Algebra 2 — Teoria dei Campi

Indrjo Dedej

Ultima revisione: 30 giugno 2024

Indice

Testi di riferimento

[Alu] P. Aluffi. *Algebra: Notes from the Underground*. In particolare i capitoli 13, 14 e 15. Cambridge University Press.

[Can21] A. Canonaco. *Algebra 2 — Teoria dei Campi*. 2021. URL: https://www-dimat.unipv.it/canonaco/2020-2021/alg2.html.

[Gar] D.J.H. Garling. *A Course in Galois Theory*. Cambridge University Press.

[Her] I.N. Herstein. *Algebra*. In particolare il capitolo 5. Editori Riuniti University Press.

[Lei] T. Leinster. *Galois Theory*. URL: https://www.maths.ed.ac.uk/~tl/gt/gt.pdf.

[Mil] James S. Milne. *Fields and Galois Theory*. In particolare i capitoli 1, 2 e 3. URL: https://www.jmilne.org/math/CourseNotes/FT.pdf.

[SG] R. Schoof e B. van Geemen. *Algebra*. In particolare il capitolo 14. URL: http://www-dimat.unipv.it/canonaco/notealgebra.pdf.

[Tsu] Yu Tsumura. *Problems in Mathematics – Field Theory*. URL: https://yutsumura.com/category/field-theory/.

Sommario

Queste pagine partono da [Can21], note usate per il corso di Algebra 2 nell'anno 2021. Tuttavia è bene tenere conto che:

- Ci sono integrazioni e cambiamenti in alcune parti.
- Sono stati inseriti alcuni richiami più o meno estesi ad argomenti di Algebra 1.
- La bibliografia originaria è stata estesa.

Importante: spesso il discorso può essere troncato nel mezzo e le notazioni possono essere incoerenti. Eventuali errori sono da attribuire a chi sta mantenendo queste note e sta facendo integrazioni.

1 Caratteristica di un anello

In queste pagine gli anelli sono tutti dotati di identità moltiplicativa e gli omomorfismi di anelli preservano questi elementi.

Lemma 1.1. Per ogni anello R esiste uno e un solo omomorfismo $\mathbb{Z} \to R$.

Dimostrazione. Scriviamo esplicitamente questo omomorfismo:

$$\phi : \mathbb{Z} \to R\,,\ \phi(n) := \begin{cases} \underbrace{\phi(1) + \ldots + \phi(1)}_{n \text{ volte}} & \text{se } n \geq 0 \\ -\phi(-n) & \text{altrimenti} \end{cases}.$$

Che questo sia effettivamente un omomorfismo e che sia l'unico è facilmente verificabile. □

Definizione 1.2. La *caratteristica* di un anello R è il numero naturale $\mathrm{char}(R)$ per cui, indicato con $\phi : \mathbb{Z} \to R$ indica l'unico omomorfismo di anelli, si ha

$$\mathrm{char}(R)\mathbb{Z} = \ker \phi.$$

$\mathbb{Z}$ è un dominio ad ideali principali: per questo, si può definire la caratteristica di R come il generatore ≥ 0 dell'ideale $\ker \phi$. In alcuni libri potreste trovare definita la caratteristica di R come proprio l'ideale $\ker \phi$.

Esempio 1.3. Alcuni esempi:

- $\mathrm{char}(\mathbb{Z}) = 0$. Infatti un omomorfismo $\mathbb{Z} \to \mathbb{Z}$ è l'identità: a causa del Lemma 1.1, questo è l'unico che può esserci. Così stando le cose, il nucleo è banale.
- $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n$ con $n \geq 1$. La proiezione al quoziente $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$: di nuovo a causa del Lemma 1.1, è l'unico che può esserci. Il nucleo di questo omomorfismo è $n\mathbb{Z}$.

  Per il Primo Teorema di Isomorfismo si ha che

$$\mathrm{im}\left(\mathbb{Z} \xrightarrow{\phi} R\right) \cong \frac{\mathbb{Z}}{\mathrm{char}(R)\mathbb{Z}}.$$

Questo vuol dire, ad esempio, che gli anelli a caratteristica n contengono al loro interno una copia isomorfa di $\mathbb{Z}/n\mathbb{Z}$. In particolare, la caratteristica è 0, l'anello contiene una copia di $\mathbb{Z}$ e quindi è necessariamente infinito.

Vale anche il viceversa: un anello che contiene una copia isomorfa a $\mathbb{Z}/n\mathbb{Z}$ ha caratteristica n. E per rendersi conto ciò abbiamo bisogno di un semplice teorema.

Proposizione 1.4. Se R e S sono due anelli e se esiste un omomorfismo iniettvo $i : R \to S$, allora $\mathrm{char}(R) = \mathrm{char}(S)$.

Dimostrazione. Scriviamo $\phi_R : \mathbb{Z} \to R$ e $\phi_S : \mathbb{Z} \to S$ gli unici omomorfismi che ci possono essere. Ne segue quindi che $\phi_S = i\phi_R$. Se riusciamo a mostrare che i due omomorfismi hanno lo stesso nucleo, allora possiamo concludere. Viceversa, se $x \in \ker \phi_S$, allora $0 = \phi_S(x) = i\left(\phi_R(x)\right)$, da cui $\phi_R(x) = 0$ perché i è iniettiva. □

Osserviamo che la caratteristica non è esattamente un affare di cardinalità. Certo, gli anelli finiti, hanno caratteristica non nulla e gli anelli a caratteristica 0 sono infiniti. Tuttavia, possiamo farci un semplice esempio in cui la caratteristica un anello sia non nulla e la sua cardinalità infinita.

Esempio 1.5. L'anello $\mathbb{Z}/2\mathbb{Z}$ ha caratteristica 2. Ma anche $\mathbb{Z}/2\mathbb{Z}[X]$ ha caratteristica 2 grazie all'inclusione $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathbb{Z}/2\mathbb{Z}[X]$, e certamente non ha cardinalità finita.

Noi ci interesseremo di campi da un certo punto in poi: è utile richiamare una proprietà fondamentale allora.

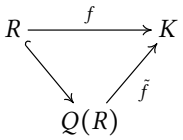
Proposizione 1.6. Sia R un anello con divisione e S un anello non banale. Allora ogni omomorfismo $f : R \to S$ è iniettivo.

Dimostrazione. $\ker f$ è banale. Infatti gli unici ideali di R sono quello banale e R stesso. Poiché S non è banale, $0 \neq 1$ e quindi $1 \notin \ker f$. Pertanto il nucleo non può essere R. □

Corollario 1.7. Gli omomorfismi di campi sono tutti iniettivi. Se esiste un omomorfismo di campi $K \to L$, allora K e L hanno la stessa caratteristica. Equivalentemente, se due campi hanno caratteristica diversa, non possono esserci omomorfismi tra loro.

Rimandiamo al corso di Algebra 1, la costruzione del *campo delle frazioni* $Q(R)$ a partire da un dominio di integrità R. A causa dell'omomorfismo iniettivo $R \to Q(R)$ che manda a in $a/1$, possiamo scrivere a al posto di $a/1$. Ricordiamo in particolare come a/b è una classe di equivalenza sotto una certa relazione di equivalenza su $R \times (R \setminus \{0\})$. Questo campo ha una notevole proprietà universale.

Lemma 1.8. Siano R un dominio di integrità, K un campo qualsiasi e $f : R \to K$ omomorfismo iniettivo. Allora esiste uno e un solo omomorfismo iniettivo $\tilde{f} : Q(R) \to K$ per cui commuta



Dimostrazione. Introduciamo immediatamente $\tilde{f}$:

$$\tilde{f}(a/b) := f(a)f(b)^{-1}.$$

È un omomorfismo: per ogni $a, c \in R$ e $b, d \in R \setminus \{0\}$ si ha

$$\begin{aligned}
\tilde{f}((a/b) + (c/d)) &= \tilde{f}((ad + bc)/(bd)) = f(ad + bc)f(bd)^{-1} = \\
&= f(a)f(b)^{-1} + f(c)f(d)^{-1} = \tilde{f}(a/b) + \tilde{f}(c/d) \\
\tilde{f}((a/b)(c/d)) &= \tilde{f}((ac)/(bd)) = f(ac)f(bd)^{-1} = \\
&= f(a)f(b)^{-1}f(c)f(d)^{-1} = \tilde{f}(a/b)\tilde{f}(c/d) \\
\tilde{f}(1) &= f(1) = 1.
\end{aligned}$$

Poiché l'omomorfismo di inclusione è iniettivo, allora i nuclei di f e $\tilde{f}$ sono uguali: quindi $\tilde{f}$ è pure iniettivo. L'unicità è praticamente contenuta nella definizione di $\tilde{f}$. □

Questo lemma è interessante. L'iniezione $f : R \to K$ individua all'interno di K una copia isomorfa a R: il lemma dice che se K ha il suo interno una copia di R, allora contiene tutto $Q(R)$. L'ovvia applicazione riguarda $\mathbb{Z}$ e $\mathbb{Q}$ e la nozione di caratteristica di anello.

Corollario 1.9. Se K è un campo di caratteristica 0, allora contiene al suo interno una e una sola copia isomorfa a $\mathbb{Q}$. Vale a dire: esiste ed un solo omomorfismo iniettivo $\mathbb{Q} \to K$.

Dimostrazione. Dal Lemma 1.1 sappiamo che c'è un unico omomorfismo $\mathbb{Z} \to K$. Da ipotesi questo omomorfismo è iniettivo e per il Lemma 1.8 esiste esattamente un omomorfismo iniettivo $\mathbb{Q} \to K$. □

Questo teorema è a riepilogo delle considerazioni fatte fino ad ora.

Teorema 1.10. Un campo K ha al suo interno una copia isomorfa a $\mathbb{Z}/p\mathbb{Z}$ con p primo (nel qual caso, $p = \operatorname{char}(K)$) oppure a $\mathbb{Q}$ (nel qual caso $0 = \operatorname{char}(K)$).

Dimostrazione. Per il Lemma 1.1, c'è un unico omomorfismo $\phi : \mathbb{Z} \to K$. Se è iniettivo, allora K ha caratteristica 0. Altrimenti, ha una caratteristica finita e $\operatorname{im}\phi \cong \mathbb{Z}/p\mathbb{Z}$ per qualche $p \geq 1$. Essendo $\mathbb{Z}$ un dominio ad ideali principali e K un campo, necessariamente la p è primo. □

Esercizio 1.11. Riesci a trovare un campo infinito ma di caratteristica $\neq 0$?

2 Polinomi e radici

Se R è un anello, indichiamo con $R[X]$ l'anello dei polinomi nell'indeterminata X, dove X è solo un mero simbolo. Indichiamo gli elementi di questo anello come somme formali

$$\sum_{k\in\mathbb{N}} a_k X^k$$

dove $a : \mathbb{N} \to R$ è una successione in cui solo un numero finito di termini a_k è diverso da zero. I polinomi $\sum_{k\in\mathbb{N}} a_k X^k$ in cui $a_k = 0$ per $k \geq 1$ sono identificati con $a_0 \in R$: quindi si potrebbe pensare R come sottoinsieme di $R[X]$.

Richiamiamo anche come sono definite la somma e il prodotto di polinomi di un qualsiasi anello $R[X]$:

$$\left(\sum_{k\in\mathbb{N}} a_k X^k\right) + \left(\sum_{k\in\mathbb{N}} b_k X^k\right) := \sum_{k\in\mathbb{N}} (a_k + b_k) X^k$$

$$\left(\sum_{k\in\mathbb{N}} a_k X^k\right)\left(\sum_{k\in\mathbb{N}} b_k X^k\right) := \sum_{k\in\mathbb{N}} \left(\sum_{h=0}^{k} a_h b_{k-h}\right) X^k$$

Il *grado* di un polinomio $p := \sum_{k\in\mathbb{N}} a_k X^k \in R[X]$ non nullo è il numero

$$\deg p := \max\{k \in \mathbb{N} \mid a_k \neq 0\}.$$

Il grado del polinomio nullo è definito come $-\infty$, anche se non è una convenzione universalmente accettata. È facile verificare che

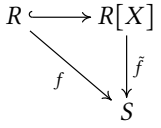
$$\deg(p + q) = \max\{\deg p, \deg q\}$$

e se R è un dominio di integrità allora anche

$$\deg(pq) = \deg p + \deg q.$$

Ora parliamo di anelli commutativi e di anelli di polinomi su anelli commutativi, visto che poi andremo piuttosto rapidamente verso i campi.

Proposizione 2.1. Siano R e S due anelli commutativi e $f : R \to S$ un omomorfismo. Allora per ogni $\alpha \in S$ esiste uno e un solo omomorfismo $\tilde{f} : R[X] \to S$ tale che



commuta e $\tilde{f}(X) = \alpha$.

Dimostrazione. Il diagramma commutativo già suggerisce come è fatto $\tilde{f}$:

$$\tilde{f}\left(\sum_{k\in\mathbb{N}} a_k X^k\right) := \sum_{k\in\mathbb{N}} f(a_k)\,\alpha^k$$

(In $\sum_{k\in\mathbb{N}} a_k X^k$ solo un numero finito di a_k è $\neq 0$, quindi $\sum_{k\in\mathbb{N}} f(a_k)\,\alpha^k$ è una somma certamente finita.) Questa funzione è un omomorfismo, vediamo.

$$\begin{aligned}
\tilde{f}\left(\sum_{k\in\mathbb{N}} a_k X^k + \sum_{k\in\mathbb{N}} b_k X^k\right) &= \tilde{f}\left(\sum_{k\in\mathbb{N}} (a_k + b_k) X^k\right) = \\
&= \sum_{k\in\mathbb{N}} f(a_k + b_k)\,\alpha^k = \\
&= \sum_{k\in\mathbb{N}} f(a_k)\,\alpha^k + \sum_{k\in\mathbb{N}} f(b_k)\,\alpha^k = \\
&= \tilde{f}\left(\sum_{k\in\mathbb{N}} a_k X^k\right) + \tilde{f}\left(\sum_{k\in\mathbb{N}} b_k X^k\right)
\end{aligned}$$

Per vedere che preserva i prodotti, abbiamo bisogno dell'assunzione della commutatività.

$$\begin{aligned}
\tilde{f}\left(\left(\sum_{k\in\mathbb{N}} a_k X^k\right)\left(\sum_{k\in\mathbb{N}} b_k X^k\right)\right) &= \tilde{f}\left(\sum_{k\in\mathbb{N}}\left(\sum_{h=0}^{k} a_h b_{k-h}\right) X^k\right) = \\
&= \sum_{k\in\mathbb{N}} f\left(\sum_{h=0}^{k} a_h b_{k-h}\right)\alpha^k = \\
&= \sum_{k\in\mathbb{N}}\sum_{h=0}^{k} f(a_h)\,f(b_{k-h})\,\alpha^k = \\
&= \sum_{k\in\mathbb{N}}\sum_{h=0}^{k} f(a_h)\,\alpha^j f(b_{k-h})\,\alpha^{k-h} = \\
&= \left(\sum_{k\in\mathbb{N}} f(a_k)\,\alpha^k\right)\left(\sum_{k\in\mathbb{N}} f(b_k)\,\alpha^k\right) = \\
&= \tilde{f}\left(\sum_{k\in\mathbb{N}} a_k X^k\right)\tilde{f}\left(\sum_{k\in\mathbb{N}} b_k X^k\right)
\end{aligned}$$

Infine, il fatto che preserva l'identità è immediato. □

Definizione 2.2 (Valutazione di polinomi)**.** Sia R un anello commutativo e $\alpha \in R$. Chiamiamo *valutazione* in α l'omomorfismo $R[X] \to R$ di anelli indotto dall'identità $\mathrm{id}_R : R \to R$ nel senso della Proposizione 2.1. In tal caso, scriviamo $p(\alpha)$ l'immagine di $p \in R[X]$ sotto l'omomorfismo di valutazione in α: cioè se

$$p = \sum_{j\in\mathbb{N}} a_j X^j,$$

allora

$$p(\alpha) = \sum_{j \in \mathbb{N}} a_j \alpha^j.$$

Corollario 2.3. Siano R e S due anelli commutativi e $f : R \to S$ un omomorfismo. Allora esiste uno e un solo omomorfismo $f_* : R[X] \to S[X]$ tale che commuta

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \downarrow & & \downarrow \\ R[X] & \xrightarrow[f_*]{} & S[X] \end{array}$$

e $f_*(X) = X$. Esplicitamente, se $f : R \to S$ è un omomorfismo di anelli, allora

$$f_*\left(\sum_{j \in \mathbb{N}} a_j X^j\right) = \sum_{j \in \mathbb{N}} f\left(a_j\right) X^j.$$

Inoltre valgono le proprietà di funtorialità:

1. $\left(\mathrm{id}_R\right)_* = \mathrm{id}_{R[X]}$ per ogni anello R.
2. Se abbiamo due omomorfismi di anelli $R \xrightarrow{f} S \xrightarrow{g} T$, allora $(g \circ f)_* = g_* \circ f_*$.

