definizione 1.10. *Un elemento non invertibile e non nullo p di un dominio D viene detto* **primo** *se $p|ab$ implica $p|a$ o $p|b$.*

Esercizio 1.11. *Mostrare che questa definizione in $\mathbb{Z}$ fornisce esattamente i numeri primi e i loro opposti.*

Definizione 1.12. *Un elemento $0 \neq a$ di $D \setminus D^{\#}$ viene detto* **irriducibile** *o* **atomo** *se $b|a$ implica $b \approx a$ o $b \in D^{\#}$. Indicheremo con $\mathcal{A}(D)$ l'insieme degli atomi di D.*

Esercizio 1.13. *Se mancasse la locuzione "non nullo" nella definizione, lo zero sarebbe primo? In generale può* 0 *essere irriducibile?*

Si noti che questa è la classica definizione di numero primo in $\mathbb{Z}$. Infatti mostriamo che un elemento primo è un atomo.

Proposizione 1.14. *Sia* $p \in D$ *primo, allora* p *è un atomo.*

Dim. Sia a un divisore di p, allora $p = ab$ per qualche $b \in D$. Quindi $p|ab$ e, per definizione, p uno dei fattori, diciamo a. Quindi $a = pc$ e $a(1 - bc) = 0$. Essendo $p \neq 0$ e D un dominio, allora $bc = 1$ e $b \in D^{\#}$, cioè $p \approx a$. q.e.d.

Nota 1.15. *Il viceversa non vale, ossia esistono atomi che non sono primi, ma gli esempi sono più difficili da trovare, quello tipico consiste in* $D = \mathbb{Z}[\sqrt{-5}]$*, ove* $2 + \sqrt{-5}$ *è irriducibile, divide* 9*, ma non divide* 3*.*

Dim. Si denoti con N la norma, ossia la mappa definita da D in $\mathbb{Z}$ come $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Siccome $N(\alpha) = \alpha\overline{\alpha}$, allora $N(\alpha\beta) = N(\alpha)N(\beta)$. Inoltre $u \in D^{\#}$ sse $N(u) = 1$. Ora $9 = N(3) = N(2 + \sqrt{-5})$, quindi $2 + \sqrt{-5}|9$ e, se $2 + \sqrt{-5}$ dividesse 3, avremmo che $2 + \sqrt{-5} \approx 3$. Ma $D^{\#} = \{\pm 1\}$. q.e.d.

Esiste però una vasta classe di anelli in cui il concetto di primo e atomo coincidono. Questo è vero in particolare pegli interi.

Definizione 1.16. *Dato un anello commutativo con identità* A*, diciamo che* I *è un* **ideale** *di* A *e scriveremo* $I \trianglelefteq A$ *se* I *è un sottoanello di* A *e, per ogni* $a \in A$*,* $aI = Ia \subseteq I$*.*

Definizione 1.17. *Un dominio D dicesi a* **ideali principali** *o in breve* **PID** *se ogni ideale I è della forma $(a) = aD = \{ad \mid d \in D\}$ per qualche elemento fissato a.*

Esercizio 1.18. *Dato un campo k, dimostrare che $k[x]$ è un dominio a ideali principali.*

Vogliamo mostrare che in un PID gli atomi sono primi.

Definizione 1.19. *Dati a, b in un dominio D, d viene detto un* **massimo comune divisore** *tra a e b se:*

1. *$d|a$ e $d|b$;*
2. *se $c|a$ e $c|b$ allora $c|d$.*

Proposizione 1.20. *Sia D un PID, allora esiste un massimo comune divisore d per ogni coppia di elementi a, b. Inoltre d' soddisfa la stessa proprietà sse $d \approx d'$. Infine esistono $x, y \in D$ tali che $ax + by = d$ (***Identità di Bézout***).*

Dim. Si indichi con (a, b) l'insieme degli elementi della forma $\{ax + by \mid x, y \in D\}$. Allora è facile mostrare che (a, b) è un ideale. Quindi esiste un elemento $d \in D$ tale che $(a, b) = dD$. In particolare $a \in dD$, quindi $d|a$ e, analogamente, $d|b$. D'altro canto se c divide a e b, allora tutti gli elementi di $dD = (a, b)$ sono dei multipli di c, ma d è uno di questi. Per cui d è un massimo comune divisore tra a e b ed ha la forma prescritta. Sia d' un altro massimo comune divisore, allora $d|d'$ e $d'|d$, cioè $d = d'u$ ed$' = dv$, quindi $d(1 - uv) = 0$. Se $d = 0$, allora $d' = 0$; altrimenti $1 = uv$ e $d \approx d'$. q.e.d.

Con una lieve ambiguità indicheremo con $\gcd(a, b)$ uno tra gli elementi associati che fungono da massimo comune divisore tra a e b.

Teorema 1.21. *Sia a un atomo in un PID. Allora a è primo.*

Dim. Supponiamo che $a|bc$, ma $a \nmid c$. Sia $(d) = (a, c)$, allora $d|a$ e $d|c$. Ma essendo a un atomo ne segue che $d \approx a$ o $d \approx 1$. Siccome $a \nmid c$ deve valere il secondo caso, quindi $1 \in (d) = (a, c)$, cioè esistono $x, y \in D$ tali che $ax+cy = 1$, da cui $a(bx + ty) = b$, ove $at = bc$, ossia $a|b$. q.e.d.

Una classe che estende i PID e che risulterà molto utile anche nel seguito è quella dei **domini a fattorizzazione unica** o UFD. Tra le molte possibili definizioni forniamo la seguente:

Definizione 1.22. *Un dominio D viene detto a fattorizzazione unica se ogni elemento si decompone in modo unico a meno dell'ordine dei fattori o di unità nel prodotto di un numero finito di atomi.*

Esercizio 1.23. *Perché bisogna specificare a meno dell'ordine o di unità nella definizione di dominio a fattorizzazione unica?*

Mostriamo che i PID sono una sottoclasse dei UFD.

Teorema 1.24. *Sia D un PID, allora ogni elemento di D^* si scrive in modo essenzialmente unico come prodotto di un numero finito di atomi.*

Dim. Se $d \in D^\#$ allora l'asserto è banale. In caso contrario mostriamo che ogni elemento d ammette un atomo come divisore. Se d è un atomo non c'è niente da dimostrare. Altrimenti esiste $d_1 \not\approx 1, d$ tale che $d = d_1 f_1$. Allora $(d) < (d_1) < D$, tutte le inclusioni proprie (perché?). Se d_1 è divisibile da un atomo abbiamo concluso altrimenti, sostituendo d con d_1, otterremmo una successione infinita di elementi d_i tali che $(d_i) < (d_{i+1}) < D$. Ora $I = \bigcup_i (d_i)$ è un ideale. Infatti se $x, y \in I$ allora $x, y \in (d_i)$ per $i >> 0$ (i abbastanza grande), quindi $x + y$ e $rx \in (d_i) \leq I$ per ogni $r \in D$. Quindi $I = (b)$, per qualche b. Sia i tale che $b \in (d_i)$, allora $(b) \leq (d_i) \leq I = (b)$ e $(b) = (d_{i+n})$ per ogni intero n. Questo contraddice l'ipotesi che (d_i) è propriamente contenuto in (d_{i+1}). Quindi uno dei d_i deve essere un atomo. Allora scegliamo al primo passo d_1 un atomo che divide d e procediamo analogamente con f_1, ossia $f_1 = d_2 f_2$ per un atomo d_2. Allora costruisco una successione d_i come sopra e questo processo deve interrompersi, cioè f_n è un atomo per qualche intero n. Sia ora $a_1 \cdots a_n = b_1 \cdots b_m$, ove a_i, b_j sono atomi. Siccome sono anche primi allora, a meno dell'ordine, $a_1 | b_1$, ossia $a_1 \approx b_1$. Cancellandoli ottengo un'identità tra due prodotti atomici con meno fattori. Per induzione sul numero dei fattori ne segue che, sempre a meno dell'ordine, $n = m$ e $a_i \approx b_i$. q.e.d.

Se D è un UFD allora si può definire il massimo comune divisore d tra due elementi a, b nel seguente modo: si scelga anzitutto un rappresentante p da ogni classe di equivalenza rispetto a $\approx$ in $\mathcal{A}(D)$, allora $a = u \prod p^{v_p(a)}$, ove $u \in D^{\#}$. Basta porre $d = \prod p^{\min(v_a(p), v_b(p))}$ per ottenere un massimo comune divisore tra a e b.

Esercizio 1.25. *Mostrare che d definito sopra è un massimo comune divisore.*

Il nostro intento è provare un teorema di trasporto dovuto a Gauss che afferma che se D è UFD allora $D[x]$ è UFD. Cominciamo da alcune definizioni.

Definizione 1.26. *Sia D un UFD e sia $f = \sum_{i=0}^{n} f_i x^i \in$*

$D[x]$, allora il **contenuto** *di f, $\mathrm{ct}(f)$, viene definito come* $\gcd(f_1, \ldots, f_n)$.

Definizione 1.27. *Diremo che un polinomio f a coefficienti in un UFD è primitivo se* $\mathrm{ct}(f) = 1$.

Lemma 1.28 (Gauss). *Sia D un UFD e siano $f, g \in D[x]$ primitivi, allora fg è primitivo.*

Dim. Per assurdo sia p un divisore primo di $\mathrm{ct}(fg)$. Siccome f è primitivo esiste $m = \min\{f_i \mid f_i \not\equiv_p 0\}$. Sia n l'analogo per g. Ora il coefficiente di x^{n+m} in fg vale $\sum_{i=0} f_{n+m-i} g_i = \sum_{i<n} f_{n+m-i} g_i + f_m g_n + \sum_{j<m} f_j g_{n+m-j}$ che è congruo a $f_m g_n$ modulo p e quindi non è divisibile per p, contro l'ipotesi che $p | \mathrm{ct}(fg)$. q.e.d.

Esercizio 1.29. *Si mostri che il Lemma di Gauss equivale alla seguente legge* $\mathrm{ct}(f)\mathrm{ct}(g) = \mathrm{ct}(fg)$.

Mostriamo come questo risultato serva a stabilire l'irriducibilità di polinomi. Ricordiamo che in modo analogo a come $\mathbb{Q}$ viene costruito da $\mathbb{Z}$, si può ottenere a partire da ogni dominio D un campo $\mathcal{Q}(D)$ detto campo dei quozienti di D, in cui D si immerge. L'esempio che utilizzeremo sarà $D = k[x]$, k un campo; in tal caso $\mathcal{Q}(D)$ consiste nel campo delle funzioni razionali, ossia elementi della forma $f(x)/g(x)$.

Definizione 1.30. *Dato un UFD D, ogni polinomio f su D si fattorizza come $\mathrm{ct}(f)g$, per qualche polinomio primitivo g che viene detto la* **parte primitiva** *di f e indicato con* $\mathrm{pp}(f)$.

Proposizione 1.31. *Sia $f \in D[x]$, D un UFD, $Q = \mathcal{Q}(D)$ il relativo campo dei quozienti. Allora $\mathcal{A}(D[x]) \subseteq \mathcal{A}(Q[x])$.*

Dim. È banale mostrare che $D[x]$ è un dominio. Per cui il grado di un prodotto coincide colla somma dei gradi dei fattori. Da ciò segue che $\mathcal{A}(D) \subseteq \mathcal{A}(D[x])$ e che $D[x]^{\#} = D^{\#}$. Se f è un atomo allora $\mathrm{pp}(f)$ o $\mathrm{ct}(f)$ sono unità in D. Nel primo caso $f \in D$ quindi è un elemento di Q. Altrimenti f è primitivo. Siccome $Q^* = Q^{\#}$, ne segue che $g \in \mathcal{A}(Q[x])$ sse g non si fattorizza nel prodotto di due polinomi di grado strettamente inferiore. Per assurdo f non sia un atomo in $Q[x]$, allora esistono polinomi (su Q) tali che $f = ab$ e $\deg a, \deg b < \deg f$. Allora $f = \frac{a'b'}{cd}$ ove $a', b' \in D[x]$ e $c, d \in D$ sono massimi comuni divisori dei denominatori dei coefficienti di a e b. Per cui $cdf = \mathrm{ct}(a')\mathrm{ct}(b')\mathrm{pp}(a')\mathrm{pp}(b')$ e, confrontando i contenuti, $cd = \mathrm{ct}(a')\mathrm{ct}(b')$; per cui, a meno di unità $f = \mathrm{pp}(a')\mathrm{pp}(b')$, una contraddizione . q.e.d.