Dimostrazione. Si tratta sostanzialmente di fare solo dei conti. Esercizio. □

È bene prendere familiarità con questo Corollario perché è uno degli strumenti essenziali nelle nozioni che verranno.

Corollario 2.4. Siano R e S anelli commutativi, $f : R \to S$ un omomorfismo e $\alpha \in S$. Allora l'omomorfismo $\tilde{f} : R[X] \to S$ della Proposizione 2.1 è

$$R[X] \to S, \ p \mapsto f_*(p)(\alpha).$$

Da un certo punto in poi parleremo di campi, quindi vediamo subito come si applicano queste cose. Abbiamo già visto che tutti che gli omomorfismi di campi sono iniettivi: quindi, se abbiamo un omomorfismo di campi $i : K \to L$, allora l'immagine di K in L è una copia di K. In questo senso, diciamo che K è contenuto in L anche se non è letteralmente un sottoinsieme di L. Confondere K con la sua immagine dentro L è un abuso di cui ci gioveremo molto spesso, cercando di essere il più chiari e trasparenti possibile. Inoltre, se $r \in K$, allora indichiamo con r anche l'elemento $i(r)$ di L che corrisponde a r. L'abuso si propaga anche sui polinomi: un elemento p di $K[X]$ viene identificato all'elemento $i_*(p)$ di $L[X]$, e quindi per evitare troppe parentesi spesso ci riferiremo a quest'ultimo come "al polinomio p visto come elemento di $L[X]$" o in modi simili.

Definizione 2.5 (Radice di un polinomio)**.** Sia $i : K \to L$ un omomorfismo di campi, $\alpha \in L$ e $p \in K[X]$. Diciamo che α è *radice* di p in L qualora $i_*(p)(\alpha) = 0$. Cioè, impiegando l'abuso di linguaggio appena spiegato, la radice di un polinomio $p \in K[X]$ in L è un $\alpha \in L$ tale che vedendo p come un elemento di $L[X]$ si ha che sia annulla valutato in α.

Esempio 2.6. Consideriamo il polinomio $X^2 + 1 \in \mathbb{R}[X]$: non ha radici in $\mathbb{R}$, ma li ha in $\mathbb{C}$. Se consideriamo l'inclusione $i : \mathbb{R} \hookrightarrow \mathbb{C}$, allora abbiamo

$$i_*\left(X^2 + 1\right) = X^2 + 1.$$

Le radici complesse sono due: i e $-i$.

Esempio 2.7. La "definizione da algebrista" di $\mathbb{C}$ è un'altra però:

$$\mathbb{C} := \frac{\mathbb{R}[X]}{(X^2+1)}$$

in cui

$$i := X + \left(X^2+1\right).$$

Vediamo come si inquadrano le cose nella forma delle definizione data. Ora l'omomorfismo

$$i : \mathbb{R} \to \mathbb{C},\ i(r) := r + \left(X^2+1\right)$$

induce l'omomorfismo $i_* : \mathbb{R}[X] \to \mathbb{C}[X]$. Usiamo X^2+1 per indicare l'immagine di X^2+1 sotto i_*, identificando i coefficienti a_j con le rispettive immagini $a_j + (X^2+1)$. Verifichiamo che i è radice di X^2+1:

$$\left(X + \left(X^2+1\right)\right)^2 + 1 = X^2 + 1 + \left(X^2+1\right) = \underbrace{0 + \left(X^2+1\right)}_{\text{lo zero di } \mathbb{C}}.$$

Definizione 2.8 (Elementi algebrici e trascendenti)**.** Sia $i : K \to L$ un'estensione e $\alpha \in L$. Diciamo che α è *algebrico* qualora esista qualche $p \in K[X]$ non nullo tale che $i_*(p)(\alpha) = 0$. Equivalentemente, α è algebrico qualora l'omomorfismo

$$K[X] \to L,\ p \mapsto i_*(p)(\alpha)$$

non è iniettivo. Invece diremo che α è *trascendente* quando α non è trascendente.

Proposizione 2.9. Sia $i : K \to L$ un'estensione e $\alpha \in L$ algebrico. Allora esiste uno e un solo $m \in K[X]$ monico e irriducibile tale che sia un generatore nucleo dell'omomorfismo

$$K[X] \to L,\ p \mapsto i_*(p)(\alpha).$$

Dimostrazione. Poiché K è un campo, $K[X]$ è un dominio ad ideali principali. Quindi il nucleo dell'omomorfismo in questione è generato da un certo $m \in K[X]$. Possiamo assumere che sia monico, essendo K un campo. Inoltre l'omomorfismo di valutazione in α induce un omomorfismo iniettivo

$$\frac{K[X]}{\langle m \rangle} \to L$$

verso un altro campo: m è pure irriducibile perché $\frac{K[X]}{\langle m \rangle}$ è un campo e $K[X]$ è un dominio ad ideali principali. Infine se $m_1, m_2 \in K[X]$ sono generatori monici del nucleo di questo omomorfismo, allora $m_1 = am_2$ per qualche $a \in K$ invertibile. Essendo entrambi monici, concludiamo che $a = 1$. □

Definizione 2.10 (Polinomio minimo)**.** Sia $i : K \to L$ un'estensione di campi e $\alpha \in L$ algebrico. Il *polinomio minimo* di α è il generatore monico del nucleo dell'omomorfismo

$$K[X] \to L,\ p \mapsto i_*(p)(\alpha).$$

Proposizione 2.11. Sia $i : K \to L$ un omomorfismo di campi, $\alpha \in L$ e $m \in K[X]$ non nullo e monico. Allora sono equivalenti:

1. m è il polinomio minimo di α su K.
2. m è irriducibile su K e $i_*(m)(\alpha) = 0$.

Dimostrazione. (1 ⇒ 2) Da definizione, m è il generatore monico dell'omomorfismo

$$K[X] \to L,\ p \mapsto i_*(p)(\alpha).$$

Quindi m come polinomio in $L[X]$ si annulla in α. Inoltre, essendo K e L campi, pure $\frac{K[X]}{\langle m \rangle}$ lo è: allora m è irriducibile perché $K[X]$ dominio a ideali principali.
(2 ⇒ 1) Scriviamo m' il generatore monico del nucleo dell'omomorfismo

$$K[X] \to L,\ p \mapsto i_*(p)(\alpha).$$

Quindi $m \in \langle m' \rangle$. Ma, essendo m irriducibile, abbiamo $m = am'$ con $a \in L$ invertibile. Trattandosi di polinomi monici, $a = 1$ necessariamente. □

La ricerca del polinomio minimo è quindi ridotta ad una questione di irriducibilità: il lettore è invitato a ripassare i criteri per l'irriducibilità di polinomi fatti ad Alegbra 1. Facciamo degli esempi.

Esempio 2.12. Sia il solito omomorfismo $\mathbb{R} \hookrightarrow \mathbb{C}$. Il polinomio minimo di $i \in \mathbb{C}$ è $X^2 + 1 \in \mathbb{R}[X]$ perché si annulla in i ed è irriducibile in $\mathbb{R}[X]$ (è un polinomio di grado due senza zeri nel campo $\mathbb{R}$). Allo stesso modo, si verifica che $-i$ ha lo stesso polinomio minimo.

Esempio 2.13. Consideriamo l'omomorfismo di inclusione $\mathbb{Q} \hookrightarrow \mathbb{R}$ e $\alpha := \sqrt{\sqrt[3]{4} - 1} \in \mathbb{R}$. Per trovare un polinomio in $\mathbb{Q}[X]$ che sia il polinomio minimo di α a volte serve un po' di inventiva. Ad esempio:

$$\begin{aligned}
\alpha &= \sqrt{\sqrt[3]{4} - 1} \\
\alpha^2 + 1 &= \sqrt[3]{4} \\
\alpha^6 + 3\alpha^4 + 3\alpha^2 + 1 &= 4 \\
\alpha^6 + 3\alpha^4 + 3\alpha^2 - 3 &= 0.
\end{aligned}$$

Quindi un candidato a polinomio minimo è $X^6 + 3X^4 + 3X^2 - 3$. Per vedere se è irriducibile possiamo usare il *Criterio di Eisenstein*: 3 non divide il coefficiente direttivo, divide tutti gli altri e 3^2 non divide il termine noto.

Esempio 2.14. Sia $i : K \to L$ un omomorfismo di campi e $\alpha \in L$. Supponiamo che anche $\alpha \in K$. Tecnicamente parlando questo è un piccolo abuso: quello che vogliamo dire è che α appartiene all'immagine di K in L tramite i, ovvero $\alpha = i(\alpha')$ per un unico $\alpha' \in K$. Calcoliamo il polinomio minimo di α. Consideriamo l'omomorfismo

$$K[X] \to L,\ p \mapsto i_*(p)(\alpha)$$

e calcoliamone il nucleo. Se $p \in K[X]$ è tale che

$$0 = i_*(p)(\alpha) = i_*(p)\left(i(\alpha')\right) = i\left(p(\alpha')\right)$$

allora per l'iniettività di i si ha

$$p(\alpha') = 0.$$

Concludiamo quindi che il polinomio minimo di $\alpha = i(\alpha')$ è $X - \alpha'$. Con un abuso di notazione, possiamo dire che il polinomio minimo di $\alpha \in K$ è $X - \alpha$. È un abuso che nemmeno si nota nel caso in cui l'omomorfismo è una semplice inclusione insiemistica.

Esempio 2.15. Consideriamo l'omomorfismo di inclusione $\mathbb{R} \hookrightarrow \mathbb{C}$. Abbiamo da poco visto che il polinomio minimo di $\alpha \in \mathbb{R}$ è di primo grado, $X - \alpha$. Sia quindi $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Chiaramente il polinomio minimo di α deve essere di grado ≥ 2. Costruiremo il polinomio minimo di α. Indicando con $\overline{\alpha}$ il coniugato di α, si verifica immediatamente che $\alpha + \overline{\alpha}$ e $\alpha\overline{\alpha}$ sono reali. Il polinomio

$$X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}$$

è a coefficienti reali ed ha come radici α e $\overline{\alpha}$. Trattandosi di un polinomio di grado 2 che non ha zeri reali, il polinomio è anche irriducibile in $\mathbb{R}[X]$.

Sotto questo punto di vista, lavorare con gli omomorfismi $\mathbb{R} \hookrightarrow \mathbb{C}$ è poco interessante: i polinomi minimi sono di grado 1 oppure di grado 2. Un po' più bizzarri sono gli omomorfismi di campo che partono da $\mathbb{Q}$. Vediamo qualche esempio.

Esempio 2.16 (Radici dell'unità)**.** Il polinomio $X^n - 1$ ha n radici complesse, che possiamo scrivere in forma esponenziale

$$\xi_k := e^{i\frac{2\pi k}{n}} \quad \text{per } k \in \{0, \dots, n-1\}$$

di cui la prima è sicuramente è reale. Se n è dispari, 1 è l'unica radice reale. Possiamo fattorizzare questo polinomio come

$$X^n - 1 = (X-1)\left(X^{n-1} + \dots + X + 1\right)$$

e quindi le radici complesse sono di $X^{n-1} + \dots + X + 1$. Ricordiamo che

Se $p \geq 3$ è primo, allora $X^{p-1} + \dots + X + 1$ è irriducibile in $\mathbb{Q}[X]$.

Quindi se consideriamo l'estensione $\mathbb{Q} \hookrightarrow \mathbb{C}$ data dalla composizione delle inclusioni $\mathbb{Q} \hookrightarrow \mathbb{R}$ e $\mathbb{R} \hookrightarrow \mathbb{C}$, e se $p \geq 3$, allora le radici complesse $\xi_1, \dots, \xi_{p-1}$ hanno tutte lo stesso polinomio minimo in $\mathbb{Q}[X]$, cioè $X^{p-1} + \dots + X + 1$. Osserviamo invece se l'omomorfismo scelto è $\mathbb{R} \hookrightarrow \mathbb{C}$, allora $X^{p-1} + \dots + X + 1$ come polinomio reale non è più irriducibile. Infatti, se α è una delle radici non reali, abbiamo visto che il polinomio minimo di α in $\mathbb{R}[X]$ è

$$X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}.$$

e divide $X^{p-1} + \dots + X + 1$.

3 Estensioni di campi

Abbiamo visto (Proposizione 1.6) che gli omomorfismi di campi sono tutti iniettivi. Presi due campi K e L, se esiste un omomorfismo $K \to L$, allora L contiene al suo interno una copia isomorfa a K. Quindi, anche se K non è propriamente un sottoinsieme di L, possiamo dire che K è contenuto in L oppure che L contiene K. In ogni caso, si è scelta una nuova parola per indicare questa inclusione.

Definizione 3.1. Un'*estensione* (di campi) è un omomorfismo di campi.

Per abuso di notazione, spesso un'estensione di campi $i : K \to L$ viene indicata semplicemente con $K \subseteq L$, come in [Alu], anche quando non è proprio un'inclusione insiemistica. Esistono altre notazioni: per esempio in [Mil] si usa L/K mentre in [Lei] viene impiegato $L : K$. Esiste anche $K \hookrightarrow L$ una combinazione di $\subset$ e $\to$.