Esercizio 1.32. *Si dimostri che $D[x]$ è un dominio e se ne deduca che $\mathcal{A}(D) \subseteq \mathcal{A}(D[x])$ e che $D[x]^{\#} = D^{\#}$.*

Si osservi che se a è un atomo di D e f un atomo in $D[x] \setminus D$, allora af è riducibile in $D[x]$, ma irriducibile in $Q[x]$. Proviamo ora un fondamentale teorema dovuto a Gauss.

Teorema 1.33. *Sia D un UFD, allora $D[x]$ è un UFD.*

Dim. Sia $f \in D[x]$. Poiché $\mathrm{pp}(f)$ non è divisibile da atomi non invertibili di D i suoi fattori atomici hanno grado positivo, quindi sono in numero finito. D'altro canto $\mathrm{ct}(f)$ è prodotto di un numero finito di atomi essendo in D. Mostriamo ora l'unicità. Sia $f = \prod_i^n a_i = \prod_j^m b_j$, con a_i, b_j atomi. Per cui i fattori sono atomi in D o polinomi primitivi per le stesse argomentazioni della precedente proposizione. Quindi il prodotto degli atomi in D nelle due fattorizzazioni coincide con $\mathrm{ct}(f)$ e siccome quest'ultimo appartiene a D, abbiamo unicità di fattorizzazione. Quindi possiamo supporre che gli a_i, b_j siano primitivi di grado positivo. Poiché $Q[x]$ è un PID, quindi un UFD, ne segue che $n = m$ e, a meno dell'ordine, $a_i \approx b_i$ in $Q[x]$. Poiché $Q[x]^{\#} = Q^*$ ne segue che $aa_i = bb_i$ per opportuni elementi a, b in D. Confrontando i contenuti si ha $a \approx b$ in D e $a_i \approx b_i$ in $D[x]$. q.e.d.

1.2 Campi ed Estensioni

Definizione 1.34. *Siano F e K due campi. Diremo che K è* **un'estensione** *di F, se $K \supseteq F$ e scriveremo $K \geq F$ o K/F.*

Proposizione 1.35. *Sia K un'estensione di F, allora K ammette la struttura di F-spazio vettoriale.*

Dim. Chiaramente $(K, +)$ è un gruppo abeliano e la mappa $(f, k) \mapsto fk$ definisce un prodotto scalare-vettore da $F \times K$ in K . q.e.d.

Esercizio 1.36. *Completare i dettagli della dimostrazione.*

Definizione 1.37. *La dimensione di K su F viene detta il* **grado** *dell'estensione K/F e sarà indicata con $[K : F]$. Se $[K : F] < \infty$ diremo che l'estensione è* **finita***; altrimenti K/F è un'estensione* **infinita***.*

Esempio 1.38. *Supponiamo noti i campi dei numeri razionali, reali e complessi che indicheremo con $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Il campo delle classi di resto modulo un primo p, $\mathbb{Z}/p\mathbb{Z}$, verrà denotato con $\mathbb{F}_p$.*

Definizione 1.39. *Un* **campo algebrico numerico** *è un'estensione finita di* $\mathbb{Q}$*.*

Esempio 1.40. *Sia* k *un campo e* x *un'indeterminata. Il* **campo delle funzioni razionali** $k(x)$ *è il campo dei quozienti dell'anello dei polinomi* $k[x]$*, ossia è costituito da tutti i quozienti della forma* $f(x)/g(x)$*,* f, g *polinomi,* $g(x) \neq 0$*, il polinomio nullo. Analogamente date* n *indeterminate* $x_1, \ldots, x_n$*, indicheremo con* $k(x_1, \ldots, x_n)$ *il campo delle funzioni razionali in tali indeterminate.*

Esempio 1.41. *Sia k un campo e* $k((x))$ *l'insieme delle* **serie di Laurent** *nell'indeterminata* x*, ossia le serie formali della forma*

$$f(x) = \sum_{i=n}^{\infty} a_i x^i,$$

per qualche $n \in \mathbb{Z}$ *dipendente da* f *e* $a_i \in k$*. Si definisca su tale insieme una* **somma puntuale**

$$\sum_{i=n}^{\infty} a_i x^i + \sum_{i=n}^{\infty} b_i x^i = \sum_{i=n}^{\infty} (a_i + b_i) x^i$$

e un **prodotto di convoluzione**

$$\sum_{i=n}^{\infty} a_i x^i * \sum_{j=m}^{\infty} b_j x^j = \sum_{k=n+m}^{\infty} (\sum_{i+j=k} a_i b_j) x^k.$$

Teorema 1.42. *Dato un campo* k*, l'insieme delle serie di Laurent* $(k((x)), +, *)$ *risulta essere un campo.*

Dim. Sia $K = k((x))$, allora si verifica facilmente che $(K, +, *)$ è un anello commutativo con identità. Resta da mostrare che ogni elemento non nullo è invertibile. Sia $f = \sum_{i=n} a_i x^i \neq 0$ ove $a_n \neq 0$. Moltiplicando per $a_n^{-1} x^{-n}$, ci riconduciamo al caso in cui $n = 0$ e $a_0 = 1$. Si tratta di determinare coefficienti b_j tali che $g = \sum_{j=0} b_j x^j$ soddisfa $g * f = 1$. Chiaramente deve essere $b_0 = 1$. Supponiamo che tutti i termini $b_0, \ldots, b_{m-1}$ siamo stati determinati, allora risolvendo l'equazione

$$0 = (f * g)_m = \sum_{k=0}^{m} a_i b_{m-i}$$

otteniamo anche b_m . q.e.d.

Esercizio 1.43. *Sia D un dominio e sia $A = D((x))$ l'insieme delle serie di Laurent su D. Dimostrare che A è un dominio. È un campo?*

Esibiamo ora alcuni esempi di estensioni.

Esempio 1.44. *L'estensione $\mathbb{C}/\mathbb{R}$ risulta finita siccome $[\mathbb{C} : \mathbb{R}] = 2$. Infatti $\{1, i\}$ è una $\mathbb{R}$-base per $\mathbb{C}$.*

Ricordiamo che $|\mathbb{R}| = 2^{\aleph}_0 > \aleph_0 = |\mathbb{Q}|$ e che, per ogni intero n, $|\mathbb{Q}^n| = |\mathbb{Q}|$ (entrambe i risultati sono dovuti a G. Cantor, il padre dell'Aritmetica Cardinale).

Nota 1.45. *Il campo dei reali è un'estensione infinita di $\mathbb{Q}$. Altrimenti $\mathbb{R}$ sarebbe in corrispondenza biunivoca con $\mathbb{Q}^n$ per qualche intero n (che va pensato come la dimensione di $\mathbb{R}$ sui razionali), contraddicendo i due risultati di Cantor summenzionati.*

Un ulteriore e più naturale esempio di estensione infinita è dato da

Esempio 1.46. *Sia k un campo e $K = k(t)$ il campo delle funzioni razionali su k nell'indeterminata t. Allora $[K :$*

$k] = \infty$. Altrimenti si dica n la dimensione di K su k, allora $1, t, \ldots, t^n$ dovrebbero essere linearmente dipendenti su k, cioè esistono coefficienti $a_0, \ldots, a_n$ in k tali che $\sum_{j=0}^{n} a_j t^j = 0$, contro l'ipotesi fatta su t.

Richiamiamo alcune definizioni che serviranno per il prossimo esempio.

Definizione 1.47. *Sia A un anello commutativo. Ricordiamo che un ideale I di A dicesi* **primo** *se $ab \in I$ implica che almeno uno dei fattori appartiene a I. Un ideale M viene detto* **massimale** *se $M \leq I \leq A$ implica $I = M$ o $I = A$.*

Caratterizziamo queste due proprietà mediante l'anello quoziente A/I.

Proposizione 1.48. *Dato un anello commutativo A e un suo ideale I allora*

1. *A/I è un dominio sse I è primo;*
2. *A/I è un campo sse I è massimale.*

Dim. Si ponga $\bar{A} = A/I$ e $\bar{a} = a + I$. Allora $ab \in I$ sse $\overline{ab} = \bar{0}$. Per cui I è primo sse $\bar{A}$ è un dominio. Sia ora $\bar{A}$ un campo, allora gli unici ideali di $\bar{A}$ sono 0 o tutto $\bar{A}$. Per il teorema di corrispondenza sugli ideali negli anelli quoziente ne segue che I è massimale. Viceversa sia I massimale, allora $\bar{A}$ non possiede ideali non banali. Sia $0 \neq x \in \bar{A}$, allora $x\bar{A} = \bar{A}$ ed esiste $y \in \bar{A}$ tale che $xy = 1$ e $\bar{A}$ è un campo . q.e.d.

Esercizio 1.49. *Dimostrare che un ideale massimale è primo. Mostrare che in un PID vale il viceversa.*

Esempio 1.50. *Sia $A = \mathbb{Q}[t]$ e $p(t) = t^3 - 2 \in A$. Allora p è irriducibile in quanto non ammette radici razionali. Sia $I = pA$, allora I è un ideale primo e siccome A è un dominio a ideali principali I è addirittura massimale. Quindi $K = A/I$ è un campo. Inoltre la mappa $j : a \mapsto a + I$, ove $a \in \mathbb{Q}$ risulta essere iniettiva. Identificando $\mathbb{Q}$ colla sua immagine mediante j, possiamo dire che K è un'estensione di $\mathbb{Q}$. Sia $f \in A$. Per l'algoritmo euclideo esistono due polinomi q ed r tali che $f = qp + r$ ove $\deg r < \deg p = 3$. Allora $f + I = r + I$ e K è generato come $\mathbb{Q}$-spazio dalle classi laterali individuate da 1, t e t^2 e non è difficile provare che sono linearmente indipendenti. Quindi $[K : \mathbb{Q}] = 3$. Mostriamo direttamente che K è un campo. L'unica difficoltà consiste nel provare che ogni elemento non nullo di K ammette inverso. Sia $f \in A \setminus I$. Allora $\gcd(f, p) = 1$, cioè esistono $a, b \in A$ tali che $af + pb = 1$, ossia l'inverso di $f + I$ è $a + I$.*

Vedremo come generalizzare questo esempio per costruire esempi di campi algebrici numerici di grado arbitrario.

Definizione 1.51. *Sia K un'estensione di F. Se X è un sottoinsieme di K, allora l'anello $F[X]$ è l'intersezione di tutti i sottoanelli di K contenenti F e X. Analogamente viene definito il campo $F(X)$. Se X è finito diremo che $F(X)$ è un'estensione* **finitamente generata**.

Per definizione $F[X]$ e $F(X)$ sono il minimo sottoanello e il minimo sottocampo di K contenente F e X. Fissato un elemento $a \in K$ sia ev_a la mappa di valutazione definita da $F[x]$ in K mediante

$$\mathrm{ev}_a(f) := f(a).$$

Esercizio 1.52. *Dimostrare che* ev_a *realizza un omomorfismo di anelli nonché di* F*-spazi vettoriali tra* $F[x]$ *e* K.

Proposizione 1.53. *Sia* K *un'estensione di* F *e* $a \in K$. *Allora*

$$F[a] = \{f(a) \mid f(x) \in F[x]\}$$

e

$$F(a) = \{f(a)/g(a) \mid f(x), g(x) \in F[x],\ g(a) \neq 0\}.$$

Inoltre $F(a)$ *è il campo dei quozienti di* $F[a]$.