Abbiamo già visto alcuni esempi banali di estensioni di campi. Un tipo di estensioni è ispirato all'Esempio 2.7.

Costruzione 3.2. Se K è un campo, allora $K[X]$ è un dominio ad ideali principali. Se oltre a K abbiamo un $p \in K[X]$ non nullo e irriducibile, allora $\frac{K[X]}{\langle p \rangle}$ è un campo. Un'estensione molto naturale quindi è

$$K \to \frac{K[X]}{\langle p \rangle}, \; r \mapsto r + \langle p \rangle .$$

Questa costruzione è molto interessante.

Proposizione 3.3. Se K è un campo e $p \in K[X]$ è non nullo e irriducibile, allora sotto l'estensione

$$K \to \frac{K[X]}{\langle p \rangle}, \; r \mapsto r + \langle p \rangle$$

p visto come elemento di $\frac{K[X]}{\langle p \rangle}$ ha almeno uno zero.

Si pensi per esempio a $\mathbb{R} \hookrightarrow \mathbb{C}$ con $X^2 + 1$: in $\mathbb{R}$ non ci sono radici, ma sicuramente ce n'è qualcuna in $\mathbb{C} = \frac{\mathbb{R}[X]}{\langle X^2+1 \rangle}$. La dimostrazione non è niente di diverso dal conto fatto nell'Esempio 2.7.

Costruzione 3.4. Sia $i : K \to L$ una estensione di campi e $\alpha \in L$ con polinomio minimo $m \in K[X]$. Abbiamo quindi un'estensione

$$K \to \frac{K[X]}{\langle m \rangle}$$

come nell'esempio precedente.

Un altro modo di avere estensioni di campi a partire da un'estensione $i : K \to L$ e da $\alpha \in L$ è il seguente.

Costruzione 3.5 (Estensioni generate)**.** Sia $i : K \to L$ un'estensione di campi e S un sottoinsieme qualunque di L. Definiamo $K(S)$ come il più piccolo sottocampo di L che contiene sia K che S. Un piccolo abuso qui: tecnicamente $K(\alpha)$ è il più piccolo sottocampo di L contenente sia l'immagine di K tramite i che S. Nel caso in cui S sia un singoletto $\{\alpha\}$, allora scriviamo $K(\alpha)$ al posto di $K(\{\alpha\})$. Quindi un'ovvia estensione è data da $i : K \to L$ stessa:

$$K \to K(S), \; r \mapsto i(r).$$

Proposizione 3.6. Sia $i : K \to E := K(U)$ un estensione generata da un $U \subseteq E$ e $j : K \to L$ un'estensione di campi. Mostrare che se $f(a) = g(a)$ per ogni $a \in K \cup U$ [tecnicamente parlando, $a \in iK \cup U$], allora $f = g$.

Dimostrazione. Prendiamo in esame l'insieme

$$A := \{a \in E \mid f(a) = g(a)\}$$

perché se mostriamo che $A = E$, allora abbiamo concluso. Per ipotesi, A contiene K [più precisamente iK] e U. Inoltre A è un sottocampo di E e quindi da definizione di estensione generata abbiamo che $E \subseteq A$. Ma è anche $A \subseteq E$ visto come è definito A. □

Una classe importante di estensioni, ovviamente, sono quelle in cui S è un insieme finito. Hanno un un nome.

Definizione 3.7 (Estensioni finitamente generate)**.** Un'estensione $i : K \to L$ è detta *finitamente generata*, qualora esiste $S \subseteq L$ finita tale che $L = K(S)$. Nel caso in cui $S = \{\alpha\}$, l'estensione $K \to L = K(\alpha)$ è detta *semplice*.

Un esempio di estensione semplice è già stato visto.

Esempio 3.8. Sia K un campo e $m \in K[X]$ irriducibile. L'estensione $K \hookrightarrow \frac{K[X]}{\langle m \rangle}$ che abbiamo già menzionato è generata. Si vede abbastanza rapidamente. Indichiamo con $K\left(X + \langle m \rangle\right)$ il più piccolo sottocampo di $\frac{K[X]}{\langle m \rangle}$ contente K (propriamente l'immagine di i) e $X + \langle m \rangle$. Ora, gli elementi di $\frac{K[X]}{\langle m \rangle}$ sono della forma $p + \langle m \rangle$ con $p \in K[X]$, cioè combinazioni lineari di $X^k + \langle m \rangle$: quindi possiamo concludere che

$$\frac{K[X]}{\langle m \rangle} = K\left(X + \langle m \rangle\right).$$

In questo senso, l'estensione $K \hookrightarrow \frac{K[X]}{\langle m \rangle}$ è semplice.

Esercizio 3.9. Considerando l'inclusione $\mathbb{Q} \subseteq \mathbb{C}$, sai dire se $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}\right)$?

Una cosa che si fa spesso sia nelle considerazioni pratiche che negli esercizi è quello di spezzare un estensione fintamente generata in estensioni intermedie.

Proposizione 3.10. Sia $i : K \to L = K(S \cup T)$ un'estensione generata dall'unione di due insiemi. Allora si può fattorizzare come segue:

$$K \xrightarrow{\tilde{i}} K(S) \hookrightarrow K(S \cup T).$$

con $\tilde{i}(r) = i(r)$.

Dimostrazione. [Facile. Ma da presentare meglio.] □

Proposizione 3.11. Sia $i : K \to L$ un'estensione e $\alpha_1, \ldots, \alpha_n \in L$, con $n \geq 2$. Allora

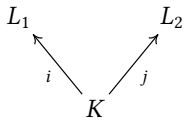
$$K\left(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n\right) = K\left(\alpha_1, \ldots, \alpha_{n-1}\right)\left(\alpha_n\right).$$

Dimostrazione. Esercizio. □

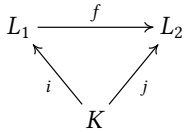
Cioè le estensioni finitamente generate possono essere introdotte iterativamente a partire dalla costruzione di estensione semplice.

Scopriremo molto presto l'importanza di questa costruzione, anche perché sotto certe ipotesi le estensioni generate hanno una descrizione esplicita molti semplice e maneggevole.

Definizione 3.12 (Morfismi di estensioni)**.** Prendiamo sue estensioni di campo



Una morfismo di estensioni da i a j è un qualsiasi omomorfismo $f : L_1 \to L_2$ per cui commuta

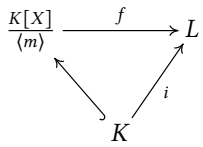


Per dire più concretamente come sono fatte un certo tipo di estensioni semplici serve un po' di lavoro preliminare.

Proposizione 3.13. Sia $i : K \to L$ una estensione e $\alpha \in L$ con polinomio minimo $m \in K[X]$. In precedenza abbiamo visto l'estensione di campi

$$K \hookrightarrow \frac{K[X]}{\langle m \rangle}, \; r \mapsto r + \langle m \rangle .$$

Allora esiste una e una sola omomorfismo $f : \frac{K[X]}{\langle m \rangle} \to L$ tale che



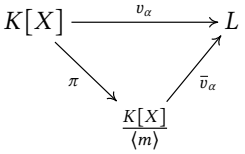
commuta e $f(X + \langle m \rangle) = \alpha$. In particolare, f ha immagine $K(\alpha)$ e quindi

$$\frac{K[X]}{\langle m \rangle} \cong K(\alpha).$$

Dimostrazione. Grazie al Primo Teorema di Isomorfismo, l'omomorfismo di valutazione in α

$$v_\alpha : K[X] \to L, \; p \mapsto i_*(p)(\alpha)$$

si fattorizza mediante la proiezione al quoziente in questo modo:



Le estensioni di campi dell'enunciato si ottengono componendo v_α e π con l'inclusione $K \hookrightarrow K[X]$: la f dell'enunciato è proprio quella che abbiamo indicato qui con $\overline{v}_\alpha$. Con questa informazione è facile verificare che che $f = \overline{v}_\alpha$ è un morfismo di estensioni e che manda $X + \langle m \rangle$ in α.
Rimane da provare l'isomorfismo che coinvolge l'estensione generata da α, e per farlo proveremo che $\operatorname{im} f = K(\alpha)$. L'immagine di $f : \frac{K[X]}{\langle m \rangle} \to L$ è un sottocampo di L che contiene K e $\alpha \in L$: quindi $K(\alpha) \subseteq \operatorname{im} f$, da definizione di estensione generata. D'altra parte, le immagini di f sono polinomi di grado $< \deg m$ di $K[X]$ valutati in α: quindi è anche vero che $\operatorname{im} f \subseteq K(\alpha)$. □

Richiamo 3.14. Sia K un campo e $p \in K[X]$ non nullo. $K[X]$ è un dominio euclideo e questo significa che gli elementi di $\frac{K[X]}{\langle p \rangle}$ sono precisamente le classi laterali

$$g + \langle p \rangle \quad \text{con } g \in K[X] \text{ e } \deg g \leq \deg p - 1.$$

Ecco quindi come sono fatte concretamente le estensioni semplici $K \to K(\alpha)$ quando α è algebrico.

Corollario 3.15. Sia $i : K \to L$ una estensione e $\alpha \in L$ con polinomio minimo $m \in K[X]$. Allora

$$K(\alpha) = \{ p(\alpha) \mid p \in K[X], \deg p \leq \deg m - 1 \} .$$

Rimaniamo ancora un po' su quanto detto nella Proposizione precedente.

Corollario 3.16. Sia $i : K \to L$ una estensione e $m \in K[X]$ monico e irriducibile. Considera anche l'usuale estensione $K \hookrightarrow \frac{K[X]}{\langle m \rangle}$, $r \mapsto r + \langle m \rangle$. Allora esiste una biezione

$$\{\alpha \in L \mid \alpha \text{ radice di } m\} \leftrightarrow \left\{\text{omomorfismi di estensioni } \frac{K[X]}{\langle m \rangle} \to L\right\}.$$

Cioè: esistono tanti modi di incorporare $\frac{K[X]}{\langle m \rangle}$ all'interno di L quante sono le radici di p in L.

Esempio 3.17. Consideriamo l'inclusione $\mathbb{Q} \hookrightarrow \mathbb{C}$ e $X^2 + 1 \in \mathbb{Q}[X]$ che è un polinomio monico e irriducibile. Le radici sono due, i e $-i$, e quindi il quoziente $\frac{\mathbb{Q}[X]}{\langle X^2+1 \rangle}$ ha le seguenti copie all'interno di $\mathbb{C}$: $\mathbb{Q}(i)$ e $\mathbb{Q}(-i)$. Osserviamo però che $\mathbb{Q}(i)$ e $\mathbb{Q}(-i)$ sono uguali (esercizio), ma questo non conta perché noi stiamo considerando il numero di estensioni $\frac{\mathbb{Q}[X]}{\langle X^2+1 \rangle} \to \mathbb{C}$.

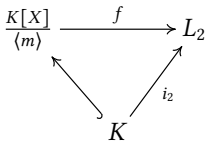
Quindi quante estensioni $K(\alpha) \to L$ ci sono? Basta rimaneggiare sfruttare l'isomorfismo che abbiamo appena visto:

Corollario 3.18. Sia $i_1 : K \to L_1$ un'estensione e $\alpha \in L_1$ con polinomio minimo $m \in K[X]$. Sia $i_2 : K \to L_2$ un'estensione. Se con $K(\alpha)$ indichiamo il più piccolo sottocampo di L_1 contenente $i_1 K$ e α, allora esiste una biezione

$$\{\text{radici di } m \text{ in } L_2\} \leftrightarrow \{\text{omomorfismi di estensioni } K(\alpha) \to L_2\}.$$

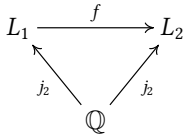
Questo Corollario permette di contare il numero di morfismi di estensioni da un'estensione semplice $K \to K(\alpha)$ con α algebrico. Ritorneremo più in là su questo conteggio dal Lemma 10.14 a seguire perché è centrale per la Teoria di Galois.

Dimostrazione. Per la Proposizione precedente, ogni $\beta \in L_2$ che soddisfa $i_{2*}(m)(\beta) = 0$ induce uno e un solo morfismo di estensioni



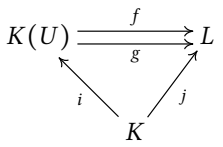
che manda $X + \langle m \rangle$ in β. Sempre per la stessa Proposizione, si $K(\alpha) \cong \frac{K[X]}{\langle m \rangle}$. □

Esercizio 3.19. Siano L_1 e L_2 due campi di caratteristica 0 e $f : L_1 \to L_2$ un omomorfismo di campi. Siano $j_1 : \mathbb{Q} \to L_1$ e $j_2 : \mathbb{Q} \to L_2$ indotte dagli omomorfismi $\mathbb{Z} \to L_1$ e $\mathbb{Z} \to L_2$ come nel Lemma 1.8. Mostrare che



commuta, cioè f è un morfismo di estensioni da j_1 a j_2.

Esercizio 3.20. Sia $i : K \to E := K(U)$ un estensione generata da un $U \subseteq E$ e $j : K \to L$ un'estensione di campi. Se abbiamo due morfismi di estensioni



Mostrare che se $f(a) = g(a)$ per ogni $a \in U$, allora $f = g$.

4 Grado di estensioni

Presa un'estensione $i : K \to L$, possiamo vedere L come uno spazio vettoriale su K. L'operazione interna è l'operazione di addizione di L, mentre la moltiplicazione per scalare deve essere introdotta:

$$\begin{aligned} K \times L &\to L \\ (k, l) &\mapsto i(k)l \end{aligned}$$

Con un abuso, possiamo identificare K con la sua immagine sotto i in L e quindi scrivere "kl" al posto di "$i(k)l$", rendendo così la moltiplicazione per scalare un affare interno a L stesso. È un abuso di notazione così radicato e comodo che anche noi faremo lo stesso facendo attenzione e cercando di essere il più chiari possibile.

Definizione 4.1. Il *grado* di un'estensione di campi $i : K \to L$ è la dimensione L come spazio vettoriale su K e si indica con $[L : K]$. L'estensione si dice *finita* qualora la dimensione di L è finita.

Quindi se $i : K \to L$ è un'estensione di grado $n < \infty$, allora esistono degli elementi $\alpha_1, \dots, \alpha_n \in L$ che formano una base di L e quindi L come campo vettoriale è isomorfo a K^n. Quando si scrive $[L : K]$ senza che appaia alcun riferimento a i è proprio per questa ragione: una volta fissati K e L, tutte le estensioni $K \to L$ hanno lo stesso grado.

Proposizione 4.2. Siano $F \subseteq K \subseteq L$ sue estensioni consecutive.