Dim. La mappa di valutazione ev_a ha come immagine $\{f(a) \mid f(x) \in F[x]\}$ che risulta così essere un sottoanello di K contenente F ed a. Se R indica un qualsiasi sottoanello di K soddisfacente tali condizioni allora ogni elemento della forma $f(a)$ appartiene a R. Questo dimostra la prima parte dell'asserto. Ora $\{f(a)/g(a) \mid f(x), g(x) \in F[x],\ g(a) \neq 0\}$ è il campo dei quozienti di $F[a]$ e risulta certamente minimale rispetto alla proprietà di contenere $F[a]$ tra i sottocampi di K . q.e.d.

In modo analogo si possono dimostrare simili risultati nel caso di un arbitrario sottoinsieme finito X di K. Si indichi con $\underline{a}$ la n-upla $(a_1, \ldots, a_n)$, ove $a_i \in K$.

Proposizione 1.54. *Sia* $X = \{a_1, \ldots, a_n\}$, *allora*

$$F[X] = \{f(\underline{a}) \mid f(\underline{x}) \in F[\underline{x}]\}$$

e

$$F(X) = \{f(\underline{a})/g(\underline{a}) \mid f(\underline{x}), g(\underline{x}) \in F[\underline{x}],\ g(\underline{a}) \neq 0\}.$$

Nel caso X sia infinito ci si può sempre ricondurre al caso finitamente generato.

Proposizione 1.55. *Sia K un'estensione di F e $X \subseteq K$. Se $\alpha \in F(X)$, allora $\alpha \in F(a_1, \ldots, a_n)$ per alcuni $a_1, \ldots, a_n \in K$. Per cui $F(X) = \bigcup\{F(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\}$, ove l'unione varia su tutti i sottoinsiemi finiti di X.*

Dim. Ovviamente ogni campo $F(a_1, \ldots, a_n)$ è contenuto in $F(X)$; quindi $L = \bigcup\{F(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\} \leq F(X)$. Per l'inclusione opposta basta mostrare che L è un campo. Siano α e β elementi di L, allora $\alpha \in F(a_1, \ldots, a_n)$ e $\beta \in F(b_1, \ldots, b_m)$ per opportuni elementi a_i e b_j in K. Allora $\alpha \pm \beta$ e α/β appartengono a $F(a_1, \ldots, a_n, b_1, \ldots, b_m)$ e quindi ad L . q.e.d.

Definizione 1.56. *Se K è un'estensione di F, allora un elemento $\alpha \in K$ dicesi* **algebrico** *su F se esiste un polinomio non nullo $f(x) \in F[x]$ tale che $f(\alpha) = 0$. Se α non è algebrico su F, allora viene detto* **trascendente** *su F. Se ogni elemento di K risulta algebrico su F, allora diremo che K/F è un'***estensione algebrica**.

Sia K un'estensione di F e sia $\alpha \in K$ algebrico su F. Si consideri

$$I = \{f \in F[x] \mid f(\alpha) = 0\},$$

allora è immediato mostrare che I è un ideale di $F[x]$. Siccome $F[x]$ è un PID, ne segue che $I = pF[x]$, per qualche polinomio $p(x)$; inoltre tale polinomio deve essere irriducibile. Ha quindi senso la seguente definizione:

Definizione 1.57. *Se α è algebrico su F, il polinomio minimo di α su F è il polinomio monico $p \in F[x]$ di grado minimo tale che $p(\alpha) = 0$; verrà denotato con $\min_F(\alpha)$. Equivalentemente $\min_F(\alpha)$ è il generatore monico della mappa ev_α.*

Esercizio 1.58. *Determinare* $\min_F(a)$ *ove* $a \in F$.

Esempio 1.59. *Il numero complesso* $i = \sqrt{-1}$ *è algebrico su* $\mathbb{Q}$ *in quanto radice del polinomio* $x^2 + 1$. *Si noti che* $\min_{\mathbb{Q}}(i) = \min_{\mathbb{R}}(i) = x^2 + 1$, *mentre* $\min_{\mathbb{C}}(i) = x - i$*; quindi il polinomio minimo dipende dal campo base. Sia* $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$, *allora* $\omega^n - 1 = 0$. *Determineremo in seguito* $\min_{\mathbb{Q}}(\omega)$.

Esempio 1.60. *Il primo esempio di numero trascendente sui razionali venne costruito da Liouville nel 1851, trattasi di* $\sum_n 10^{-n!}$. *Nel 1873 Hermite dimostrò che* e*, la base dei logaritmi neperiani, è trascendente. Analogo risultato venne provato da Lindemann nel 1882 per* π*, chiudendo così un classico problema che datava più di 2000 anni. D'altro canto* π *è banalmente algebrico su* $\mathbb{Q}(\pi)$*, quindi l'essere algebrico o trascendente dipende dal campo base.*

Esercizio 1.61. *Sia* $a = \sqrt{2}$ *e* $b = \sqrt{3}$*, determinare i polinomi minimi su* $\mathbb{Q}$ *di* $a, b, a + b$ *e* ab.

Proposizione 1.62. *Sia* K *un'estensione di* F *e sia* $K \ni \alpha$ *algebrico su* F.

1. *il polinomio* $\min_F(\alpha)$ *è irriducibile su* F*;*
2. *se* $g(x) \in F[x]$*, allora* $g(\alpha) = 0$ *sse* $\min_F(\alpha)$ *divide* g*;*
3. *se* $n = \deg \min_F(\alpha)$*, allora gli elementi* $1, \alpha, \dots, \alpha^{n-1}$ *costituiscono una base per* $F(\alpha)$ *su* F*, sicché* $[F(\alpha) : F] < \infty$. *Inoltre* $F[\alpha] = F(\alpha)$.

Dim. Sia $p(x) = \min_F(\alpha)$. Se p non fosse irriducibile, allora α sarebbe radice di uno dei suoi fattori, contro la minimalità del grado di p. Abbiamo già osservato che $\ker(\mathrm{ev}_\alpha)$ è un ideale principale di $F[x]$. Ancora per minimalità si ha che p ne è generatore. Infine $F[x]/\ker(\mathrm{ev}_\alpha) \simeq F[\alpha]$ è un dominio di integrità essendo un sottoanello del campo K. Quindi per la Proposizione 1.48 $pF[x]$ è un ideale primo. Siccome $F[x]$ è un PID, ogni ideale primo è massimale e $F[\alpha]$ è un campo, quindi coincide con $F(\alpha)$. Infine dato $g(x) \in F[x]$, mediante l'algoritmo euclideo è possibile determinare q, r tali che $g = pq + r$ e $\deg r < \deg p$, per cui $g(\alpha) = r(\alpha)$ e $1, \alpha, \ldots, \alpha^{n-1}$ generano $F[\alpha]$ come F-spazio. D'altra parte se fossero linearmente dipendenti avremmo un polinomio non nullo di grado inferiore a n di cui α è radice . q.e.d.

Nota 1.63. *Si noti che la condizione $F(\alpha) = F[\alpha]$ vale sse α è algebrico su F. La sufficienza è appena stata provata. Sia $F(\alpha) = F[\alpha]$, allora $1/\alpha \in F(\alpha)$ si può esprimere come un polinomio f valutato in α, da cui risulta che α annulla il polinomio $xf(x) - 1$ ed è quindi algebrico su F.*

Richiamiamo un risultato dovuto al matematico tedesco Eisenstein.

Teorema 1.64. *Sia D un UFD, p un elemento primo di D e $f(x) = \sum_{i=0}^{n} f_i x^i$ un polinomio a coefficienti in D tali che $f_i \equiv_p 0$, per $i \leq n-1$, ma $p^2 \not| f_0$ e $f_n \not\equiv_p 0$, allora $f(x)$ è un elemento irriducibile di $\mathcal{Q}(D[x])$.*

Dim. Per assurdo sia $f = gh$, dove per il Lemma di Gauss si può assumere che i coefficienti di g e h siano in D. Si indichi con $\bar{l}$ la riduzione modulo p del polinomio l, allora $\bar{f} = \bar{g}\bar{h}$, ma $\bar{f} = \bar{f}_n \bar{x}^n$. Quindi $\bar{g} = \bar{g}_m \bar{x}^m$ e $\bar{h} = \bar{h}_d \bar{x}^d$ con $m, d > 0$. Per cui $g = g'_m x^m + pg'(x)$ e $h = h'_d x^d + ph'(x)$, per opportuni polinomi g', h' in $D[x]$ e g'_m, h'_d in D.

Moltiplicando tali espressioni si ottiene che $f = f_n x^n + pxf'(x) + p^2 f'_0$, contro le ipotesi . q.e.d.

Esempio 1.65. *Sia $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, allora per il criterio di Eisenstein con $p = 2$, f è irriducibile e risulta essere il polinomio minimo per $\sqrt[3]{2}$ su $\mathbb{Q}$. In particolare $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Se p è un primo allora $x^n - p$ è irriducibile sempre come conseguenza del criterio di Eisenstein e $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Sia ω una radice cubica dell'unità sui complessi diversa da 1, allora $\omega^3 - 1 = 0$. Ora $x^3 - 1 = (x-1)(x^2 + x + 1)$, quindi ω annulla il secondo fattore. Siccome questi non ammette radici razionali è il polinomio minimo di ω.*

Esercizio 1.66. *Stabilire per quali interi n, $x^2 - n$ è irriducibile su $\mathbb{Q}$.*

Dim. È ovvio che se $n = a^2$, $a \in \mathbb{Z}$, allora il polinomio è irriducibile. Altrimenti sia $n = a^2 b$, ove b non è divisibile per quadrati (tali interi vengono detti **square-free**). Si ponga $y = x/a$, allora $x^2 - n$ è irriducibile sse $y^2 - b$ lo è (perché?). A questo punto se esiste un primo che divide b, l'ultimo polinomio è irriducibile per il criterio di Eisenstein, altrimenti è riducibile (b deve essere ± 1) . q.e.d.

Nota 1.67. *Una completa caratterizzazione dei monomi irriducibili della forma $x^n - a$, con a, n interi è dovuta al matematico siciliano Capelli e verrà trattata in seguito come applicazione della Teoria di Galois.*

Il prossimo esercizio mostra che non sempre il criterio di Eisenstein si può applicare.

Esercizio 1.68. *(Difficile) Determinare per quali valori di n $f(x) = x^n - p^2$ è irriducibile su $\mathbb{Q}$ con p primo.*

Dim. Chiaramente n deve essere dispari. Sia questo il caso e si supponga che $f = gh$. Per il Lemma di Gauss possiamo assumere che i polinomi g, h siano a coefficienti interi. Si deduce facilmente che devono essere monici. Si indichi con $\bar{l}$ la riduzione di un polinomio intero modulo p, allora $\bar{x}^n = \bar{f} = \bar{g}\bar{h}$. Per cui $\bar{g} = \bar{x}^{2l}$ e $\bar{h} = \bar{x}^{2k-1}$, per opportuni interi positivi l e k. Sicché $g = x^{2l} + pg'$ e $h = x^{2k+1} + ph'$. Da $f = gh$ segue che $x^{2l}g' = -x^{2k-1}h'$. Siccome x è un atomo e $\mathbb{Z}[x]$ un UFD, allora $x|g'$. Da cui segue che $x|1$, che è manifestamente impossibile . q.e.d.

Esempio 1.69. *Sia p un primo e $\omega = e^{\frac{2\pi i}{p}} = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p})$ annulla il polinomio $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$ e quindi annulla il secondo fattore. Poniamo $\Phi(x) = \sum_{i=0}^{p-1} x^i$, allora $\Phi(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$. Siccome i coefficienti binomiali soddisfano le ipotesi del criterio di Eisenstein rispetto al primo p, ne segue che $\Phi(x+1)$ e quindi $\Phi(x)$ sono irriducibili su $\mathbb{Q}$. Per cui $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$.*

Vedremo in seguito come questo risultato si generalizza nel caso di radici di 1 di indice composto n e quali conseguenze comporta nella risoluzione del classico problema della costruzione del n-gono regolare con riga e compasso. Il prossimo esempio fornisce alcune informazioni sui sottocampi del campo delle funzioni razionali.

Definizione 1.70. *Siano f, g elementi di un dominio a fattorizzazione unica. Diremo che f e g sono* **coprimi** *se* $\gcd(f, g)$ *vale* 1 *e scriveremo $f \perp g$.*

Esempio 1.71. *Sia k un campo e $K = k(t)$ il campo delle funzioni razionali su k nell'indeterminata t. Sia $u \in K$, $u \notin k$, quindi $u = f(t)/g(t)$, ove $f, g \in k[t]$ e $f \perp g$. Si ponga $F = k(u)$. Vogliamo dimostrare che*

$$[K : F] = \max(\deg f, \deg g).$$

In particolare K/F è un'estensione finita.

Dim. Si noti anzitutto che $K = F(t)$. Si tratta allora di determinare il polinomio minimo di t su F. Si consideri $p(x) = ug(x) - f(x) \in F[x]$. Allora t è una radice di p e $[K : F] < \infty$. Siano $f(x) = \sum_{i=0}^{n} f_i x^i$ e $g(x) = \sum_{i=0}^{m} g_j x^j$, con $a_n b_m \neq 0$, allora $\deg p = \max(\deg f, \deg g)$. Se così non fosse si dovrebbe avere $n = m$ e dovrebbe annullarsi il coefficiente di x^n in p. Ma questi eguaglia $uf_n - g_n$ e se fosse nullo avremmo $u \in k$. Poiché $\infty = [K : k] = [K : F][F : k]$, u è trascendente su k. Per cui $k[x] \simeq k[u]$. Se p fosse riducibile su $k(u)$ allora lo sarebbe su $k[u]$ per la Proposizione 1.31 applicata al dominio $D = k[u]$. Sia $p(x, u) = h(x, u)l(x, u)$ in $k[x, u]$. Siccome $\deg_u p = 1$ si ha $\deg_u h = 1$ e $\deg_u l = 0$, ossia $l = l(x) \in k[x]$. Quindi $l(x)|\mathrm{ct}_x(p) = \gcd(f(x), g(x)) = 1$ da cui segue $l \in k$ e p è irriducibile su $k(u) = F$ e $p = \min_F(t)$. q.e.d.

Fatto molto più importante è che tutti i sottocampi intermedi tra $k(t)$ e k sono della forma $k(u)$, per qualche $u \in k(t)$. In particolare $[k(t) : L] < \infty$ per ognuno di tali sottocampi L. Questo risultato è noto come Teorema di Lüroth.

Definizione 1.72. *Sia $K = F(a)$, per qualche $a \in K$, allora K dicesi* **un'estensione semplice** *di F.*

Esercizio 1.73. *Posti* $a = \sqrt{(}2)$ *e* $b = sqrt(3)$*, si dimostri che* $\mathbb{Q}(a,b)/\mathbb{Q}$ *è semplice (coincide con* $\mathbb{Q}(a+b)$*).*

Dim. Un semplice calcolo mostra che $(a+b)^3 = 11a+9b$. Siccome la matrice $\begin{pmatrix} 11 & 9 \\ 1 & 1 \end{pmatrix}$ è invertibile, ne segue che a, b si esprimono come combinazioni lineari a coefficienti razionali in $(a+b)$ e $(a+3)^3$. Quindi $a, b \in \mathbb{Q}(a+b)$. Ma chiaramente $\mathbb{Q}(a+b) \leq \mathbb{Q}(a,b)$ e quindi coincidono.

Esempio 1.74. *Sia* K *un'estensione finitamente generata di* F*, ossia* $K = F(a_1, \ldots, a_n)$ *e siano* L_i *i campi intermedi definiti ricorsivamente come segue:* $L_0 = F$ *e* $L_{i+1} = L_i(a_{i+1})$*. Allora* K *coincide con* L_n *e può quindi essere ottenuto mediante un numero finito di estensioni semplici.*

Nota 1.75. *La precedente definizione e il precedente esercizio mostrano che talvolta estensioni finitamente generate sono semplici. Dimostreremo che questo è sempre vero se consideriamo estensioni finitamente generate dei razionali mediante elementi algebrici.*

Conviene notare che finora abbiamo usato il termine finitamente generato in tre accezioni distinte. Dati due campi K ed F tali che $K \geq F$, K può essere finitamente generato come F-spazio vettoriale, come F-anello o come F-campo. Nel primo caso semplicemente diciamo che $[K : F] < \infty$, nel secondo $K = F[a_1, \ldots, a_n]$ e nel terzo $K = F(a_1, \ldots, a_n)$. È altresì ovvio che ogni accezione implica la successiva. Al fine di esplorare meglio questi concetti dimostriamo una serie di risultati.

Lemma 1.76. *Se* K *è un'estensione finita di* F *allora* K *è algebrico e finitamente generato su* F *(come campo).*

Dim. Sia $\alpha_1, \dots, \alpha_n$ una base per K su F, allora ogni elemento di K è della forma $\sum a_i \alpha_i$ e $K = F(\alpha_1, \dots, \alpha_n)$ è finitamente generato su F. Sia $a \in K$, allora $1, a, \dots, a^n$ sono linearmente dipendenti su F, il che equivale ad asserire che a è algebrico su F . q.e.d.

Vale anche il viceversa ma la dimostrazione richiede alcune proprietà del grado.

Proposizione 1.77. *Siano $F \leq L \leq K$ campi, allora*

$$[K : F] = [K : L][L : F].$$

Dim. Sia $\{a_i \,|\, i \in I\}$ una base per L/F e $\{b_j \,|\, i \in J\}$ una per K/L. Mostriamo che $\{a_i b_j \,|\, i \in I, j \in J\}$ è una base per K/F. Se x appartiene a K, allora esistono $\alpha_j \in L$ tali che $x = \sum_j \alpha_j b_j$. Inoltre esistono $\beta_{ij} \in F$ tali che $\alpha_j = \sum_i \beta_{ij} a_i$, quindi $x = \sum_{i,j} \beta_{ij} a_i b_j$ e $a_i b_j$ generano K come spazio su F. Sia $\sum_{i,j} \beta_{ij} a_i b_j = 0$, allora $\sum_i \beta_{ij} a_i = 0$ per l'indipendenza dei b_j su L. Usando la F-indipendenza degli a_i segue che $\beta_{ij} = 0$, quindi gli $a_i b_j$ costituiscono una F-base per K e $[K : F] = |I||J| = [K : L][L : F]$. q.e.d.

Proviamo che finitamente generata e algebrica implica finita.

Proposizione 1.78. *Sia K un'estensione di F. Se $\alpha_i \in K$ è algebrico, allora $F[\alpha_1, \dots, \alpha_n]$ è un'estensione finita di F, inoltre*

$$[F[\alpha_1, \dots, \alpha_n] : F] \leq \prod_{i=1}^{n} [F[\alpha_i] : F].$$

Dim. Procediamo per induzione su n. Il caso $n = 1$ segue dalla Proposizione 1.62. Si ponga $E = F[\alpha_1, \dots, \alpha_n]$

e $L = F[\alpha_1, \dots, \alpha_{n-1}]$, allora $[L : F] \leq \prod_{i=1}^{n-1}[F[\alpha_i] : F]$. Allora $E = L[\alpha_n]$ è un campo, poiché α_n è algebrico su L e siccome $\min_L(\alpha_n) | \min_F(\alpha_n)$ ancora per 1.62, si ha $[E : L] \leq [F[\alpha_n] : F]$. Allora induzione e 1.77 implicano

$$[E : F] = [E : L][L : F] \leq \prod_{i=1}^{n}[F[\alpha_i] : F],$$

come richiesto . q.e.d.

Notiamo che la disuguaglianza può essere stretta.

Esempio 1.79. *Sia* $a = \sqrt[4]{2}$ *e* $b = \sqrt[4]{18}$, *allora* $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(b) : \mathbb{Q}] = 4$, *poiché* $x^4 - 2$ *e* $x^4 - 18$ *sono irriducibili su* $\mathbb{Q}$ *per il criterio di Eisenstein. Tuttavia* $\mathbb{Q}(a, b) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$ *che ha grado* 8 *su* $\mathbb{Q}$*. Infatti* $(b/a)^4 = 3$, *quindi* $\sqrt{3} \in \mathbb{Q}(a, b)$. *Ora* $[\mathbb{Q}(a, b) : \mathbb{Q}(a)] \leq 2$, *poiché* b *soddisfa il polinomio* $x^2 - 3\sqrt{(2)} = x^2 - 3a^2 \in \mathbb{Q}(a)[x]$. *Per 1.77*

$$\begin{aligned} [\mathbb{Q}(a, b) : \mathbb{Q}] &= [\mathbb{Q}(a, b) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] \leq \\ 8 &= [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}]. \end{aligned}$$

Siccome $\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) \leq \mathbb{Q}(a, b)$, *otteniamo l'eguaglianza.*

Esercizio 1.80. *Dimostrare che* $8 = [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}]$.

Dim. Si ponga $a = \sqrt[4]{2}$ e $b = \sqrt{3}$. Siccome $[\mathbb{Q}(a) : \mathbb{Q}] = 4$, basta provare che $\deg \min_{\mathbb{Q}(a)}(b) = 2$, ossia che $b \notin \mathbb{Q}(a)$. Altrimenti $b = w + xa + ya^2 + za^3$ un elemento di $\mathbb{Q}(a)$ (si ricordi che $1, a, a^2, a^3$ sono una base per $\mathbb{Q}(a)$). Quadrando si avrebbe

$$\begin{cases} wz + 2yx &= 0 \\ 2wy + x^2 + 2z^2 &= 0 \\ wx + 2zy &= 0 \\ w^2 + 4zx + 2y^2 &= 3 \end{cases}.$$

$w = 0$ implicherebbe $x = z = 0$, ma $2y^2 = 3$ non ammette soluzioni in $\mathbb{Q}$. Quindi $z = -2\frac{xy}{w}$ e $\frac{x}{w}(w^2 - 2y^2) = 0$, il che impone $w = 0$. q.e.d.

Mostreremo questo fatto come applicazione della teoria di Galois.

Corollario 1.81. *Se K estende F, allora $\alpha \in K$ è algebrico su F sse $[F(\alpha) : F] < \infty$. Inoltre K è algebrico su F se $[K : F] < \infty$.*

Non vale però il viceversa, ossia esistono estensioni algebriche di grado infinito.

Proposizione 1.82. *Sia K un'estensione di F e sia X un sottoinsieme di K costituito da elementi algebrici. Allora $F(X)$ è algebrica su F. Se $|X| < \infty$, allora $[F(X) : F] < \infty$.*

Dim. Sia $a \in F(X)$. Per 1.55 esistono $\alpha_1, \dots, \alpha_n \in X$ tali che $a \in F(\alpha_1, \dots, \alpha_n)$. Per 1.78, $F(\alpha_1, \dots, \alpha_n)$ e, a fortiori, a sono algebrici su F. Per cui $F(X)$ è algebrico su F. L'ultimo fatto segue da 1.78 . q.e.d.

Possiamo alfine provare che essere algebrico è una proprietà transitiva.

Teorema 1.83. *Siano $F \leq L \leq K$ campi. Se L/F e K/L sono estensioni algebriche, allora K/F lo è.*

Dim. Sia $\alpha \in K$ e sia $f(x) = \sum_{i=0}^{n} f_i x^i$ il polinomio minimo di α su L. Siccome L/F è algebrica, allora il campo $L_0 = F(f_0, \dots, f_{n-1})$ è un'estensione finita di F per 1.81. Ora $f(x) \in L_0[x]$, per cui α è algebrico su L_0. Allora $[L_0[\alpha] : F] = [L_0[\alpha] : L_0] = [L_0 : F] < \infty$. Poiché $F(\alpha) \leq L_0(\alpha)$, si vede che $[F(\alpha) : F] < \infty$ e α è algebrico su F. Data l'arbitrarietà di a, si ha che K/F è algebrica . q.e.d.