1. Se $F \subseteq L$ è un'estensione finita, allora anche $F \subseteq K$ e $K \subseteq L$ lo sono
2. Se $\{\alpha_1, \dots, \alpha_m\}$ è una base di K come spazio vettoriale su F e $\{\beta_1, \dots, \beta_n\}$ è una base di L come spazio vettoriale su K, allora

   $$\{\alpha_i \beta_j \mid i = 1, \dots, m, j = 1, \dots, n\}$$

   è una base di L come spazio vettoriale su F. In particolare, se $F \subseteq K$ e $K \subseteq L$ sono entrambe finite, allora pure $F \subseteq L$ lo è. Inoltre

   $$[L : F] = [L : K][K : F]. \tag{4.1}$$

$$\underbrace{F \xrightarrow{[K:F]} K \xrightarrow{[L:K]} L}_{[L:K]}$$

La formula 4.1 ricorda una proprietà dell'indice dei sottogruppi in un gruppo: vedremo in seguito che è una importante coincidenza.

Dimostrazione. Sia $F \subseteq L$ un'estensione finita. L'estensione $F \subseteq K$ è ovviamente finita perché K è un sottospazio vettoriale di L. Inoltre L come spazio vettoriale su F possiede una base $\{\alpha_1, \dots, \alpha_n\} \subseteq L$ e quindi gli elementi di L possono essere

anche ottenute come combinazioni lineari con coefficienti in K. Pertanto anche l'estensione $K \subseteq L$ è finita.
Viceversa [forse è meglio riscriverla...] siano $[K : F] = m$ e $[L : K] = n$, cioè $K \cong F^m$ come spazi vettoriali su F e $L \cong K^n$ come spazi vettoriali su K e quindi anche su F. Allora

$$L \cong (F^m)^n \cong F^{mn}$$

come spazi vettoriali su F. Concludiamo quindi che $[L : F] = mn$. □

[I morfismi di estensioni sono applicazioni lineari. Parlare di questo e delle conseguenze sugli endomorfismi di estensioni finite: cioè sono automorfismi.]

Vediamo ora il grado delle estensioni che abbiamo fino ad ora introdotto.

Esempio 4.3. Sia K un campo e $p \in K[X]$ non nullo. Allora $\frac{K[X]}{\langle p \rangle}$ è uno spazio vettoriale su K di grado $\deg p$ perché una sua base è

$$\left\{1 + \langle p \rangle, X + \langle p \rangle, \dots, X^{\deg p - 1} + \langle p \rangle\right\}.$$

Questo è interessante perché se p è irriducibile, allora abbiamo il grado dell'estensione di campi $K \to \frac{K[X]}{\langle p \rangle}$, $r \mapsto r + \langle p \rangle$. Ecco come prosegue la cosa grazie alla Proposizione 3.13.

Proposizione 4.4. Sia $i : K \to L$ un'estensione e $\alpha \in L$ con polinomio minimo $m \in K[X]$. Allora il grado dell'inclusione $K \hookrightarrow K(\alpha)$ è uguale a $\deg m$.

Dimostrazione. In realtà il Corollario 3.15 ha già fatto tutto il lavoro: una base di $K(\alpha)$ come spazio vettoriale su K è $\left\{1, \alpha, \dots, \alpha^{\deg m - 1}\right\}$. □

Abbiamo appena compreso che il calcolo del grado di una estensione $K \hookrightarrow K(\alpha)$ con α algebrico passa per il calcolo del polinomio minimo di α. Quindi il lettore deve capire che è necessario una certa familiarità con i criteri di irriducibilità di polinomi.

Non è difficile ora formulare delle condizioni equivalenti all'essere elementi algebrici in termini del grado di un'opportuna estensione.

Proposizione 4.5. Sia $i : K \to L$ un'estensione e $\alpha \in L$. Allora sono equivalenti:

1. α è algebrico su K.
2. $K \hookrightarrow K(\alpha)$ è finita. In questo caso $[K(\alpha) : K]$ è il grado del polinomio minimo di α su $K[X]$.

Dimostrazione. Se α è algebrico, allora ammette un polinomio minimo $m \in K[X]$ e quindi siamo nelle ipotesi della Proposizione precedente. Il viceversa richiede un po' di Algebra Lineare. Se $[K(\alpha) : K] = n < \infty$, allora sicuramente gli $n + 1$ elementi

$$1, \alpha, \dots, \alpha^{n-1}, \alpha^n$$

sono linearmente dipendenti. Cioè esistono $a_0, \dots, a_n \in K$ non tutti nulli per cui

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0.$$

Abbiamo quindi trovato un polinomio non nullo che sia annulla in α. □

Definizione 4.6. Un'estensione $K \subseteq L$ è detta *algebrica* quando ogni elemento di L è algebrico su K.

Proposizione 4.7. Sia $K \subseteq L$ un'estensione. Allora sono equivalenti:

1. $K \subseteq L$ è finita;
2. $K \subseteq L$ è algebrica e finitamente generata;
3. Esistono $\alpha_1, \dots, \alpha_n \in L$ algebrici su K tali che $L = K(\alpha_1, \dots, \alpha_n)$.

Dimostrazione. (1 $\Rightarrow$ 2) Sia $\alpha \in L$. Allora $[K(\alpha) : K] \leq [L : K(\alpha)][K(\alpha) : K] = [L : K] < \infty$. Ora, poiché $[L : K] = n < \infty$, allora L come spazio vettoriale su K è generato da n elementi linearmente indipendenti $\alpha_1, \dots, \alpha_n \in L$. Pertanto $L = K(\alpha_1, \dots, \alpha_n)$ immediatamente dalla definizione di estensione generata.
(2 $\Rightarrow$ 3) Ovvia.
(3 $\Rightarrow$ 1) Se α_i è algebrico su K, allora α_i lo è anche su $K_i := K(\alpha_1, \dots, \alpha_{i-1})$. Quindi per ogni $i = 1, \dots, n$ si ha

$$[L : K] = \prod_{i=1}^{n} [K_{i+1} : K_i] < \infty. \qquad \square$$

[Come cambia il polinomio minimo su al variare di F in $K \subseteq F \subseteq L$?]

Proposizione 4.8. Siano $F \subseteq K \subseteq L$ estensioni. Allora $F \subseteq L$ è algebrica se e solo se $F \subseteq K$ e $K \subseteq L$ lo sono.

Dimostrazione. Una implicazione dovrebbe essere semplice a questo punto. Viceversa, siano $F \subseteq K$ e $K \subseteq L$ algebriche e mostriamo che $[F(\alpha) : F] < \infty$ per ogni $\alpha \in L$. Poiché $K \subseteq L$ è algebrica esiste un $p \in K[X]$ non nullo che abbia α come radice: indichiamo con $a_0, \dots, a_n \in K$ i coefficienti del polinomio. Quindi α è algebrico su $F(a_0, \dots, a_n)$. Per l'implicazione 3 $\Rightarrow$ 1 della Proposizione precedente, si ha $F \subseteq F(a_0, \dots, a_n)$ è finita. Anche $F(a_0, \dots, a_n) \subseteq F(a_0, \dots, a_n)(\alpha) = F(a_0, \dots, a_n, \alpha)$ è finita. Componendo le due estensioni finite, si ottiene l'estensione finita $F \subseteq F(a_0, \dots, a_n, \alpha)$. Possiamo a questo punto scrivere

$$\underbrace{[F(a_0, \dots, a_n, \alpha) : F]}_{<\infty} = [F(a_0, \dots, a_n, \alpha) : F(\alpha)][F(\alpha) : F]$$

da cui si ha che $[F(\alpha) : F] < \infty$. $\square$

5 Esercizi 1

Un classico esercizio è quello di calcolare il grado di estensioni finitamente generate, cosa che spesso passa per la ricerca di polinomi minimi (quindi criteri di irriducibilità).

Esercizio 5.1. 1. Mostrare che $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.
2. Mostrare che $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
3. Mostrare che $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
4. Determinare il polinomio minimo di $\sqrt{2} + \sqrt{3}$ in $\mathbb{Q}[X]$.

Svolgimento. 1. Possiamo considerare le seguenti estensioni consecutive

$$\mathbb{Q} \hookrightarrow \mathbb{Q}\left(\sqrt{2}\right) \hookrightarrow \mathbb{Q}\left(\sqrt{2}\right)(i) = \mathbb{Q}\left(\sqrt{2}, i\right)$$

ed usare la Proposizione 4.4 per determinare il grado di ciascuna di si queste. Un polinomio razionale irriducibile e monico che ha come radice $\sqrt{2}$ è

$X^2 - 2$: ecco il polinomio minimo di $\sqrt{2}$. Cerchiamo ora un $p \in \mathbb{Q}\left(\sqrt{2}\right)[X]$ monico e irriducibile che abbia i come radice. Il polinomio $X^2 - 2 \in \mathbb{Q}[X]$ continua ad essere irriducibile pure in $\mathbb{Q}\left(\sqrt{2}\right)$: poiché $\sqrt{2}$ è algebrico su $\mathbb{Q}$, sappiamo che

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$$

e qui non si possono trovare le radici di $X^2 - 2$ visto come elemento di $\mathbb{Q}\left(\sqrt{2}\right)[X]$. Questo basta per l'irriducibilità, visto che si tratta di un polinomio di grado 2 e a coefficienti in un campo che non ha radici nello stesso campo. Quindi il grado delle estensioni è

$$\mathbb{Q} \xhookrightarrow{2} \mathbb{Q}\left(\sqrt{2}\right) \xhookrightarrow{2} \mathbb{Q}\left(\sqrt{2}\right)(i) = \mathbb{Q}\left(\sqrt{2}, i\right)$$

e l'estensione $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, i\right)$ è di grado 4. Il lettore potrebbe provare invece a considerare le estensioni

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(i) \hookrightarrow \mathbb{Q}\left(\sqrt{2}, i\right)$$

per risolvere l'esercizio.

2. Possiamo considerare le estensioni consecutive

$$\mathbb{Q} \hookrightarrow \mathbb{Q}\left(\sqrt{2}\right) \hookrightarrow \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$$

e provare a fare come nel punto precedente. Conosciamo già il grado della prima estensione, perciò concentriamoci sulla seconda. Un elemento di $\mathbb{Q}[X]$ che ha come radice $\sqrt{3}$ è $X^2 - 3$: vediamo se come elemento di $\mathbb{Q}\left(\sqrt{2}\right)[X]$ continua a essere irriducibile. È un polinomio a coefficienti nel campo $\mathbb{Q}\left(\sqrt{2}\right)$ di grado 2, quindi controlliamo se le sue radici sono $\mathbb{Q}\left(\sqrt{2}\right)$. Ora, poiché $\sqrt{2}$ è algebrico su $\mathbb{Q}$, possiamo scrivere

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}.$$

Vediamo allora se $\sqrt{3} = a + b\sqrt{2}$ per qualche $a, b \in \mathbb{Q}$: non è il caso perché

$$\sqrt{3} = a + b\sqrt{2} \Rightarrow 3 = a^2 + 2b^2 + 2ab\sqrt{2} \Rightarrow \underbrace{\frac{3 - a^2 - 2b^2}{2ab}}_{\in\mathbb{Q}} = \underbrace{\sqrt{2}}_{\notin\mathbb{Q}}.$$

Possiamo quindi concludere che pure l'estensione $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ in esame ha grado 2.

3. Ovviamente $\alpha := \sqrt{2} + \sqrt{3} \in \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, e quindi $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Per dimostrare l'inclusione inversa, basta verificare che $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$. Possiamo per esempio ragionare così: l'inversa di α è $\alpha^{-1} = -\sqrt{2} + \sqrt{3}$ e possiamo scrivere

$$\sqrt{2} = \frac{\alpha - \alpha^{-1}}{2} \quad \text{e} \quad \sqrt{3} = \frac{\alpha + \alpha^{-1}}{2}.$$

E questo basta per concludere che $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$.

4. Come al solito cerchiamo prima di tutto un polinomio che abbia come radice $\alpha := \sqrt{2} + \sqrt{3}$.

$$\begin{aligned} \alpha^2 &= 5 + 2\sqrt{6} \\ \left(\alpha^2 - 5\right)^2 &= 24 \\ \alpha^4 - 10\alpha^2 + 1 &= 0. \end{aligned}$$

Quindi ecco un possibile polinomio minimo: $X^4 - 10X^2 + 1 = 0$. I possibili candidati a radici sono 1 e -1, ma nessuno tra questi lo è. Quindi se $X^4 - 10X^2 + 1 = 0$ è riducibile, allora deve essere fattorizzabile in due polinomi di grado 2. Nemmeno questa è una possibilità perché $Y^2 - 10Y + 1 = 0$ è un polinomio di grado 2 a coefficienti in $\mathbb{Q}$ che non ha radici in $\mathbb{Q}$. □

Esercizio 5.2 (Estensioni di $\mathbb{Q}$)**.** 1. Mostrare che per ogni $n \geq 1$ esiste $\alpha \in \mathbb{R}$ tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
2. $[\mathbb{R} : \mathbb{Q}] = [\mathbb{C} : \mathbb{Q}] = \infty$.

Svolgimento. 1. L'idea è di trovare degli $\alpha_n \in \mathbb{R}$ radici di polinomi irriducibili $p_n \in \mathbb{Q}[X]$ tali che $\deg p_n = n$. Infatti, grazie alla Proposizione 4.4 si ha $[\mathbb{Q}(\alpha_n) : \mathbb{Q}] = \deg p_n$. Ad esempio, i numeri $\alpha_n := \sqrt[n]{2}$ hanno rispettivamente come polinomio minimo $X^n - 2 \in \mathbb{Q}[X]$. La verifica che questi polinomi siano tutti irriducibili è lasciato come esercizio.
2. Se l'estensione $\mathbb{Q} \to \mathbb{R}$ fosse di grado n, allora abbiamo visto che si può costruire una estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ di grado $n+1$, ma ciò non è possibile. Il fatto che pure $\mathbb{Q} \subseteq \mathbb{C}$ è di grado infinito segue immediatamente. □

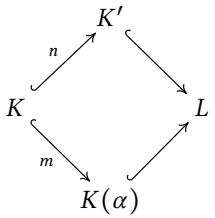
Esercizio 5.3 (Problema 399 di [Tsu])**.** Dimostra che $X^3 - 2$ è irriducibile sul campo $\mathbb{Q}(i)$.

Svolgimento. È un polinomio di grado 3 a coefficienti in un campo: basta quindi far vedere che non ha radici in quel campo. Sia $\alpha \in \mathbb{Q}(i)$ una qualsiasi delle radici di $X^3 - 2$. In particolare si ha l'inclusione $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(i)$ e si può scrivere

$$[\mathbb{Q}(i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}].$$

Calcoliamo prima quello che siamo immediatamente in grado di fare. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ perché $X^3 - 2 \in \mathbb{Q}[X]$ è il polinomio minimo di α e $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ perché $X^2 + 1 \in \mathbb{Q}[X]$ è polinomio minimo di i. E siamo caduti in un assurdo perché $3 \nmid 2$. □

Esercizio 5.4. Siano $K \subseteq K' \subseteq L$ due estensioni e $\alpha \in L$. Sia anche $[K' : K] = n$ e $[K(\alpha) : K] = m$.