Per cui ha senso la seguente definizione.

Definizione 1.84. *Sia K un'estensione di F. L'insieme*

$$\{a \in K \mid a \quad \text{è algebrico su} \quad F\}$$

viene detto la **chiusura algebrica** *di F in K.*

Corollario 1.85. *Sia L la chiusura algebrica di F in K, allora L è un campo e quindi la massima estensione algebrica di F contenuta in K.*

Dim. Siano $a, b \in L$. Allora $F(a, b)$ è algebrico su F per 1.83 quindi contenuto in L. Ma $a + b, a/b$ e ab stanno in $F(a, b)$. Quindi L è un campo. D'altro canto ogni elemento algebrico su F sta in L, da cui segue la parte finale dell'asserto . q.e.d.

Definizione 1.86. *Dati due sottocampi L_1 e L_2 di un campo F, dicesi* **composto** *di L_1 e L_2 il campo $L_1(L_2) = L_2(L_1)$, ossia il più piccolo sottocampo contenente entrambi. Verrà indicato con L_1L_2, che non va confuso con il prodotto insiemistico.*

Esercizio 1.87. *Posti $a = \sqrt{2}$, $b = \sqrt{3}$, si dimostri che $\mathbb{Q}(a)\mathbb{Q}(b) = \mathbb{Q}(a + b)$, ma $a + b$ non appartiene al prodotto insiemistico di questi due campi.*

Dim. Abbiamo già mostrato che $\mathbb{Q}(a + b) = \mathbb{Q}(a, b)$, ma chiaramente quest'ultimo contiene $\mathbb{Q}(a)$ e $\mathbb{Q}(b)$ e quindi contiene anche il loro composto. Viceversa $\mathbb{Q}(a, b) =$

$\mathbb{Q}(a)(b) \leq \mathbb{Q}(a)\mathbb{Q}(b)$. Se $a + b$ appartenesse al prodotto insiemistico di questi due campi dovrebbero esistere x_0, x_1 e y_0, y_1 in $\mathbb{Q}$ tali che $a + b = (x_0 + x_1 a)(y_0 + y_1 b)$. Siccome $1, a, b, ab$ è una base per $\mathbb{Q}(a, b)$ su $\mathbb{Q}$, ne segue che $x_i y_i = 0$ e $x_i y_j = 1$, ove $i, j \in \{1, 2\}$ e $i \neq j$. Ma queste condizioni sono incompatibili . q.e.d.

Esempio 1.88. *Sia $a = \sqrt[3]{2}$ e $\omega = e^{\frac{2\pi i}{3}}$. Allora $\mathbb{Q}(a)\mathbb{Q}(\omega) = \mathbb{Q}(a, \omega) = \mathbb{Q}(a + \omega)$. La prima identità si dimostra come sopra. Per la seconda si ponga $b = a + \omega$, allora $(b - \omega)^3 = 2$. Espandendo e tenendo conto del fatto che $\omega^3 = 1$ e $\omega^2 = -1 - \omega$, si ha $\omega = \frac{b^3 - 3b - 3}{3b^2 + 3b}$. Quindi $\omega \in \mathbb{Q}(b)$ e $a = b - \omega \in \mathbb{Q}(b)$, da cui $\mathbb{Q}(a, \omega) = \mathbb{Q}(b)$.*

1.3 Automorfismi

Ricordiamo che un omomorfismo di anelli è una mappa che preserva prodotto, somma e identità.

Definizione 1.89. *Sia K un campo. Un isomorfismo di anelli da K in K viene detto un* **automorfismo** *di K.*

Esercizio 1.90. *Dimostrare che ogni omomorfismo da un campo in sé è iniettivo.*

Dim. Sia $f \in \mathrm{End}(K)$, allora $N = \ker f$ è un ideale di K, allora $N = 0$ o K. Siccome $f(1_K) = 1_L$, il secondo caso non si verifica . q.e.d.

Definizione 1.91. *Siano K ed L estensioni di F. Allora un omomorfismo τ da K in F viene detto un* **F-omomorfismo** *se $\tau(a) = a$, $\forall a \in F$. L'insieme di tali mappe viene indicato* *con* $\hom_F(K, L)$. *Se* $L = K$ *parleremo di* F-**endomorfismi** *di* K *e li indicheremo con* $\mathrm{End}_F(K)$.

In modo equivalente $\tau \in \hom_F(K, L)$ se la restrizione di τ ad F coincide colla mappa identica, $\tau_{\restriction F} = \mathrm{id}_F$. Si noti che $\tau \in \hom_F(K, L)$ soddisfa $\tau(\alpha a) = \tau(\alpha)\tau(a) = \alpha\tau(a)$, ossia è F-lineare. Per quanto visto τ è iniettivo. Se $[K : F] = [L : F] < \infty$, allora τ è anche suriettivo, quindi un isomorfismo.

Esercizio 1.92. *Sia* $[K : F] = [L : F] < \infty$. *Si dimostri che ogni* F*-omomorfismo da* K *in* L *è una biezione.*

Il prossimo esercizio mostra che la condizione di finitezza del grado è necessaria.

Esercizio 1.93. *Sia* $X = \{x_i \mid i \in \mathbb{N}\}$ *e* F *un campo. Sia* τ *la mappa da* $K = F(X)$ *in sé definita sostituendo in ogni funzione razionale l'indeterminata* x_i *con* x_{i+1}. *Provare che* τ *è iniettiva ma non suriettiva.*

Definizione 1.94. *Sia* K *un'estensione di* F. *Il* **gruppo di Galois** $\mathrm{Gal}(K/F)$ *è l'insieme di tutti gli* F*-automorfismi di* K.

In generale se $K = F(X)$, allora un F-automorfismo è definito dichiarando l'immagine dei generatori.

Lemma 1.95. *Sia* $K = F(X)$. *Se* $\sigma, \tau \in \mathrm{Gal}(K/F)$ *e* $\sigma_{\restriction X} = \tau_{\restriction X}$, *allora* $\sigma = \tau$. *Per cui* F*-automorfismi sono determinati dalla loro azione sui generatori.*

Dim. Si ponga $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$. Sia $a \in K$, allora esistono $\alpha_1, \ldots, \alpha_n \in K$ tali che $a \in F(\underline{\alpha})$ e $f, g \in F[x_1, \ldots, x_n]$ tali che $a = f(\underline{\alpha})/g(\underline{\alpha})$. Sia $f(x) = \sum_I b_I x^I$, dove I è un **multiindice** $(i_1,\ldots,i_n)$, $b_I\in F$ e $x^I=x_1^{i_1}\cdots x_n^{i_n}$. Ora

$$\begin{aligned}\sigma(f(\alpha_1,\ldots,\alpha_n)) &= \sum_I b_I\sigma(\alpha_1)^{i_1}\cdots\sigma(\alpha_n)^{i_n} = \\ \sum_I b_I\tau(\alpha_1)^{i_1}\cdots\tau(\alpha_n)^{i_n} &= \tau(f(\alpha_1,\ldots,\alpha_n)),\end{aligned}$$

quindi $\sigma(a)=\tau(a)$. q.e.d.

Lemma 1.96. *Sia* $\tau\in\hom_F(K,L)$ *e* $\alpha\in K$ *algebrico su* F. *Se* $f(\alpha)=0$, *ove* $f\in F[x]$, *allora* $f(\tau(\alpha))=0$. *Quindi* τ *permuta le radici di* $\min_F(\alpha)$. *Inoltre* $\min_F(\alpha)=\min_F(\tau(\alpha))$.

Dim. Sia $f(x)=\sum_{i=0}^n f_ix^i$. Allora

$$0=\tau(0)=\sum_{i=0}^n\tau(f_i)\tau(\alpha)^i.$$

Ma $\tau(f_i)=f_i$ in quanto $f_i\in F$. Allora $f(\tau(\alpha))=0$. In particolare questo vale per $p=\min_F(\alpha)$. Da $p(\tau(\alpha))=0$ segue che $\min_F(\tau(\alpha))|p$, ma p è irriducibile e allora coincide con $\min_F(\tau(\alpha))$. q.e.d.

Corollario 1.97. *Se* $[K:F]<\infty$, *allora* $\mathrm{Gal}(K/F)<\infty$.

Dim. Chiaramente K/F è finitamente generata, ossia $K=F(a_1,\ldots,a_n)$ con a_i algebrico su F. Ora ogni F- automorfismo è univocamente determinato dalle immagini degli a_i e queste, per 1.96, possono essere scelte in un numero finito di modi . q.e.d.

Esempio 1.98. *Mostriamo che* $\mathrm{Gal}(\mathbb{C}/\mathbb{R})=\{\mathrm{id},\sigma\}$, *ove* σ *indica la coniugazione complessa. Chiaramente questi* *sono automorfismi. Viceversa si osservi che* $\mathbb{C} = \mathbb{R}(i)$*, ove* $i^2 + 1 = 0$*, quindi per ogni* $\mathbb{R}$*-automorfismo* $\tau(i) = \pm i$ *e* $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ *ammette solo due elementi.*

Esempio 1.99. *Sia* $a = \sqrt[3]{2}$*, allora* $\mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q}) = 1$*. Sia* $\sigma \in \mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q})$*, allora* $\sigma(a)$ *deve essere una radice di* $x^3 - 2$ *ed un elemento di* $\mathbb{Q}(a)$ *che è un sottocampo di* $\mathbb{R}$*. Siccome le altre radici di* $x^3 - 2$ *non sono reali,* $\sigma(a) = a$ *e* $\sigma = \mathrm{id}$.

Esempio 1.100. *Sia* $K = \mathbb{F}_2(t)$ *e* $F = \mathbb{F}_2(t^2)$*. Allora* $[K : F] = 2$*. Infatti* t *annulla* $x^2 - t^2 \in F[x]$*. D'altro canto* $x^2 - t^2 = (x - t)^2$ *ammette un'unica radice,* t*. Per cui* $\mathrm{Gal}(K/F) = \mathrm{id}$.

Esempio 1.101. *Sia* $F = \mathbb{F}_2$*. Il polinomio* $1 + x + x^2$ *è irriducibile su* F *poiché non ha ivi radici. Sia* $M = (1 + x + x^2)F[x]$ *e* $K = F[x]/M$*. Per 1.48* K *è un campo i cui elementi sono della forma* $a + bx + M$*, ove* $a, b \in F$*. Ora* F *è isomorfo a e può venire identificato con* $\{a + M\}$*. Si ponga* $\alpha = x + M$*, allora* $K = F(\alpha)$*. Per definire un* F*-automorfismo* σ *di* K *basta specificare* $\sigma(\alpha)$*. Questi deve essere una radice di* $1+x+x^2$*. Ma* $1+x+x^2 = (x-\alpha)(x-\alpha-1)$ *su* K*, allora* $\sigma(\alpha) = \alpha$ *o* $\alpha+1$*. Nel primo caso* $\sigma = \mathrm{id}$*. Nel secondo caso è facile provare che* $\sigma(a+b\alpha) = a+b+b\alpha$ *definisce un* F*-automorfismo. Quindi* $\mathrm{Gal}(K/F) = \{\mathrm{id}, \sigma\}$.

Esercizio 1.102. *Mostrare che* $\sigma(a + b\alpha) = a + b + b\alpha$ *definisce un automorfismo di* $F(\alpha)/F$ *ove* $\alpha^2 + \alpha + 1 = 0$ *e* $F = \mathbb{F}_2$.

L'idea chiave della Teoria di Galois è lasciare interagire teoria dei gruppi e teoria dei campi.