1. Dimostrare che $\mathrm{mcm}(m, n) \mid [K'(\alpha) : K] \leq mn$. (Dunque $[K'(\alpha) : K] = mn$ se $\mathrm{mcd}(m, n) = 1$.)
2. Far vedere che $[K'(\alpha) : K] \nmid mn$ se $K = \mathbb{Q}$, $L = \mathbb{C}$, $K' = \mathbb{Q}(\beta)$ con α e β radici distinte di $X^3 - 2$.

Svolgimento. [Da riscrivere.]

1. $m' := [K'(\alpha) : K'] \leq m$, $K \subseteq K' \subseteq K'(\alpha)$ estensioni $\Rightarrow l := [K'(\alpha) : K] = [K'(\alpha) : K'][K' : K] = m'n \leq mn$. $K \subseteq K(\alpha) \subseteq K'(\alpha)$ estensioni $\Rightarrow m \mid l$; $n \mid l = m'n \Rightarrow \mathrm{mcm}(m, n) \mid l$.

2. $\mathrm{m}_\alpha = \mathrm{m}_\beta = X^3 - 2$ (perché monico e irriducibile in $\mathbb{Q}[X]$) $\Rightarrow m = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_\alpha) = 3$ e analogamente $n = 3$.
$\omega := \alpha\beta^{-1} \in \mathbb{C}$ tale che $K'(\alpha) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta, \omega)$.
$\omega^3 = \alpha^3\beta^{-3} = 1 \Rightarrow \omega$ radice di $X^3 - 1 = (X-1)f$ con $f := (X^2 + X + 1)$ monico e irriducibile in $\mathbb{Q}[X]$; $\omega \neq 1 \Rightarrow \omega$ radice di $f \Rightarrow \mathrm{m}_\omega = f \Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\mathrm{m}_\omega) = 2$.
$[K'(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta, \omega) : \mathbb{Q}] = 3 \cdot 2 = 6 \nmid mn = 9$. □

6 Chiusura algebrica

[Da riscrivere.]

Lemma 6.1. Sia $K \subseteq L$ un'estensione. Allora la *chiusura algebrica* di K in L

$$\overline{K}^L := \{\alpha \in L : \alpha \text{ algebrico su } K\}$$

è un sottocampo di L. Inoltre l'estensione $K \subseteq \overline{K}^L$ è algebrica e $\overline{\overline{K}^L}^L = \overline{K}^L$.

Dimostrazione. Chiaramente $K \subseteq \overline{K}^L$ (in particolare $1 \in \overline{K}^L$).
$\alpha, \beta \in \overline{K}^L \Rightarrow$ per la Proposizione di prima $K \subseteq K(\alpha, \beta)$ è un'estensione algebrica $\Rightarrow \alpha - \beta, \alpha\beta \in K(\alpha, \beta)$ sono algebrici su $K \Rightarrow \alpha - \beta, \alpha\beta \in \overline{K}^L$.
Analogamente $0 \neq \alpha \in \overline{K}^L \Rightarrow K \subseteq K(\alpha)$ estensione algebrica $\Rightarrow \alpha^{-1} \in K(\alpha)$ algebrico su $K \Rightarrow \alpha^{-1} \in \overline{K}^L$.
Per definizione l'estensione $K \subseteq \overline{K}^L$ è algebrica. Analogamente è algebrica l'estensione $\overline{K}^L \subseteq \overline{\overline{K}^L}^L$, e quindi anche $K \subseteq \overline{\overline{K}^L}^L$ per la Proposizione precedente. Allora $\overline{\overline{K}^L}^L \subseteq \overline{K}^L$, per cui $\overline{\overline{K}^L}^L = \overline{K}^L$. □

Definizione 6.2. Una *chiusura algebrica* di un campo K è un'estensione algebrica $K \subseteq \overline{K}$ con $\overline{K}$ algebricamente chiuso.

Corollario 6.3. $K \subseteq L$ estensione con L algebricamente chiuso $\Rightarrow K \subseteq \overline{K}^L$ è una chiusura algebrica di K.

Dimostrazione. $K \subseteq \overline{K}^L$ estensione algebrica per la Definizione-Proposizione. $\overline{K}^L$ algebricamente chiuso: $f \in \overline{K}^L[X] \setminus \overline{K}^L \subseteq L[X] \setminus L \Rightarrow \exists\, \alpha \in L$ tale che $f(\alpha) = 0$ (perché L algebricamente chiuso) $\Rightarrow \alpha$ algebrico su $\overline{K}^L \Rightarrow \alpha \in \overline{\overline{K}^L}^L = \overline{K}^L$. □

Esempio 6.4. $\mathbb{Q} \subseteq \overline{\mathbb{Q}} := \overline{\mathbb{Q}}^{\mathbb{C}}$ è una chiusura algebrica di $\mathbb{Q}$. Si dice che $\alpha \in \mathbb{C}$ è *algebrico* (risp. *trascendente*) se $\alpha \in \overline{\mathbb{Q}}$ (risp. $\alpha \notin \overline{\mathbb{Q}}$).

Lemma 6.5. Sia K un campo. Allora esiste un'estensione $K \to K'$ tale che ogni polinomio non costante a coefficienti in K ha una radice in K'.

Dimostrazione. Consideriamo l'insieme

$$U := \{f \in K[X] \mid f \text{ irriducibile e monico}\}$$

e per ogni $f \in U$ assegniamo un simbolo X_f che svolgerà il ruolo di indeterminata per certi polinomi. Consideriamo infatti l'anello dei polinomi a coefficienti in K e nelle indeterminate X_f, con $f \in U$,

$$A := K\left[X_f \mid f \in U\right].$$

[Abbiamo parlato di polinomi in un un numero arbitrario di indeterminate?]
L'insieme $I := \left(f(X_f) \mid f \in U\right)$ è un ideale di A. Mostriamo che $I \subsetneq A$: Se fosse $I = A$, allora esisterebbero $f_1, \dots, f_n \in U$ distinti e $g_1, \dots, g_n \in A$ tali che

$$h := \sum_{l=1}^{n} f_i\left(X_{f_i}\right) g_i = 1.$$

$K \subseteq L$ campo di spezzamento di $\prod_{i=1}^{n} f_i \Rightarrow \forall\, i = 1, \dots, n\ \exists\, \alpha_i \in L$ tale che $f_i(\alpha_i) = 0$. Valutando $h = 1$ in

$$X_f = \begin{cases} \alpha_i & \text{se } f = f_i \text{ per qualche } i = 1, \dots, n \\ 0 & \text{altrimenti} \end{cases}$$

si ottiene $0 = 1$ in L, assurdo.
$\exists\, J \subset A$ ideale massimale tale che $I \subseteq J \Rightarrow K' := A/J$ campo e $\pi|_K : K \to K'$ (con $\pi : A \to K'$ proiezione) estensione di campi con la proprietà richiesta: dato $f \in K[X] \setminus K$, posso supporre $f \in U \Rightarrow f(\pi(X_f)) = \pi(f(X_f)) = 0$ perché $f(X_f) \in I \subseteq J = \ker(\pi)$. □

Teorema 6.6. Ogni campo K ha una chiusura algebrica $K \subseteq \overline{K}$.

Dimostrazione.
- Posto $K_0 := K$, per il Lemma induttivamente $\forall\, n \in \mathbb{N}\ \exists\, K_n \subseteq K_{n+1}$ estensione tale che $f \in K_n[X] \setminus K \Rightarrow f$ ha una radice in K_{n+1}.
- $L := \bigcup_{n \in \mathbb{N}} K_n$ campo (*esercizio*) tale che $K \subseteq L$ estensione con L algebricamente chiuso: $f \in L[X] \setminus L \Rightarrow \exists\, n \in \mathbb{N}$ tale che $f \in K_n[X] \Rightarrow f$ ha una radice in $K_{n+1} \subseteq L$.
- $\overline{K} := \overline{K}^{L}$ tale che $K \subseteq \overline{K}$ chiusura algebrica di K (già visto). □

7 Campi di spezzamento

In generale, un $f \in K[X]$ non nullo può non avere tutte le radici all'interno del campo K. Successivamente abbiamo visto che si può costruire una chiusura algebrica in cui ogni polinomio a coefficienti in quel campo ha radici. Coi campi di spezzamento facciamo un passo indietro: dato $f \in K[X]$, aggiungere al campo K quanto basta per poter scrivere f come prodotto di polinomi di grado 1. Quindi è una costruzione che parte da un fissato polinomio.

Definizione 7.1 (Campo di spezzamento)**.** Sia K un campo e $f \in K[X]$ non nullo. Un *campo di spezzamento* di f è un'estensione $i : K \to K_f$ tale che:

1. f si *spezza* su K_f, vale a dire esistono $c \in K^*$ e $\alpha_1, \dots, \alpha_n \in K_f$ tali che

$$i_*(f) = c \prod_{k=1}^{n} (X - \alpha_k).$$

   Con il solito abuso possiamo pure scrivere f invece di $i_*(f)$ a patto di ricordarsi che il polinomio così fattorizzato è visto come elemento di $K_f[X]$, anello in cui si può effettivamente scrivere questa fattorizzazione.
2. $K_f = K(\alpha_1, \dots, \alpha_n)$, ovvero $i : K \to K_f$ è una estensione generata dalle radici di f in K_f.

Tecnicamente, un campo di spezzamento è un'estensione $K \to K_f$, ma talvolta si chiama campo di spezzamento anche solo il campo K_f.

Esempio 7.2. Consideriamo il polinomio $X^2 + 1 \in \mathbb{Q}[X]$. Come polinomio a coefficienti complessi ha due radici, i e $-i$. Il campo di spezzamento si costruisce aggiungendo le radici, cioè $\mathbb{Q}(i, -i)$. Certo, due generatori sono sovrabbondanti perché si verifica subito che $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$. Sicuramente il polinomio in esame ha radici in $\mathbb{C}$, ma è il campo di spezzamento è definito come il più piccolo che si può ottenere aggiungendo le radici di quel polinomio.

[Fare altri esempi.]

Abbiamo già visto come dato un qualsiasi polinomio irriducibile $p \in K[X]$, allora in $\frac{K[X]}{\langle p \rangle}$ una radice di p è $X + \langle p \rangle$. Questo è anche vero per ogni polinomio non nullo, visto che $K[X]$ è un dominio a fattorizzazione unica. Possiamo reiterare questo processo fino ad aggiungere tutte le radici e questo è il risultato del seguente teorema.

Teorema 7.3 (Esistenza campo di spezzamento)**.** Sia K un campo e $f \in K[X]$ non nullo. Allora

1. Esiste un campo di spezzamento $K \hookrightarrow K_f$ di f.
2. $\left[K_f : K\right] \leq (\deg f)!$.
3. Se f è pure irriducibile in $K[X]$, allora $\deg f$ divide $\left[K_f : K\right]$.

Dimostrazione. Il terzo punto non richiede particolare sforzo, perciò lo liquidiamo subito. Scriviamo $f = cg$ con $c \in K$ e $g \in K[X]$ monico: se f è irriducibile, lo è anche g e quindi g è il polinomio minimo delle sue radici in K_f (Proposizione 2.11). In particolare, se $\alpha \in K_f$ è una qualsiasi di queste, abbiamo che

$$\left[K_f : K\right] = \left[K_f : K(\alpha)\right] \underbrace{\left[K(\alpha) : K\right]}_{=\deg g = \deg f}.$$

Proviamo i primi due punti simultaneamente per induzione sul grado del polinomio $n := \deg f$. Se $n = 0$, allora il polinomio è un elemento invertibile e quindi basta prendere $K_f = K$; è ovvio anche che $1 = \left[K_f : K\right] \leq (\deg f)!$. Sia ora $n > 0$. Scegliamo $g \in K[X]$ irriducibile che divide f, esiste poiché $K[X]$ è un dominio a fattorizzazione unica. Possiamo assumere senza perdere nulla anche che f e g siano monici. Sappiamo che un campo che ha sicuramente qualche radice di g e quindi di f è

$$E := \frac{K[X]}{\langle g \rangle}.$$

Abbiamo visto anche come E può essere visto come il campo $K(\alpha)$, dove α è una delle radici di g in E. Abbiamo, vale a dire, un'estensione

$$i : K \to E = K(\alpha_1)$$

con $\alpha_i \in E$ radice di f. Quindi il polinomio f visto come elemento di $E[X]$ è divisibile per $X - \alpha_1$. Più rigorosamente:

$$i_*(f) = (X - \alpha_1) f_1 \text{ per qualche } f_1 \in E[X].$$

Qui f_1 ha grado $\deg f - 1$ e quindi, per induzione esiste un campo di spezzamento

$$j : E \to L := E(\alpha_2, \dots, \alpha_n)$$

in cui $j_*(f_1) = (X-\alpha_2)\cdots(X-\alpha_n)$ con $\alpha_2, \dots, \alpha_n \in L$. Mostriamo ora come la composizione delle estensioni $K \xrightarrow{i} E \xrightarrow{j} L$ è un campo di spezzamento per f. Infatti

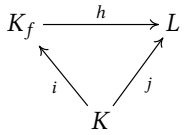
$$(ji)_*(f) = j_*(i_*(f)) = (X - j(\alpha_1))j_*(f_1) = (X-j(\alpha_1))(X-\alpha_2)\cdots(X-\alpha_n).$$

Da costruzione poi $L = E(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Vediamo il secondo punto: per il passo induttivo possiamo scrivere

$$[L:K] = \underbrace{[L:E]}_{\leq (n-1)!}\underbrace{[E:K]}_{=\deg g} \leq n!. \qquad \square$$

[Fare anche un esempio concreto per spiegare la dimostrazione sopra?]

Teorema 7.4 (Unicità campo di spezzamento)**.** Sia $i : K \to K_f$ campo di spezzamento di un $f \in K[X]$ non nullo e $j : K \to L$ estensione. Allora esiste almeno un morfismo di estensioni $h : K_f \to L$

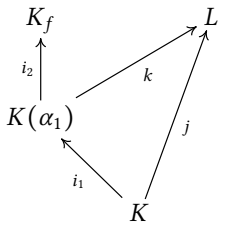


se e solo se f si spezza su L. In particolare, il campo di spezzamento di un polinomio non nullo è unico a meno di isomorfismi.

Dimostrazione. Allora esistono $c \in K^*$ e $\alpha_1, \dots, \alpha_n \in K_f$, con $n := \deg f$, tali che $i_*(f) = c\prod_{l=1}^{n}(X-\alpha_l)$ e $K_f = K(\alpha_1, \dots, \alpha_n)$.
Se abbiamo un morfismo di estensioni $h : K_f \to L$, allora

$$j_*(f) = (hi)_*(f) = \underbrace{h_*i_*(f) = h_*\left(c\prod_{l=1}^{n}(X-\alpha_l)\right)}_{f \text{ si spezza su } K_f} = h(c)\prod_{l=1}^{n}(X - h(\alpha_l)).$$

Vediamo il viceversa per induzione. La base dell'induzione $n = 0$ funziona perché $K_f \cong K$ e possiamo scegliere $h = ji^{-1}$. Passiamo al passo induttivo. Sia $n > 0$. Il polinomio minimo $m \in K[X]$ di α_1 si spezza su L, cioè $j_*(m)$ si scrive come prodotto di fattori lineari. Se indichiamo con $\beta \in L$ una delle radici di m, allora esiste un morfismo di estensioni $k : K(\alpha_1) \to L$ che manda α_1 in β.



Poiché $\alpha_1 \in K(\alpha_1)$ è una radice di $i_{1*}(f)$, allora

$$i_{1*}(f) = (X-\alpha_1)g \text{ per qualche } g \in K(\alpha_1)[X].$$

Il polinomio g è di grado $n-1$. Osserviamo come $i_2 : K(\alpha_1) \to K_f$ campo di spezzamento di g e g si spezza su L, perché g divide f e f si spezza su L. Per induzione esiste un morfismo di estensioni da i_2 a k che chiamiamo $h : K_f \to L$. Segue subito che h è un morfismo di estensioni come nell'enunciato. $\square$

8 Estensioni normali

Definizione 8.1. Un'estensione algebrica $K \hookrightarrow L$ è *normale* quando il polinomio minimo di ogni elemento di L si spezza su L.

Proposizione 8.2. Sia $i : K \to L$ un'estensione. Allora sono equivalenti:

1. $i : K \to L$ è normale.
2. Ogni $f \in K[X]$ irriducibile che ha una radice in L si spezza in L.

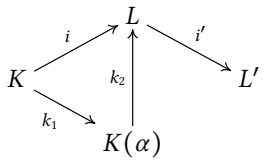
Dimostrazione. $(1 \Rightarrow 2)$ Sia $f \in K[X]$ irriducibile e indichiamo con $\alpha \in L$ una delle sue radici. Siano $g \in K[X]$ monico e $c \in K^*$ tali che $f = cg$. Ora α è radice di g e g è irriducibile: quindi, grazie alla Proposizione 2.11, g è proprio il polinomio minimo di α. Assumendo (1), possiamo concludere che f si spezza completamente in L.
$(2 \Rightarrow 1)$ Banale. □

Molto presto vedremo altre definizioni di estensioni normali, forse più interessanti per la piega che prenderanno le cose.

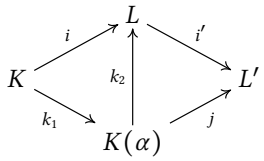
Proposizione 8.3. Un'estensione finita è normale se e solo se è il campo di spezzamento di un polinomio non nullo.

Un verso è banale, l'altro dovrebbe sorprenderti: un campo di spezzamento di *un* polinomio non nullo consente di spezzare completamente tutti i polinomi minimi. Non è banale, richiederà del lavoro non indifferente, e manca solo di introdurre la separabilità per poter parlare delle *estensioni di Galois*, il fine di queste pagine.

Dimostrazione. $(\Rightarrow)$ Esercizio.
$(\Leftarrow)$ Sia $i : K \to L$ campo di spezzamento di un fissato $f \in K[X]$ non nullo e preso $\alpha \in L$ proviamo che il polinomio minimo $m \in K[X]$ si spezza completamente in L. Chiaramente $\alpha \in L$, quindi mostriamo che qualsiasi altra sua radice β appartiene a L. Siamo più precisi: dove dovrebbero vivere le radici? Costruiamo a questo fine il campo di spezzamento $j : L \to L'$ di $i_*(m) \in L[X]$, cioè un campo che sicuramente contiene tutte le radici di m. Quindi, tecnicamente parlando, non giungeremo a provare che $\beta \in L$, ma che β sta nella copia di L da qualche parte. Se ancora il discorso è fumoso, ci arriveremo piano piano. Disegniamo per cominciare:



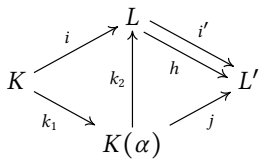
Qui introduciamo notazioni: k_1 manda $r \in K$ in $i(r)$ mentre k_2 è una mera inclusione insiemistica. Se $\beta \in L'$ è una delle radici di $m \in K[X]$, allora possiamo costruire un morfismo di estensioni $j : K(\alpha) \to L'$ da k_2 a $i'i$ che manda α in β:



Adesso constatiamo che f si spezza completamente pure su L'. Infatti se f si spezza come $c\prod_{l=1}^{n}(X-\alpha_l)$ in L, abbiamo

$$(i'i)_*(f) = i'_* i_*(f) = i'_*\left(c\prod_{l=1}^{n}(X-\alpha_l)\right) = i'(c)\prod_{l=1}^{n}(X-i'(\alpha_l)).$$

Questo fatto apparentemente inutile non lo è se si ricorda $i'i = jk_1$: segue che $k_{1*}(f)$ si spezza completamente su L'. Per il Teorema 7.4 esiste un morfismo di estensioni $h : L \to L'$ da k_2 a j.



Qui abbiamo che $h(\alpha) = h(k_2(\alpha)) = \beta$. Avevamo detto che volevamo vedere che $\beta \in L$: a essere precisi abbiamo trovato β appartiene alla copia di L dentro L'. Va bene... no? □

Esercizio 8.4. Quindi nella dimostrazione sopra a cos'è servito i'?

9 Estensioni separabili

Definizione 9.1. Sia K un campo. Un $f \in K[X]$ non nullo è detto *separabile* quando ha $\deg(f)$ radici distinte in un campo di spezzamento di f.

Richiamo 9.2 (Derivata di un polinomio)**.** Dato R un anello e $f := \sum_{k\in\mathbb{N}} a_k X^k \in R[X]$, la *derivata* di f è definito come il polinomio

$$f' := \sum_{k\geq 1} k a_k X^{k-1}.$$

Ricordiamo anche che soddisfa le note proprietà della derivazione vista in Analisi: in particolare $(f+g)' = f' + g'$ e $(fg)' = f'g + fg'$ e la derivata dei polinomi costanti è 0.
Questa nozione è importante per stabilire la molteplicità delle radici. Se $K \subseteq L$ è un'estensione, $f \in K[X]$ e $\alpha \in L$ è radice di f, allora α è radice multipla di f (vale a dire che cioè $(X-\alpha)^2$ divide f) se e solo se α è radice di f'.

Torniamo al discorso della definizione di polinomio separabile. È molto semplice provare la separabilità di un polinomio, ma questo richiede un'osservazione preliminare.

Osservazione 9.3. Sia $i : K \to L$ un'estensione e $f, g \in K[X]$. Se $\mathrm{mcd}(f,g) = 1$, allora $\mathrm{mcd}(i_*(f), i_*(g)) = 1$, cioè le estensioni preservano la relazione di essere coprimi.

Lemma 9.4. Sia K un campo e $f \in K[X]$ non nullo. Allora sono equivalenti:

1. f è separabile.
2. $\mathrm{mcd}(f, f') = 1$.

Dimostrazione. Sia $K \subseteq L$ un campo di spezzamento di f. Per $\alpha \in L$ radice di f, indichiamo con m_α la molteplicità algebrica di α. Possiamo quindi scrivere

$$f = (X - \alpha)^{m_\alpha} g_\alpha$$

dove in particolare g_α non si annulla in 0. Deriviamo:

$$f' = m_\alpha (X - \alpha)^{m_\alpha - 1} g_\alpha + (X - \alpha)^{m_\alpha} g'_\alpha = (X - \alpha)^{m_\alpha - 1} \left(m_\alpha g_\alpha + (X - \alpha) g'_\alpha \right).$$

Se $m_\alpha = 1$ per ogni radice α, allora f e f' non hanno alcun divisore comune $X - \alpha$. Quindi f e f' devono essere coprimi. Viceversa, se $\mathrm{mcd}(f, f') = 1$, allora tutti gli m_α devono essere 1. □

Proposizione 9.5. Sia K un campo e $f \in K[X]$ irriducibile . Allora un f è separabile se e solo se $f' \neq 0$.

È straordinariamente semplice verificare se un polinomio irriducibile è separabile o meno.

Dimostrazione. Se $f \neq 0$, allora $\mathrm{mcd}(f, f') = 1$ perché f è irriducibile. Quindi f è separabile. Viceversa, se f è separabile, allora $\mathrm{mcd}(f, f') = 1$, cioè $fg + f'h = 1$ per qualche $g, h \in K[X]$. Valutando in una delle radici $\alpha \in L$ di f, si ha $f'(\alpha)h(\alpha) = 1$, e quindi $f'(\alpha) \neq 0$. Possiamo tranquillamente concludere che $f' \neq 0$. □

Definizione 9.6. Un'estensione algebrica $K \subseteq L$ è detta *separabile* qualora il polinomio minimo di ogni elemento di L è separabile.

Per fortuna, per certe estensioni $K \subseteq L$ non è necessario dimostrare che tutti gli elementi di L abbiano polinomio minimo separabile.

Proposizione 9.7. Sia $K \subseteq L$ un'estensione generata da $\alpha_1, \ldots, \alpha_n \in L$ algebrici. Se i polinomi minimi degli α_i sono separabili, allora l'estensione $K \subseteq L$ è separabile.

Dimostrazione. [Da scrivere.] □

Definizione 9.8 (Campi perfetti)**.** [Scrivere.]

Proposizione 9.9. Sia K un campo di caratteristica 0. Tutti gli $f \in K[X]$ irriducibili sono separabili. Pertanto tutte le estensioni algebriche di campi di caratteristica 0 sono separabili.

Dimostrazione. Se f è irriducibile, in particolare $n := \deg f > 0$. Scriviamo $f := \sum_{k=0}^{n} a_k X^k$ con $a_n \neq 0$. Derivando, $f' = \sum_{k=1}^{n} k a_k X^{k-1}$. Il polinomio sicuramente non nullo: $n a_n \neq 0$ perché K ha caratteristica 0. Concludiamo quindi che f è separabile. □

Proposizione 9.10. Sia K un campo di caratteristica p primo. Tutti gli $f \in K[X]$ irriducibili sono separabili. Quindi le estensioni algebriche di siffatti campi sono separabili.

Dimostrazione. [Da scrivere.] □

Teorema 9.11 (Elemento primitivo)**.** Sia $K \subseteq L$ un'estensione finita e separabile. Allora $L = K(\alpha)$ per qualche $\alpha \in L$.

Dimostrazione. [Vedi la dimostrazione di Wikipedia.] □

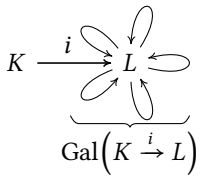


Figura 1. Il gruppo di Galois di un'estensione.

10 Gruppo di Galois

Definizione 10.1. Il *gruppo di Galois* di un'estensione $i : K \to L$ è

$$\mathrm{Gal}\left(K \xrightarrow{i} L\right) := \{\sigma : L \to L \text{ automorfismo} \mid \sigma \circ i = i\}.$$

Qualche volta l'omomorfismo è chiaro dal contesto o è una semplice inclusione, quindi non ci si scomoda a dargli un nome: alcune notazioni alternative sono $\mathrm{Gal}(K \hookrightarrow L)$, $\mathrm{Gal}(K \subseteq L)$, $\mathrm{Gal}(L/K)$ oppure $\mathrm{Gal}_K(L)$.

Cioè il gruppo di Galois di $i : K \to L$ è il gruppo degli automorfismi $L \to L$ che fissano gli elementi dell'immagine di K in L. Se usiamo il solito abuso, possiamo dire che è il gruppo degli automorfismi di L che fissano gli elementi di K, il che non scatena grossi intoppi in molti casi concreti.

In generale, il gruppo di Galois può essere complicato da calcolare: partiamo quindi dai casi in cui per lo meno abbiamo qualche appiglio a cui appoggiarsi, come il gruppo di Galois di un'estensione semplice e finita.

Proposizione 10.2. Sia $i : K \to L = K(\alpha)$ un'estensione semplice e $m \in K[X]$ polinomio minimo di α. Allora esiste una corrispondenza biunivoca tra l'insieme delle radici di m in L e l'insieme degli elementi di $\mathrm{Gal}_K(L)$: la funzione

$$\{\text{radici di } m \text{ in } L\} \to \mathrm{Gal}_K(L)$$

che manda una radice γ in L nell'automorfismo che manda α in γ. In particolare $\mathrm{Gal}_K(L)$ ha cardinalità $\leq [L : K] = \deg m$ e vale l'uguaglianza se e solo se m ha $\deg m$ radici distinte in L.

Dimostrazione. Tutto il lavoro è fatto nel Corollario 3.18. [Quasi: scrivere anche come mai gli endomorfismi di estensioni finite sono automorfismi.] □

La Proposizione dice precisamente quali sono gli elementi del gruppo e la sua cardinalità in un certo caso. È importante notare tuttavia che gruppi con la stessa cardinalità non necessariamente sono isomorfi, quindi la Proposizione sopra da qualche indicazione ma in generale non risolve totalmente il problema della determinazione del gruppo di Galois: dei conti vanno fatti e della Teoria dei Gruppi Finiti può sempre far comodo.

Un caso fortunato è quello in cui il gruppo di Galois ha ordine primo: in questo caso, il gruppo di Galois è ciclico è la questione è immediatamente dipanata.

Esempio 10.3 (Gruppo di Galois di $\mathbb{Q} \subseteq \mathbb{Q}(i)$)**.** Il numero complesso i ha polinomio minimo $X^2 + 1 \in \mathbb{Q}[X]$. Notiamo anche che $\mathbb{Q}(i)$ contiene entrambe le radici, i e $-i$, e che queste sono tutte distinte. Quindi $|\mathrm{Gal}(\mathbb{Q} \subseteq \mathbb{Q}(i))| = 2$. Il

gruppo di Galois è quindi (isomorfo a) C_2. Scriviamo comunque gli automorfismi esplicitamente: uno è quello che manda i in i ed è l'identità, mentre l'altro manda i in $-i$. Ricordando che si può scrivere $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, si ha che quest'ultimo automorfismo è

$$\mathbb{Q}(i) \to \mathbb{Q}(i)\,,\ a + bi \mapsto a - bi.$$

Esercizio 10.4. Studiare il gruppo di Galois di $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right)$.

Vediamo qualche esempio in cui bisogna operare delle scelte. Ricordiamo a tal proposito che se G è un gruppo di ordine p^2 con p primo, allora G è isomorfo a C_{p^2} oppure a $C_p \times C_p$.