Definizione 1.103. *Data un'estensione K/F e un campo intermedio $F \leq L \leq K$ definiamo $\mathrm{Gal}(K/L)$ come il gruppo degli L-automorfismi di K. Viceversa dato un sottoinsieme $S \subseteq \mathrm{Aut}(K)$, definiamo*

$$\mathcal{F}(S) = \{a \in K \mid \tau(a) = a, \forall \tau \in S\}.$$

Esercizio 1.104. *Provare che per ogni $S \subseteq \mathrm{Aut}(K)$ è un sottocampo di K.*

In particolare se $S \subseteq \mathrm{Gal}(K/F)$, allora $K \geq \mathcal{F}(S) \geq F$, cioè $\mathcal{F}(S)$ è un campo intermedio.

Lemma 1.105. *Sia K un campo.*

1. *Se $L_1 \leq L_2$ sono sottocampi di K, allora $\mathrm{Gal}(K/L_1) \geq \mathrm{Gal}(K/L_2)$;*
2. *se $L \leq K$, allora $L \leq \mathcal{F}(\mathrm{Gal}(K/L))$;*
3. *se $S_1 \subseteq S_2$ sono sottoinsiemi di $\mathrm{Aut}(K)$, allora $\mathcal{F}(S_1) \supseteq \mathcal{F}(S_2)$;*
4. *se $S \subseteq \mathrm{Aut}(K)$, allora $S \subseteq \mathrm{Gal}(K/\mathcal{F}(S))$;*
5. *se $L = \mathcal{F}(S)$, allora $L = \mathcal{F}(\mathrm{Gal}(K/L))$;*
6. *se $H = \mathrm{Gal}(K/L)$, allora $H = \mathrm{Gal}(K/\mathcal{F}(H))$.*

Dim. I primi quattro punti sono facili conseguenze della definizione. Ad esempio se $\sigma \in \mathrm{Gal}(K/L_2)$, allora $\sigma(a) = a$, per ogni $a \in L_2$. Siccome $L_2 \geq L_1$, $\sigma \in \mathrm{Gal}(K/L_1)$. Per il punto 5 si supponga che $L = \mathcal{F}(S)$ per qualche sottoinsieme S di $\mathrm{Aut}(K)$. Allora $S \subseteq \mathrm{Gal}(K/L)$ e $\mathcal{F}(\mathrm{Gal}(K/L)) \leq \mathcal{F}(S) = L$. Ma $L \leq \mathcal{F}(\mathrm{Gal}(K/L))$, quindi $L = \mathcal{F}(\mathrm{Gal}(K/L))$. Per il punto 6, se $H = \mathrm{Gal}(K/L)$, per qualche sottocampo L di K, allora $L \leq \mathcal{F}(\mathrm{Gal}(K/L))$ e

$$\mathrm{Gal}(K/\mathcal{F}(\mathrm{Gal}(K/L)) \leq \mathrm{Gal}(K/L) = H.$$

Tuttavia per il punto 4, $H \leq \mathrm{Gal}(K/\mathcal{F}(H))$, quindi $H = \mathrm{Gal}(K/\mathcal{F}(H))$ e l'asserto se ne deduce . q.e.d.

Corollario 1.106. *Sia K un'estensione di F, allora esiste una biezione che inverte le inclusioni tra i sottogruppi di $\mathrm{Gal}(K/F)$ della forma $\mathrm{Gal}(K/L)$ con $L \geq F$ e l'insieme dei sottocampi intermedi $K \geq L \geq F$ della forma $\mathcal{F}(S)$ per qualche sottoinsieme S di $\mathrm{Gal}(K/F)$. La corrispondenza è data da $L \mapsto \mathrm{Gal}(K/L)$ e l'inversa da $H \mapsto \mathcal{F}(H)$.*

Dim. È un immediata conseguenza del Lemma 1.105. Se $\mathcal{G}$ e $\mathcal{F}$ sono i gruppi e i campi relativi all'enunciato, allora $L \mapsto \mathrm{Gal}(K/L)$ definisce una mappa da $\mathcal{F}$ in $\mathcal{G}$. Tale mappa è una biezione per il punto 5 del suddetto lemma. Il punto 6 dimostra che $H \mapsto \mathcal{F}(H)$ ne definisce l'inversa . q.e.d.

Data un'estensione finita K/F, sotto quali condizioni la corrispondenza $L \mapsto \mathrm{Gal}(K/L)$ definisce una corrispondenza che inverte le inclusioni tra tutti i sottogruppi di $\mathrm{Gal}(K/F)$ e tutti i sottocampi intermedi $K \geq L \geq F$?

È necessario che $F = \mathrm{Gal}(K/F)$. In realtà tale condizione risulterà anche sufficiente. Stabiliamo ora alcune relazioni tra $|\mathrm{Gal}(K/F)|$ e $[K : F]$.

Definizione 1.107. *Se G è un gruppo e K un campo, allora un* **carattere** *è un omomorfismo da G in K^*.*

Ponendo $G = K^*$, si vede che gli F-automorfismi possono essere considerati come caratteri da G in K^*.

Lemma 1.108 (Dedekind). *Siano $\tau_1, \dots, \tau_n$ caratteri distinti da G in K^*. Allora i τ_i sono linearmente indipendenti su K, ossia $\sum_i c_i \tau_i(g) = 0$ per ogni $g \in G$ implica $c_i = 0$.*

Dim. Sia k minimo tale che $\sum_{i=1}^{k} c_i\tau_i = 0$. Allora $c_i \neq 0$. Poiché $\tau_1 \neq \tau_2$, esiste $h \in G$ tale che $\tau_1(h) \neq \tau_2(h)$. Si ha $\sum_{i=1}^{k} c_i\tau_1(h)\tau_i(g) = 0$ e

$$\sum_{i=1}^{k} c_i\tau_i(gh) = \sum_{i=1}^{k} c_i\tau_i(h)\tau_i(g) = 0.$$

Sottraendo si ottiene $\sum_{i=1}^{k} c_i(\tau_1(h) - \tau_i(h))\tau_i(g) = 0$, ossia una combinazione non nulla che rappresenta l'endomorfismo nullo con meno di k termini, contro la minimalità di k . q.e.d.

Questo Lemma è il capostipite di altri risultati che sono noti come leggi di ortogonalità nell'ambito della teoria delle rappresentazioni, di cui Dedekind viene indirettamente considerato uno dei fondatori.

Proposizione 1.109. *Sia K/F finita, allora* $|\mathrm{Gal}(K/F)| \leq [K : F]$.

Dim. Il gruppo $\mathrm{Gal}(K/F)$ è finito per 1.97. Sia $\mathrm{Gal}(K/F) = \{\tau_1, \ldots, \tau_n\}$ e sia $[K : F] < n$. Sia $\alpha_1, \ldots, \alpha_m$ una F-base per K. La matrice $A = (\tau_i(\alpha_j)) \in (K)_{n\times m}$ ha quindi righe linearmente dipendenti su K. Allora esistono $c_i \in K$ non tutti nulli tali che $\sum_i \tau_i(\alpha_j) = 0$ per ogni j. Sia $G = K^*$, allora $G \ni g = \sum_j f_j\alpha_j$ per opportuni $f_j \in F$. Sicché

$$\sum_i c_i\tau_i(g) = \sum_i c_i \sum_j f_j\tau_i(\alpha_j) = \sum_j f_j(\sum_i c_i\tau_i(\alpha_j)) = 0.$$

Per il Lemma 1.108 $c_i = 0$, contro le ipotesi. Quindi $|\mathrm{Gal}(K/F)| \leq [K : F]$. q.e.d.

Si noti che il precedente risultato sarebbe ovvio se $K =$

$F[\alpha]$ fosse un'estensione semplice. In quel caso ogni automorfismo σ è determinato da $\sigma(\alpha)$. Ma questa deve essere una radice di $\min_F(\alpha)$, il cui grado coincide con $[K : F]$. Inoltre gli esempi 1.99 e 1.100 mostrano che la disuguaglianza può essere stretta.

Proposizione 1.110 (Artin). *Sia G un sottogruppo finito di $\mathrm{Aut}(K)$ e $F = \mathcal{F}(G)$. Allora $|G| = [K : F]$ e $G = \mathrm{Gal}(K/F)$.*

Dim. Per 1.109 $|G| \leq [K : F]$. Sia $n = |G| < [K : F]$ e si scelgano $\alpha_1, \ldots, \alpha_{n+1} \in K$ linearmente indipendenti su F. Se $G = \{\tau_1, \ldots, \tau_n\}$, allora $A = (\tau_i(\alpha_j)) \in (K)_{n\times(n+1)}$ ha colonne linearmente dipendenti. Sia k il minimo numero di colonne linearmente dipendenti (ad esempio siano le prime k). Allora esistono $c_i \in K$ tali che $\sum_{i=1}^k c_i\tau_j(\alpha_i) = 0$ per ogni j. Per minimalità $c_i \neq 0$, allora posso supporre che $c_1 = 1$. Se $c_i \in F$, allora $0 = \tau_j(\sum_i c_i\alpha_i)$ e l'argomento di τ_j sarebbe nullo contro la F-indipendenza degli α_i. Allora esiste $c_2 \notin F$ e quindi $\sigma \in G$ tale che $\sigma(c_2) \neq c_2$. Applicando σ ottengo $\sum_i \sigma(c_i)\tau_j(\alpha_j) = 0$ per ogni j. Sottraendo la somma originaria ottengo $\sum_{i=2}^k(\sigma(c_i) - c_i)\tau_j(\alpha_i) = 0$ per ogni j, contro la minimalità di k. Pertanto $|G| = [K : F]$. In particolare $G = \mathrm{Gal}(K/F)$ essendo $G \leq \mathrm{Gal}(K/F)$ e $|G| = [K : F] \geq \mathrm{Gal}(K/F)$. q.e.d.

Definizione 1.111. *Sia K un'estensione algebrica di F. Allora K dicesi* **estensione di Galois** *di F se $F = \mathcal{F}(\mathrm{Gal}(K/F))$.*

Noi ci occuperemo esclusivamente del caso $[K : F] < \infty$.

Corollario 1.112. *Sia K/F finita, allora K/F è di Galois sse $|\mathrm{Gal}(K/F)| = [K : F]$.*

Dim. Se K/F è di Galois, allora $F = \mathcal{F}(\mathrm{Gal}(K/F))$ e, per 1.110 $|\mathrm{Gal}(K/F)| = [K : F]$. Viceversa si ponga $L = \mathcal{F}(\mathrm{Gal}(K/F))$. Allora $\mathrm{Gal}/K/F) = \mathrm{Gal}(K/L)$ per 1.110 e $|\mathrm{Gal}(K/F)| = [K : L] \leq [K : F]$. Siccome $|\mathrm{Gal}(K/F)| = [K : F]$, si ha $[K : L] = [K : F]$, per cui $F = L$. q.e.d.

Purtroppo determinare $\mathrm{Gal}(K/F)$ è un compito difficile in generale.

Corollario 1.113. *Sia $K = F[a]$ un'estensione algebrica semplice di F. Allora $|\mathrm{Gal}(K/F)|$ è uguale al numero di radici distinte di $\min_F(a)$. Per cui K/F è Galois sse $\min_F(a)$ ha n radici distinte, ove $n = \deg \min_F(a)$.*

Dim. Sia $\tau \in G = \mathrm{Gal}(K/F)$, allora $\tau(a)$ è una radice di $\min_F(a)$. Siccome $\tau(a)$ determina unicamente τ, si ha che $|G|len$. Viceversa sia $b \in K$ una radice di $\min_F(a)$ e si definisca una mappa $\tau \in F^F$, mediante $\tau(f(a)) = f(b)$ (ossia τ coincide colla sostituzione $a \mapsto b$). Allora è immediato provare che $\tau \in G$. Quindi $|G|$ è uguale al numero di radici distinte di $\min_F(a)$. Siccome $[K : F] = \deg \min_F(a)$, K/F è di Galois sse $\min_F(a)$ ha tutte radici distinte in K . q.e.d.

Esistono due casi in cui $p = \min_F(a)$ non abbastanza radici distinte in K: o non tutte le radici di p stanno in K, oppure p ammette radici multiple. Gli esempi 1.99 e 1.100 mostrano che entrambi i casi sono possibili.

Esempio 1.114. *L'estensione $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è di Galois, poiché ha grado 3 ma $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ è banale.*

Definizione 1.115. *Dato un campo K sia $u : \mathbb{Z} \to K$ definita via $n^u = n1_K$. Ovviamente u è un omomorfismo di anelli. Siccome K è un dominio, $\ker u$ è un ideale primo o* *nullo di $\mathbb{Z}$. Sia p il suo generatore, allora p viene detto la* **caratteristica**, $\mathrm{char}(K)$ *di K.*

Esercizio 1.116. *Dimostrare che* $\ker u$ *è un ideale primo o nullo di $\mathbb{Z}$.*

Esempio 1.117. *Sia k un campo di caratteristica $p > 0$ e $K = k(t)$ il campo delle funzioni razionali su k. Allora l'estensione $k(t)/k(t^p)$ ha grado p. D'altra parte il polinomio $x^p - t^p = (x-t)^p$ ammette una sola radice in $k(t)$. Quindi $k(t)/k(t^p)$ non è di Galois.*

Esempio 1.118. *Sia F un campo tale che* $\mathrm{char}(F) \neq 2$*, sia $a \in F \smallsetminus F^2$, ove F^2 indica l'insieme dei quadrati di F e sia infine $M = (x^2 - a)$ l'ideale generato da $x^2 - a$. Allora $K = F[x]/M$ è un campo, essendo $x^2 - a$ irriducibile. Posto $u = x + M \in K$, si vede che $K = F[u]$. Ora $[K : F] = 2$. Sia $\sigma(a + bu) = a - bu$, per ogni $a, b \in F$, allora σ è un F-automorfismo di K, allora $2 \leq |\mathrm{Gal}(K/F)| \leq [K : F]$ e K/F è di Galois.*

Esempio 1.119. *Sia $a = \sqrt[3]{2}$, $b = e^{\frac{2\pi i}{3}}$, e $K = \mathbb{Q}(a, b)$ allora $K/\mathbb{Q}$ è di Galois. Infatti il grado dell'estensione è 6 essendo $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, $[\mathbb{Q}(b) : \mathbb{Q}] = 2$ e $b \notin \mathbb{Q}(a)$. Siccome ogni $\mathbb{Q}$-automorfismo σ di K è univocamente determinato da $\sigma(a), \sigma(b)$, possiamo individuare σ mediante una coppia (a', b') di elementi di K. Inoltre a' è radice di $x^3 - 2$ e b' di $x^2 + x + 1$. Quindi ho 6 possibili coppie $(a, b), (ab, b), (a, b^2), (ab^2, b), (ab, b^2), (ab^2, b^2)$. Ognuna di esse realizza un automorfismo.*

Esercizio 1.120. *Sia $a = \sqrt[3]{2}$, $b = e^{\frac{2\pi i}{3}}$, e $K = \mathbb{Q}(a, b)$. Detta τ la mappa individuata da (ab, b) e σ quella individuata da (a, b^2), dimostrare che realizzano automorfismi di K e* *provare che $\langle \tau, \sigma \rangle$ è il gruppo diedrale di ordine 6 (ossia il gruppo delle simmetrie di un triangolo equilatero).*

Esempio 1.121. *Sia k un campo, $\underline{x} = (x_1, \dots, x_n)$ e $K = k(\underline{x})$. Data una permutazione $\sigma \in S_n$, il gruppo simmetrico su n oggetti, sia $\underline{x}^\sigma = (x_{1^\sigma}, \dots, x_{n^\sigma})$. Estendiamo σ a tutto K come segue:*

$$\left(\frac{f(\underline{x})}{g(\underline{x})}\right)^\sigma = \frac{f(\underline{x}^\sigma)}{g(\underline{x}^\sigma)}.$$

Un po' di fatica consente di provare che σ definisce un k-automorfismo di K. Quindi $S_n \leq \mathrm{Aut}(K)$. Sia $F = \mathfrak{F}(S_n)$. Per 1.110 K/F è un'estensione di Galois con $\mathrm{Gal}(K/F) = S_n$. F viene detto il campo delle **funzioni simmetriche** *negli x_i. Questo segue dal fatto che $\frac{f(\underline{x})}{g(\underline{x})} \in F$ implica $\frac{f(\underline{x})}{g(\underline{x})} = \frac{f(\underline{x}^\sigma)}{g(\underline{x}^\sigma)}$. Siano*

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n, \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ &\vdots \\ s_n &= x_1x_2 \cdots x_n. \end{aligned}$$

I polinomi s_i vengono detti i polinomi simmetrici elementari. Ovviamente $k(s_1, \dots, s_n) \leq F$. Si noti che

$$\prod_{i=1}^{n}(t - x_i) = t^n + \sum_{i=0}^{n-1}(-)^i s_i t^{n-i},$$

ove $s_0 = 1$.

1.4 Estensioni Normali

Abbiamo visto che un'estensione algebrica semplice $F[a]/F$ è di Galois sse tutte le radici di $\min_F(a)$ stanno in $F[a]$ e sono distinte. In questo paragrafo analizziamo il primo caso.

Lemma 1.122 (Ruffini). *Sia* $f(x) \in F[x]$ *e* $a \in F$*, allora* $f(a) = 0$ *sse* $x - a | f(x)$*. Inoltre* f *ammette al più* $\deg(f)$ *radici.*

Dim. Per l'algoritmo della divisione $f = q \cdot (x - a) + r$, ove $\deg r < \deg x - a$, ossia $r \in F$. Ma $f(a) = r$, quindi $f(a) = 0$ sse $x - a | f(x)$. Sia ora a una radice di f, allora $f = (x - a)q$, ove $q \in F[x]$. Per induzione su $\deg f$ possiamo assumere che il numero di radici di q sia al più $\deg q = \deg f - 1$, da cui segue la seconda parte dell'asserto . q.e.d.

Definizione 1.123. *Sia* $f \in F[x]$ *e* K *un'estensione di* F*. Allora si dice che* f **spezza** *su* K *se* $f(x) = a \prod_i (x - a_i)$ *per opportuni elementi* $a_i \in K$*.*

Esercizio 1.124. *Dimostrare che* $x^2 + 1 \in \mathbb{R}[x]$ *si spezza su* $\mathbb{C}$*. Più in generale, sia* $p(x) \in F[x]$ *un polinomio di grado due e sia* $a \in K$*,* K *un'estensione di* F*, una radice di* p*. Mostrare che* p *spezza in* K*.*

Esercizio 1.125. *Sia* p *un primo e* $f = \sum_{i=0}^{p-1} x^i \in \mathbb{Q}[x]$*. Sia* $\omega = e^{\frac{2\pi i}{p}}$*. Provare che* f *spezza su* $\mathbb{Q}(\omega)$*.*

Teorema 1.126 (Kronecker). *Abbia* $f(x) \in F[x]$ *grado* n*. Allora esiste un'estensione* K *di* F *che contiene una radice di* f *e* $[K : F] \leq n$*. Inoltre esiste un 'estensione* L/F *su cui* f *spezza e* $[L : F] \leq n!$*.*

Dim. Sia $p(x)$ un fattore irriducibile di $f(x)$ in $F[x]$ e sia $M = (p(x))$. Allora $K = F[x]/M$ è un campo ed esiste monomorfismo da F in K, ossia la mappa $\phi : a \mapsto a + M$. Rimpiazzando F con $\phi(F)$, possiamo assumere che K sia un'estensione di F. Inoltre $\alpha = x + M \in K$ è una radice di p e quindi di f. Poiché $[K : F] = \deg p \leq \deg f$, abbiamo la prima parte dell'asserto.

Ora $f(x) = (x-\alpha)g(x)$ in $K[x]$. Per induzione su n esiste un'estensione L/K di grado minore o uguale a $(n-1)!$ su cui g si spezza. Ma allora anche f spezza su L e $[L : F] = [L : K][K : F] \leq n(n-1)! = n!$. q.e.d.

Definizione 1.127. *Sia K un'estensione di F e $f(x) \in F[x]$.*

1. *Se $f(x) \in F[x]$, allora K è un* **campo di spezzamento** *per f su F se f si spezza su K e $K = F(a_1, \ldots, a_n)$, ove $a_1, \ldots, a_n$ sono le radici di f;*

2. *se S è un insieme di polinomi non costanti su F, allora K è un campo di spezzamento per S su F se ogni $f \in S$ si spezza su K e $K = F(X)$, ove X è l'insieme di tutte le radici di tutti i polinomi in S.*

Intuitivamente un campo di spezzamento per un insieme S è la minima estensione su cui i polinomi in S si spezzano.

Corollario 1.128. *Sia $S = \{f_1, \ldots, f_n\}$ un sottoinsieme finito di $F[x]$. Allora esiste un campo di spezzamento per S su F.*

Dim. Si ponga $f = \prod_i f_i$, allora K è un campo di spezzamento per f sse lo è per S. Per 1.126 segue il risultato . q.e.d.

Esempio 1.129. *Sia $a = \sqrt[3]{2}$ e $b = e^{\frac{2\pi i}{3}}$, allora il campo $K = \mathbb{Q}(a, b)$ è di spezzamento per il polinomio $p = x^3 - 2 \in \mathbb{Q}[x]$. Infatti questo polinomio ammette a, ab, ab^2 come radici. Quindi p si spezza su K. Inoltre ogni campo di* *spezzamento contiene necessariamente a e $b = ab/a$, quindi contiene K.*

Corollario 1.130. *Sia $f \in F[x]$ di grado n. Se K è un campo di spezzamento di f su F, allora $[K : F] \leq n!$.*

Dim. Per induzione su $\deg f$. Se $n = 1$ è ovvio. Sia K di spezzamento per f su F e sia $a \in K$ una radice di f. Allora $f = (x - a)g$ e $\deg g = n - 1$. Inoltre K è di spezzamento per g su $F[a]$. Ma $[F[a] : F] \leq n$, essendo $\min_F(a)$ un divisore di f, quindi $[K : F] = [K : F[a]][F[a] : F] \leq (n-1)!n$. q.e.d.

Esempio 1.131. *Sia k un campo e $K = k(x_1, \ldots, x_n)$. Abbiamo già visto come definire un'azione di S_n su K. Sia $F = \mathcal{F}(S_n)$, allora $S_n = \mathrm{Gal}(K/F)$ per 1.110 e $[K : F] = |S_n| = n!$. Siano s_i le funzioni simmetriche elementari, ossia $s_i = \sum_I x^I$, ove $I = (i_1, \ldots, i_n)$ è un multiindice di lunghezza $|I| = \sum_j i_j = i$, $i_j \in \mathbb{N}_{\geq 0}$ e $x^I = \prod_j x_j^{i_j}$. Allora $k(s_1, \ldots, s_n) \leq F$. Vogliamo mostrare che $k(s_1, \ldots, s_n) = F$. Sia $f(t) = \prod_{i=1}^n (t - x_i) \in K[t]$, allora $f(t) = \sum_{i=0}^n (-)^i s_i x^{n-i}$, ove si pone $s_0 = 1$. Ora K è generato dagli x_i su k, quindi è un campo di spezzamento per $f(t)$ su $k(s_1, \ldots, s_n)$. Poiché $[K : F] = |S_n| = n!$, $[K : k(s_1, \ldots, s_n)] \geq n!$. Tuttavia $[K : k(s_1, \ldots, s_n)] \leq n!$ per 1.130. Per cui $F = k(s_1, \ldots, s_n)$ e ogni funzione razionale simmetrica è una funzione razionale nelle funzioni simmetriche elementari.*

Chiusure Algebriche

Lemma 1.132. *Sia K un campo allora le seguenti affermazioni sono equivalenti:*

1. *Non esistono estensioni algebriche proprie di K;*
2. *non esistono estensioni finite proprie di K;*
3. *se L è un'estensione di K, allora $K = \{a \in L \mid a \text{ è algebrico su } F\}$;*
4. *ogni $f(x) \in K[x]$ si spezza;*
5. *ogni $f(x) \in K[x]$ ammette una radice in K;*
6. *ogni polinomio irriducibile su K ha grado* 1.