Esempio 10.5. Calcoliamo il gruppo di Galois dell'estensione $\mathbb{Q} \subseteq L := \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Come abbiamo visto, $L = \mathbb{Q}(\alpha)$, con $\alpha := \sqrt{2} + \sqrt{3}$, e il polinomio minimo di α è $f := X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$. Questo polinomio ha 4 radici distinte tutte in L, che sono:

$$-\sqrt{3} - \sqrt{2}\,,\ -\sqrt{3} + \sqrt{2}\,,\ \sqrt{3} - \sqrt{2}\,,\ \sqrt{3} + \sqrt{2}.$$

Quindi il gruppo di Galois ha cardinalità 4, per cui le possibilità sono due: e isomorfo a C_4 oppure a $C_2 \times C_2$. Quale delle due? La proposizione sopra ci dice chi sono gli elementi del gruppo di Galois, che sono determinati da quale radice di f è mandato $\sqrt{2} + \sqrt{3}$. Ecco il piano: se il gruppo di Galois contiene qualche elemento di ordine 4, allora è C_4, altrimenti è $C_2 \times C_2$.
L'automorfismo σ_1 che manda α in α è l'identità, quindi la mettiamo da parte. Vediamo l'automorfismo σ_2 che manda α in $-\sqrt{3} - \sqrt{2}$.

$$\alpha \xrightarrow{\sigma_2} -\alpha \xrightarrow{\sigma_2} -\sigma_2(\alpha) = \alpha$$

e quindi l'ordine di σ_2 è 2. Vediamo l'automorfismo σ_3 che manda α in $-\sqrt{3} + \sqrt{2} = -\frac{1}{\alpha}$.

$$\alpha \xrightarrow{\sigma_3} -\frac{1}{\alpha} \xrightarrow{\sigma_3} -\frac{1}{\sigma_3(\alpha)} = \alpha$$

e quindi l'ordine di σ_3 è ancora 2. Vediamo l'automorfismo σ_4 che manda α in $\sqrt{3} - \sqrt{2} = \frac{1}{\alpha}$.

$$\alpha \xrightarrow{\sigma_4} \frac{1}{\alpha} \xrightarrow{\sigma_4} \frac{1}{\sigma_4(\alpha)} = \alpha$$

e quindi l'ordine di σ_3 è ancora 2. Possiamo concludere che $\mathrm{Gal}_{\mathbb{Q}}(L) \cong C_2 \times C_2$.

Non siamo così fortunati in generale per le estensioni finitamente generate, anche se abbiamo una proprietà che restringe il campo di ricerca degli elementi dei gruppi di Galois.

Proposizione 10.6. Sia $i : K \to L$ un'estensione finitamente generata, cioè $L = K(\alpha_1, \dots, \alpha_n)$ per degli $\alpha_1, \dots, \alpha_n \in L$. Ogni $\phi \in \mathrm{Gal}_K(L)$ è univocamente determinato da $\phi(\alpha_1), \dots, \phi(\alpha_n)$. In particolare, $\mathrm{Gal}_K(L)$ è isomorfo ad un sottogruppo di S_n.

Dimostrazione. Da definizione, gli elementi di $\mathrm{Gal}_K(L)$ fissano gli elementi di K e se due elementi di $\mathrm{Gal}_K(L)$ sono uguali su $\{\alpha_1, \dots, \alpha_n\}$, allora sono uguali ovunque. □

E qui è chiaro anche come mai ci sia un interesse verso i gruppi simmetrici S_n e i suoi sottogruppi, perché sostanzialmente gli elementi di $\mathrm{Gal}_K(L)$ sono permutazioni degli α_i.

Proposizione 10.7. Sia $i : K \to L$ un'estensione, $f \in K[X]$ e $\phi \in \mathrm{Gal}_K(L)$. Allora per ogni $\alpha \in L$ si ha

$$i_*(f)(\phi(\alpha)) = \phi\left(i_*(f)(\alpha)\right).$$

Quindi gli elementi di $\mathrm{Gal}_K(L)$ mandano le radici di f in L in radici di f in L.

Dimostrazione. Scriviamo $f := \sum_{k\in\mathbb{N}} a_k X^k$ e ricordiamo che $\phi \circ i = i$.

$$\begin{aligned} i_*(f)(\phi(\alpha)) &= \sum_{k\in\mathbb{N}} i(a_k)\left(\phi(\alpha)\right)^k = \\ &= \sum_{k\in\mathbb{N}} \phi\left(i(a_k)\right)\phi\left(\alpha^k\right) = \\ &= \phi\left(\sum_{k\in\mathbb{N}} i(a_k)\,\alpha^k\right) = \\ &= \phi\left(i_*(f)(\alpha)\right). \end{aligned}$$

□

Perché questo è importante? Per questo motivo ad esempio.

Corollario 10.8. Sia $i : K \to L = K(\alpha_1, \dots, \alpha_n)$ un'estensione finitamente generata e $m_1, \dots, m_n \in K[X]$ polinomio di minimi di $\alpha_1, \dots, \alpha_n$ rispettivamente. Allora gli elementi di $\mathrm{Gal}_K(L)$ per ogni $i \in \{1, \dots, n\}$ mandano α_i in radici di m_i in L.

Definizione 10.9. Sia K un campo, e $f \in K[X]$ non nullo. Il *gruppo di Galois* di f su K è il gruppo di Galois di un campo di spezzamento per f. Viene indicato molto semplicemente come $\mathrm{Gal}_K(f)$.

Abbiamo visto che il campo di spezzamento è unico a meno di isomorfismo, e anche il corrispondente gruppo di Galois è definito a meno di isomorfismo. È importante capire che è importante avere una certa manualità nel calcolo dei campi di spezzamento di polinomi.

Corollario 10.10. Sia K un campo e $f \in K[X]$ non nullo. Allora $\mathrm{Gal}_K(f)$ è isomorfo ad un sottogruppo delle permutazioni delle radici di f e in particolare, se f ha d radici distinte, allora $|\mathrm{Gal}_K(f)|$ divide $d!$.

Per polinomi di grado piccolo, 2 oppure 3, questo è interessante.

Esempio 10.11 (Gruppo di Galois di polinomi di secondo grado)**.** [Nessun problema per quanto riguarda la caratteristica di K?] Sia K un campo e $f := aX^2+bX+c \in K[X]$. Se f ha una sola radice distinta, allora $\mathrm{Gal}_K(f)$ deve essere necessariamente banale. Se invece, ha due radici distinte, allora le possibilità sono due: $\mathrm{Gal}_K(f)$ è banale oppure ha ordine 2, cioè è ciclico di ordine 2. Vediamo quando accade ciò.

- f è riducibile su $K[X]$, e quindi ha due radici K. In questo caso il campo di spezzamento è K stesso e il gruppo di Galois di f è banale.
- f è irriducibile su $K[X]$, e quindi non ha radici K. Dobbiamo ricorrere ad un campo di spezzamento $K \subseteq K(\alpha_1, \alpha_2)$ che per il Teorema 7.3 ha grado 2. Pure il sottospazio $K(\alpha_1)$ ha grado 2 perché il polinomio minimo di α_1 ha grado 2. Quindi $K(\alpha_1, \alpha_2) = K(\alpha_1) = \{a + b\alpha_1 \mid a, b \in K\}$. Il gruppo di Galois allora contiene, oltre all'identità, sicuramente l'automorfismo che manda α_1 in α_2. Il gruppo di Galois quindi è (a meno di isomorfismi) C_2.

Esercizio 10.12. Al variare di K potrebbe variare anche il gruppo di Galois. Calcolare, ad esempio, $\mathrm{Gal}_{\mathbb{Q}}(X^2-2)$ e $\mathrm{Gal}_{\mathbb{R}}(X^2-2)$.

Esempio 10.13 (Gruppo di Galois di polinomi di terzo grado)**.** [...]

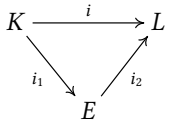
Fortunatamente riusciamo ancora ad avere ancora qualche indicazione sulla cardinalità del gruppo di Galois per estensioni finite.

Lemma 10.14. Sia $i : K \to L$ un'estensione finita e $j : K \to L'$ un'altra estensione. Allora il numero dei morfismi di estensioni $L \to L'$ da i a j è $\leq [L : K]$. Inoltre vale l'uguaglianza se e solo se per ogni $\alpha \in L$ il suo polinomio minimo come elemento di $L'[X]$ si spezza ed è separabile.

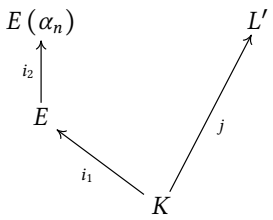
Dimostrazione. A causa della Proposizione 4.7, se $i : K \to L$ è finita, allora esistono $\alpha_1, \dots, \alpha_n \in L$ algebrici tali che $L = K(\alpha_1, \dots, \alpha_n)$. Andiamo a dimostrare per induzione sul numero n di generatori $\alpha_i \in L$ il seguente fatto:

> Sia $i : K \to L = K(\alpha_1, \dots, \alpha_n)$ un'estensione con $\alpha_1, \dots, \alpha_n$ algebrici e $j : K \to L'$ un'altra estensione. Allora il numero dei morfismi di estensioni $L \to L'$ da i a j è $\leq [L : K]$. Vale l'uguaglianza se e solo se ogni $\alpha_i \in L$ ha un polinomio minimo si spezza in $L'[X]$ ed è separabile.

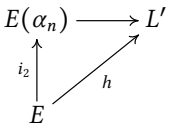
Il caso base, $n = 1$, è La Proposizione 10.2. Sia ora $n > 0$. Introduciamo il campo $E := K(\alpha_1, \dots, \alpha_{n-1})$, per cui $L = E(\alpha_n)$, e decomponiamo l'estensione $i : K \to L$ come segue



dove $i_1(r) := i(r)$ e $i_2(s) := s$. Disegniamo allora



Induttivamente, ci sono al massimo $[E : K]$ morfismi di estensioni da i_1 a j e per ciascuno dei siffatti $h : E \to L'$, grazie al Corollario 3.18, sappiamo che il numero di morfismi di estensioni da i_2 a h



è minore o uguale a $[E(\alpha_n) : E]$. Per costruzione questi morfismi di estensioni sono morfismi da i a j. Quindi al massimo ci sono

$$[E(\alpha_n) : E][E : K] = [L : E][E : K] = [L : K]$$

estensioni da i a j. È immediato anche constatare come se i polinomi minimi si spezzano su L' e sono separabili, allora il numero dei morfismi di estensioni è esattamente $[L : K]$. Per il viceversa, supponiamo che ci siano $[L : K]$ morfismi di estensioni da i a j. [Qui è da riscrivere meglio...] □

Definizione 10.15. Un'estensione è detta *di Galois* qualora è finita, normale e separabile. Equivalentemente, un'estensione è di Galois quando è campo di spezzamento di un qualche polinomio non nullo separabile.

Il Lemma sopra fornisce quindi un criterio che può essere comodo a volte per capire se un'estensione $K \subseteq L$ è di Galois, a patto di avere l'informazione della cardinalità di $\mathrm{Gal}_K(L)$.

Proposizione 10.16 (Cardinalità gruppi di Galois)**.** Se $K \subseteq L$ è un'estensione finita, allora $|\mathrm{Gal}_K(L)| \leq [L : K]$. Vale l'uguaglianza se e solo se l'estensione è di Galois.

Dimostrazione. Poiché $K \subseteq L$ è un'estensione finita, allora i morfismi di estensioni da $K \subseteq L$ sono tutti automorfismi. Ricordiamo infatti che i morfismi di estensioni sono applicazioni lineari se si vede L come spazio vettoriale su K di dimensione finita. Allora $\mathrm{Gal}_K(L)$ è il gruppo dei morfismi di estensione dall'estensione $K \subseteq L$ in sé: si applica il Lemma di sopra. □

Quindi il gruppo di Galois di un'estensione finita è finito: l'interesse per i gruppi di ordine finito risiede anche in questo. [Fare qualche esempio in cui il gruppo di Galois è infinito.]

Proposizione 10.17. Se $F \subseteq K \subseteq L$ sono estensioni con $F \subseteq L$ di Galois, allora anche $K \subseteq L$ è di Galois.

Dimostrazione. [Ancora da scrivere.] □

Osservazione 10.18. Un caso particolarmente fortunato è quello dei campi perfetti. Abbiamo visto infatti che se K è perfetto, allora le estensioni algebriche $K \subseteq L$ sono tutte separabili. Se con $K \subseteq L$ è il campo di spezzamento di un certo $f \in K[X]$ non nullo, allora $K \subseteq L$ è di Galois. Se scriviamo G il gruppo di Galois di questa estensione, e $|G| = [L : K]$ e $|G|$ divide $(\deg f)!$; se inoltre f è pure irriducibile, possiamo dire anche che $\deg f$ divide $|G|$.

Esercizio 10.19. Determinare il campo di spezzamento e il gruppo di Galois di $f := X^4 - 4X^2 + 2$ su $\mathbb{Q}$.

Svolgimento. Anzitutto f è irriducibile per il Criterio di Eisenstein. In particolare, è anche monico, quindi è il polinomio minimo delle sue radici in qualche campo di spezzamento (vedi Proposizione 2.11). Le radici di f sono $\pm\alpha, \pm\beta$ con $\alpha := \sqrt{2+\sqrt{2}}$ e $\beta := \sqrt{2-\sqrt{2}}$ e possiamo scrivere il campo di spezzamento $\mathbb{Q} \subseteq L := \mathbb{Q}(\alpha, \beta)$. Tuttavia osserviamo che è sufficiente un solo generatore, perché

$$\beta = \sqrt{2-\sqrt{2}}\frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{2}}{\alpha} = \underbrace{\frac{\alpha^2-2}{\alpha}}_{\in\mathbb{Q}(\alpha)}.$$

Quindi $L = \mathbb{Q}(\alpha)$. Scriviamo G il gruppo di Galois dell'estensione in esame. Dato che $\mathbb{Q} \subseteq L$ è di Galois ($\mathbb{Q}$ perfetto e $\mathbb{Q} \subseteq L$ campo di spezzamento) possiamo dirne la cardinalità

$$|G| = [L : \mathbb{Q}] = \deg f = 4.$$

Grazie al Corollario 3.18, sappiamo che c'è un $\sigma \in G$ tale che $\sigma(\alpha) = \beta$. Riusiamo la relazione che abbiamo ricavato sopra tra α e β:

$$\sigma^2(\alpha) = \sigma(\beta) = \sigma\left(\frac{\alpha^2-2}{\alpha}\right) = \frac{\beta^2-2}{\beta} = \frac{-\sqrt{2}}{\beta} = -\alpha$$

Quindi $\sigma^2 \neq \mathrm{id}_L$. Questo è importante perché $|G| = 4$: quindi σ ha ordine 4. Possiamo concludere che $G \cong C_4$. □

Esercizio 10.20. Determinare il campo di spezzamento e il gruppo di Galois di $f := X^4 - 4X^2 - 2$ su $\mathbb{Q}$.

Svolgimento. Per il Criterio di Eisenstein f è irriducibile. Inoltre è monico, quindi è il polinomio minimo delle sue radici in qualche campo di spezzamento. Le radici di f sono

$$\pm\sqrt{2 \pm \sqrt{6}}.$$

Per semplicità, $\alpha := \sqrt{\sqrt{6}+2}$ e $\beta := \sqrt{\sqrt{6}-2}$. Quindi il campo di spezzamento è $L = \mathbb{Q}(\alpha, \beta i)$. Vediamo di trovare dei generatori più comodi o addirittura di ridurli. Osserviamo che $\alpha\beta i = \sqrt{2}i$ e quindi $\sqrt{2}i \in L$. Possiamo scrivere che $L = \mathbb{Q}\left(\alpha, \sqrt{2}i\right)$. L'estensione $\mathbb{Q} \subseteq L$ è di Galois la stessa ragione dell'esercizio precedente. Calcoliamo il grado dell'estensione $\mathbb{Q} \subseteq L$.

$$[L : \mathbb{Q}] = \left[\mathbb{Q}\left(\alpha, \sqrt{2}i\right) : \mathbb{Q}(\alpha)\right][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Qui, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è facile da calcolare, fa $\deg f = 4$. Rimane il grado dell'altra estensione, che è 2 (esercizio per te!). Quindi $|G| = 8$. Siamo fortunati perché questo ci basta: G si può identificare con un sottogruppo di S_4 e l'unico sottogruppo di S_4 che ha ordine 8 è il *gruppo diedrale* di ordine 8

$$D_4 := \left\langle r, s \,\middle|\, r^4 = s^2 = (sr)^2 = 1 \right\rangle. \qquad \square$$

Osservazione 10.21. Come vedi, qualche nozione sui gruppi finiti serve sempre.