Dim. $(1) \Rightarrow (2)$: Infatti ogni estensione finita è algebrica.
$(2) \Rightarrow (3)$: Sia a algebrico su K, allora $K(a)$ è un'estensione finita di K e $K(a) = K$, cioè $a \in K$.
$(3) \Rightarrow (4)$: Sia $f(x) \in K[x]$ e sia L un campo di spezzamento di f su K. Siccome L è algebrico su K, ne segue che $L = K$, ossi f si spezza su K.
$(4) \Rightarrow (5)$: banale.
$(5) \Rightarrow (6)$: Sia $f \in K[x]$ irriducibile. Allora f ammette una radice in K, ossia f ha un fattore lineare e quindi f ha grado 1, essendo irriducibile. $(6) \Rightarrow (1)$: Sia L un'estensione algebrica di K. Si prenda $a \in L$ e sia $p(x) = \min_K(a)$. Allora $\deg p = 1$ e $a \in K$. q.e.d.

Definizione 1.133. *Se K soddisfa una delle condizioni equivalenti del Lemma 1.132, allora K dicesi* **algebricamente chiuso**. *Se K è un'estensione algebrica di F e K è algebricamente chiuso, allora K dicesi una* **chiusura algebrica** *di F.*

Esempio 1.134. *Il campo dei complessi $\mathbb{C}$ è algebricamente chiuso, fatto che verrà in seguito provato sotto il nome di* **Teorema Fondamentale dell'Algebra**. *Sia*

$$\mathbb{A} = \{a \in \mathbb{C} \mid a \text{ è algebrico su } \mathbb{Q}\},$$

allora $\mathbb{A}$ è algebricamente chiuso. Infatti se $f(x) \in \mathbb{A}[x]$, allora f si spezza in $\mathbb{C}$. Ne sia a una radice, allora a è algebrica su $\mathbb{A}$ e quindi su $\mathbb{Q}$ per 1.83, cioè $a \in \mathbb{A}$. Si noti che $\mathbb{A} \neq \mathbb{C}$, poiché $\mathbb{C}/\mathbb{Q}$ non è algebrica.

Desideriamo provare che ogni campo ammette una chiusura algebrica e quindi che ogni insieme di polinomi ammette un campo di spezzamento. A tal fine abbiamo bisogno di alcuni risultati di Aritmetica Cardinale e del Lemma di Zorn. Si ricorda che $\aleph_0 = |\mathbb{N}|$.

Lemma 1.135. *Se K/F è algebrica, allora $|K| \leq \max\{|F|, \aleph_0\}$.*

Dim. Dato $a \in K$, siano $a_1, \ldots, a_n$ le radici di $\min_F(a)$ in K. Se $\mathcal{M}$ è l'insieme di tutti i polinomi monici su F si definisca $f : K \to \mathcal{M} \times \mathbb{N}$ mediante $f(a) = (\min_F(a), r)$ se $a = a_r$. Essendo f iniettiva, allora $|K| \leq |\mathcal{M} \times \mathbb{N}| = \max\{|\mathcal{M}|, \aleph_0\}$. Basta mostrare che $|\mathcal{M}| \leq \max\{|F|, \aleph_0\}$. Sia $\mathcal{M}_n$ l'insieme dei polinomi monici di grado n, allora $|\mathcal{M}_n| = |F^n|$, essendo $(a_0, \ldots, a_{n-1}) \mapsto x^n \sum_{i=0}^{n-1} a_i x_i$ una biezione. Se F è finito, allora F^n è finito, altrimenti $|F^n| = |F|$ (in particolare i punti di un segmento sono i corrispondenza biunivoca coi punti di un quadrato). Pertanto $|\mathcal{M}| = |\bigcup \mathcal{M}_n| = \max\{|F|, \aleph_0\}$. q.e.d.

Esercizio 1.136. *Sia $I = [0, 1] \subset \mathbb{R}$, allora ogni elemento di I è descritto dalla sua espansione decimale $a = 0.a_1a_2\ldots$. Si definisca $f : I^2 \to I$, come segue $f(a, b) = 0.a_0b_0a_1b_1\ldots$. Provare che f realizza una biezione tra I^2 e I.*

Teorema 1.137. *Sia F un campo. Allora F ammette una chiusura algebrica.*

Dim. Sia S un insieme contente F tale che $|S| > \max\{|F|, \aleph_0\}$. Sia $\mathcal{A}$ l'insieme di tutte le estensioni algebriche di F interne ad S. Allora $\mathcal{A}$ è ordinato rispetto all'inclusione. Per il Lemma di Zorn esiste un elemento massimale M di $\mathcal{A}$. Vogliamo provare che M è una chiusura algebrica di F. Sia L un'estensione algebrica di M. Allora per 1.135

$$|L| \leq \max\{|M|, \aleph_0\} \leq \max\{|F|, \aleph_0\} < |S|.$$

Per cui esiste una funzione $f : L \to S$ tale che $f_{\restriction M} = \mathrm{id}$. Definendo $f(a+b) = f(a) + f(b)$ e $f(a).f(b) = f(ab)$, allora $f(L)$ risulta essere un'estensione di M ed f un omomorfismo. Per massimalità $f(L) = M$ e $L = M$. Per tanto M è algebricamente chiuso. essendo algebrico su F, ne è chiusura algebrica . q.e.d.

Esercizio 1.138 (Artin). *(Difficile) Sia F un campo e sia S l'insieme dei polinomi monici irriducibili su F. Sia $A = F[x_f \,|\, f \in S]$ un anello di polinomi in una variabile per ogni $f \in S$. Sia $I \trianglelefteq A$, l'ideale generato da $f(x_f)$, $f \in S$. Provare che $I \neq A$. Sia allora M un ideale massimale che contiene I e $F_1 = A/I$. Provare che F_1 è un'estensione di F e che ogni f ammette una radice in F_1. Dato F_i si costruisca F_{i+1} ripetendo questa procedura. Sia $L = \bigcup_{i=1}^{\infty} F_i$. Mostrare che f si spezza in L e che la chiusura algebrica di F in L è una chiusura algebrica di F.*

Traiamo subito una conseguenza da questo risultato tecnico.

Corollario 1.139. *Sia S un insieme di polinomi non costanti su F. Allora S ammette un campo di spezzamento su F.*

Dim. Sia K una chiusura algebrica di F. Allora tutti gli elementi di S si spezzano su K e sia X l'insieme delle relative radici. Allora $F(X) \leq K$ è un campo di spezzamento per S su F . q.e.d.

Corollario 1.140. *Se F è un campo, allora il campo di spezzamento L di tutti i polinomi non costanti su F è una chiusura algebrica di F.*

Dim. Chiaramente L/F è algebrica. Sia K una chiusura algebrica di L e sia $a \in L$. Allora per 1.83 a è algebrico su F. Siccome $\min_F(a)$ si spezza su L ne segue che $a \in L$ e L è algebricamente chiuso . q.e.d.

Provata l'esistenza ci si può chiedere quanti campi di spezzamento è possibile determinare. Dato $\sigma \in \hom(F, F')$ è possibile estendere σ a tutto $F[x]$, definendo $(\sum_i a_i x^i)^\sigma = \sum_i a_i^\sigma x^i$. Se $f(x) = \prod_i (x - a_i)$, allora $f(x)^\sigma = \prod_i (x - a_i^\sigma)$.

Lemma 1.141. *Sia $\sigma \in \hom(F, F')$ un isomorfismo di campi. Sia $f(x) \in F[x]$ irriducibile. Sia α una radice di f in qualche estensione K di F e α' una radice di f^σ in qualche estensione K' di F'. Allora esiste un isomorfismo $\tau : F(\alpha) \to F'(\alpha')$, tale che $\tau(\alpha) = \alpha'$ e $\tau_{\restriction F} = \sigma$.*

Dim. Siccome f è irriducibile e $f(\alpha) = 0$, il polinomio minimo di α su F è un multiplo scalare di f. Quindi f e $\min_F(\alpha)$ generano lo stesso ideale principale M in $F[x]$. Allora esiste un F-isomorfismo $\phi : F[x]/M \to F(\alpha)$ definito da $\phi(g(x) + M) = g(\alpha)$. Analogamente esiste $\psi : F'[x]/M' \to F'(\alpha')$ definito da $\psi(g(x) + M) = g(\alpha')$, ove $M' = (f^\sigma)$. Inoltre $\nu : F[x]/M \to F'[x]/M'$ definito da $\nu(g(x) + M) = g(x) + M'$ realizza un F isomorfismo.

Pertanto $\tau = \phi^{-1} \circ \nu \circ \psi : F(\alpha) \to F'(\alpha')$ è un isomorfismo che estende σ e tale che $\tau(\alpha) = \alpha'$. q.e.d.

Lemma 1.142. *Sia $\sigma \in \hom(F, F')$ un isomorfismo di campi, K un'estensione di F e K' un'estensione di F'. Sia K un campo di spezzamento per $\{f_i\}$ su F e $\tau : K \to K'$ sia un omomorfismo tale che $\tau_{\restriction F} = \sigma$. Se $f_i' = f_i^\sigma$, allora $\tau(K)$ è un campo di spezzamento per $\{f_i'\}$ su F'.*

Dim. Poiché K è un campo di spezzamento per $\{f_i\}$, esistono $a, \alpha_1, \ldots, \alpha_n \in K$ tali che $f_i(x) = a \prod_i (x - \alpha_i)$. Allora $f_i^\tau = a^\tau \prod_i (x - \alpha_i^\tau)$. Siccome K è generato dalle radici di f_i su F, K^τ è generato dalle radici degli f_i', ossia è un campo di spezzamento per $\{f_i'\}$ su F' . q.e.d.

Mostriamo ora il teorema di estensione di un isomorfismo, uno strumento cruciale per la determinazione del gruppo di Galois e per la costruzione di automorfismi.

Teorema 1.143. *Sia $\sigma \in \hom(F, F')$, $f(x) \in F[x]$ e $f^\sigma \in F'[x]$ il polinomio corrispondente. Siano K e K' campi di spezzamento per f e f^σ su F e F' rispettivamente. Allora esiste un isomorfismo $\tau \in \hom(K, K')$, tale che $\tau_{\restriction F} = \sigma$. Inoltre se α è una radice di f in K e α' è una qualsiasi radice di $\min_F(\alpha)^\sigma$ in K', allora τ può essere scelto in modo che $\alpha^\tau = \alpha'$.*

Dim. Per induzione su $n = [K : F]$. Se $n = 1$, allora f spezza su F e $\tau = \sigma$. Si assuma il risultato vero per estensioni di grado minore di n. Se f si spezza su F, allora il risultato è vero. Altrimenti sia $p(x)$ un fattore irriducibile di f e α una radice di p e α' una di p^σ. Si ponga $L = F(\alpha)$ e $L' = F(\alpha')$. Allora $[L : F] > 1$ e $[K : L] < n$. Per il Lemma 1.141 esiste un isomorfismo $\rho \in \hom(L, L')$ tale che $\rho(\alpha) = \alpha'$. Siccome K è un campo di spezzamento per f su L e K' lo è per f' su F', ρ si estende ad un isomorfismo $\tau \in \hom(K, K')$ che soddisfa le richieste dell'asserto. Ovviamente τ estende σ . q.e.d.

Teorema 1.144. *Sia* $\sigma \in \hom(F, F')$ *un isomorfismo. Sia* $S = \{f_i\}$ *un insieme di polinomi*