Esercizio 10.22 (Problema 231 di [Tsu])**.** Far vedere che $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ è di Galois e il corrispondente gruppo di Galois è C_4.

11 Campo fisso

Consideriamo un'estensione di campi $K \xrightarrow{i} L$ e un polinomio $f \in K[X]$. Come un qualunque $\sigma \in \mathrm{Gal}_K(L)$ fissa gli elementi di K, l'automorfismo indotto $\sigma_* : L[X] \to L[X]$ fissa i polinomi a coefficienti in K. Più precisamente,

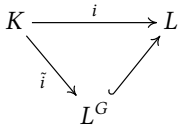
$$\sigma_* i_* = (\sigma i)_* = i_*.$$

La domanda ora è: $\mathrm{Gal}_K(L)$ fissa gli elementi di K, ma sono gli elementi di K gli unici che vengono fissati dagli elementi di $\mathrm{Gal}_K(L)$? Una domanda apparentemente innocente, ma che ci porta da qualche parte con l'introduzione di nuove idee.

Proposizione 11.1. Sia $K \xrightarrow{i} L$ un'estensione finita e G un sottogruppo di $\mathrm{Gal}_K(L)$. Allora

$$L^G := \{a \in L \mid \sigma(a) = a \text{ per ogni } \sigma \in G\}.$$

è un sottocampo di L. Inoltre l'estensione $K \xrightarrow{i} L$ si fattorizza come segue



dove $\tilde{i}(r) = i(r)$. Inoltre:

1. $L^G \subseteq L$ è finita
2. $L^G \subseteq L$ è separabile
3. $L^G \subseteq L$ è normale
4. $G = \mathrm{Gal}_{L^G}(L)$ e $|G| = \left[L^G : L\right]$.

Dimostrazione. [Vedi [Alu].] □

Corollario 11.2. Sia $K \xrightarrow{i} L$ un'estensione. Allora sono equivalenti:

1. $K \xrightarrow{i} L$ è di Galois
2. $K \xrightarrow{i} L$ è finita e $|\mathrm{Gal}_K(L)| = [L : K]$
3. $K \xrightarrow{i} L$ è finita e $K \to L^{\mathrm{Gal}_K(L)}$, $r \to i(r)$ è un isomorfismo di campi.

Dimostrazione. [Vedi [Alu].] □

12 Discriminante polinomi

Abbiamo visto che, assegnata un'estensione $K \xrightarrow{i} L$ e un $f \in K[X]$ con r radici in un campo L, allora $\mathrm{Gal}_K(L) \leq S_r$. Scriviamo le sue radici (anche ripetendole in caso di radici multiple) enumerandole in qualche modo

$$\alpha_1, \dots, \alpha_n$$

e introduciamo il *discriminante* di f

$$\delta_f := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Questo numero gode di qualche semplice proprietà:

1. f ha radici multiple se e solo se $\delta_f = 0$.
2. $\sigma\left(\delta_f\right) = \mathrm{sgn}\left(\sigma|_{\{\alpha_1,\dots,\alpha_r\}}\right) \delta_f$ per ogni $\sigma \in \mathrm{Gal}_K(L)$.

Proposizione 12.1. Sia K un campo e $f \in K[X]$ non nullo e separabile di grado n. Indichiamo con G_f il gruppo di Galois di f. Allora:

1. $\delta_f^2 \in K$.
2. $G_f \leq A_n$ se e solo se $\delta_f \in K$.

Dimostrazione. [Usare risultati della sezione precedente.] □

13 Campi finiti

Abbiamo visto degli esempi di campi finiti, cioè $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ per p che varia tra i numeri primi. Le estensioni finite di questi campi sono molto particolari.

Proposizione 13.1. Sia p primo. Se $\mathbb{F}_p \xrightarrow{i} L$ è un'estensione di grado n, allora il campo L ha p^n elementi, L è l'insieme degli zeri di $X^{p^n} - X \in \mathbb{F}_p[X]$. In particolare, $\mathbb{F}_p \xrightarrow{i} L$ è il campo di spezzamento del polinomio separabile $X^{p^n} - X \in \mathbb{F}_p[X]$, cioè è un'estensione di Galois. Viceversa, per ogni $n \in \mathbb{N}$, il polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$ ha campo di spezzamento di grado n.

Dimostrazione. La cardinalità di L è facile da determinare. Come spazio vettoriale ha una base di n elementi di L, mentre $\mathbb{F}_p$ ha p elementi: quindi L consiste di p^n combinazioni lineari degli elementi della base scelta. L'insieme degli elementi invertibili $L^\times$ ha cardinalità $p^n - 1$ e forma un gruppo con la moltiplicazione ereditata da L. Per il Teorema di Lagrange, ogni elemento $a \in L$ non nullo soddisfa $a^{p^n-1} = 1$. Possiamo quindi che tutti gli elementi di L sono zeri del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$. Per la Proposizione 9.5, questo polinomio è separabile, quindi ammette p^n radici distinte. Abbiamo quindi provato che $\mathbb{F}_p \xrightarrow{i} L$ è il campo di spezzamento del polinomio. [Scrivere il viceversa.] □

Definizione 13.2. Sia $p \geq 2$ primo. Scriviamo $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ uno qualsiasi dei campi di spezzamento di $X^{p^n} - X \in \mathbb{F}_p[X]$ (sappiamo che sono tutti isomorfi tra loro). Vale a dire, $\mathbb{F}_{p^n}$ è la L della Proposizione 13.1.

Le estensioni finite di $\mathbb{F}_p$, dove p è primo, sono quindi della forma $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ e campi di spezzamento di, rispettivamente, $X^{p^n} - X \in \mathbb{F}_p[X]$. E non è tutto: ogni $\mathbb{F}_{p^n}$ è l'insieme degli zeri di $X^{p^n} - X \in \mathbb{F}_p[X]$.

Per rendersi conto di come sono speciali queste extensioni, si pensi infatti come non sono rari gli esempi di estensioni finite $K \hookrightarrow L$ in cui non è proprio possibile che tutti gli elementi di L siano radici di un solo polinomio in $K[X]$.

Ecco una prima conseguenza: il problema di trovare il campo di spezzamento di un polinomio di $\mathbb{F}_p[X]$ è subito risolto.

Proposizione 13.3. Sia p primo e $f \in \mathbb{F}_p[X]$ irriducibile di grado d. Allora il suo campo si spezzamento è $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$ e f divide $X^{p^d} - X \in \mathbb{F}_p[X]$. In generale, se $f \in \mathbb{F}_p[X]$ è non nullo e si fattorizza i termini irriducibili in $\mathbb{F}_p[X]$ come $f = f_1 \cdots f_r$, allora il campo di spezzamento di f è $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$, dove $d := \operatorname{mcm}(\deg f_1, \dots, \deg f_r)$.

Dimostrazione. Prendiamo in esame l'estensione

$$\mathbb{F}_p \hookrightarrow E := \frac{\mathbb{F}_p[X]}{\langle f \rangle}, \ a \mapsto a + \langle f \rangle$$

di cui sappiamo che è di grado d e E contiene una radice di f. Per la Proposizione 13.1, questa estensione è il campo di spezzamento $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$ di $X^{p^d} - X \in \mathbb{F}_p[X]$ in cui $\mathbb{F}_{p^d}$ è l'insieme degli zeri di questo polinomio. Possiamo dire che f divide $X^{p^d} - X$, essendo f il polinomio minimo di qualche radice di questo polinomio. □

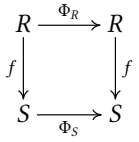
E se questa questione è definitivamente risolta, rimane da capire come calcolare il gruppo di Galois. Ad ora sappiamo che il gruppo di Galois di $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ è il gruppo di Galois del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$.

Lemma 13.4 (The freshman's dream)**.** Sia R un anello commutativo di caratteristica $p \geq 2$ primo. Allora

$$\Phi_R : R \to R, \ \Phi_R(a) := a^p$$

è un omomorfismo di anelli, che chiameremo *omomorfismo di Frobenius*. Inoltre se $f : R \to S$ è un omomorfismo di anelli di caratteristica $p \geq 2$ primo, allora

commuta



Dimostrazione. Poiché R è commutativo, allora $\Phi_R(ab) = \Phi_R(a)\Phi_R(b)$ per ogni $a, b \in R$. L'unica parte che può suscitare qualche perplessità è quella che riguarda la somma. Ricordiamo che per ogni anello commutativo R vale la *formula del binomio di Newton*, cioè

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

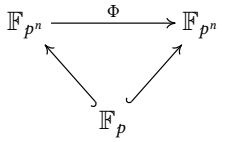
dove $\binom{n}{k} := \frac{n!}{k!(n-k)!}$. Osserviamo che $\binom{p}{k}$ è multiplo di p se $k \in \{2, \dots, p-1\}$: infatti p divide $p!$ ma nessuno degli $q!$ con $q < p$. Essendo R di caratteristica p della sommatoria $\sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$ sopravvive solo $a^p + b^p$. Per quanto riguarda l'ultima parte, si scrive in una riga:

$$f(\Phi_R(a)) = f(a^p) = f(a)^p = \Phi_S(f(a)) \quad \text{per ogni } a \in R. \qquad \square$$

Lemma 13.5 (Piccolo Teorema di Fermat)**.** L'omomorfismo di Frobenius $\Phi_{\mathbb{F}_p}$ è l'identità.

Dimostrazione. L'insieme degli elementi invertibili $\mathbb{F}_p^\times$ di $\mathbb{F}_p$ è un gruppo con la moltiplicazione ereditata da $\mathbb{F}_p$. Da Algebra 1 sappiamo che la cardinalità di questo gruppo è $p-1$. Quindi per il Teorema di Lagrange abbiamo che $a^{p-1} = 1$ per ogni $a \in \mathbb{F}_p^\times$, da cui segue che $a^p = a$. $\square$

Proposizione 13.6. Sia $p \geq 2$ primo e l'estensione $i : \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Allora l'omomorfismo di Frobenius $\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ è un automorfismo di estensioni



Inoltre

$$\mathrm{Gal}\left(\mathbb{F}_p \subseteq \mathbb{F}_{p^n}\right) = \mathrm{Gal}_{\mathbb{F}_p}\left(X^{p^n} - X\right) \cong C_n$$

e un suo generatore è Φ.

Dimostrazione. La prima parte è solo la combinazione dei due Lemmi precedenti. Inoltre Φ è biettivo perché è gli omomorfismi di campi sono iniettivi e $\mathbb{F}_{p^n}$ ha cardinalità finita.[1] Quindi effettivamente $\Phi \in \mathrm{Gal}\left(\mathbb{F}_p \subseteq \mathbb{F}_{p^n}\right)$. Di questo gruppo possiamo dire subito l'ordine: essendo $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ di Galois (Proposizione 13.1), il gruppo di Galois ha cardinalità $\left[\mathbb{F}_{p^n} : \mathbb{F}_p\right] = n$. Ecco il piano: se riusciamo a trovare un elemento di questo gruppo che ha ordine n abbiamo finito. Mostriamo che un elemento con questo requisito è Φ.
Scriviamo esplicitamente le potenze di Φ:

$$\Phi^k(a) = \underbrace{\Phi \circ \cdots \circ \Phi}_{k \text{ volte}}(a) = a^{p^k}$$

1. Se X è un insieme finito, allora le funzioni $X \to X$ iniettive sono biunivoche.

Dalla Proposizione 13.1 sappiamo che gli elementi di $\mathbb{F}_{p^n}$ sono le radici di $X^{p^n} - X$. Cioè Φ^n è l'identità. Questo è il più piccolo k per cui Φ^k è l'identità. Se $0 < m < n$, allora $X^{p^m} - X$, essendo separabile, ha p^m soluzioni distinte: questo significa che Φ^m fissa $p^m < p^n$ elementi, cioè non tutti gli elementi di $\mathbb{F}_{p^n}$. □

Riassumendo, il calcolo della campo di spezzamento di un $f \in \mathbb{F}_p[X]$ non nullo e di $\mathrm{Gal}_{\mathbb{F}_p}(f)$ è tutta questione di saper decomporre f in fattori irriducibili di $\mathbb{F}_p[X]$. Svolgiamo un esercizio a titolo d'esempio.

Esercizio 13.7. Determinare il gruppo di Galois G di $f := X^5 - X + 3 \in \mathbb{F}_q[X]$ per $q \in \{2, 3, 4, 5\}$.

Svolgimento. Ecco il piano: con l'aiuto della Proposizione 13.3 determiniamo il campo di spezzamento di f, perché per la Proposizione 13.6 il gruppo di Galois di f è in ogni caso un C_d con d da determinare.

$q = 2$ Il polinomio non ha radici, perché $f(0) = f(1) = 1$. Quindi se è riducibile, allora è decomponibile in due fattori, uno di grado 2 e l'altro di grado 3, senza radici in $\mathbb{F}_2$. L'unico di grado 2 in $\mathbb{F}_2[X]$ con questi requisiti è $(X^2 + X + 1)$: in effetti, compiendo la divisione Euclidea, si ha

$$f = (X^2 + X + 1)(X^3 + X^2 + 1).$$

Possiamo concludere: il campo di spezzamento è $\mathbb{F}_2 \subseteq \mathbb{F}_{2^6} = \mathbb{F}_{64}$ è il gruppo di Galois è (isomorfo a) C_6.

$q = 3$ In questo caso il polinomio è semplicemente $X^5 - X$. Raccogliendo:

$$f = X^5 - X = X(X - 1)(X + 1)(X^2 + 1).$$

Il campo di spezzamento di f è $\mathbb{F}_3 \subseteq \mathbb{F}_{3^2} = \mathbb{F}_9$ e il gruppo di Galois è C_2.

$q = 4$ Qui 4 non è primo, come gli altri, e quindi bisogna ingegnarsi. Il campo $\mathbb{F}_4$ suggerisce di considerare $\mathbb{F}_2 \subseteq \mathbb{F}_4$. Il caso $q = 2$ visto prima può aiutare:

$$\mathbb{F}_2 \subseteq \mathbb{F}_4 \subseteq \mathbb{F}_{64}.$$

L'estensione $\mathbb{F}_2 \subseteq \mathbb{F}_{64}$ è campo di spezzamento di f, e lo è quindi anche $\mathbb{F}_4 \subseteq \mathbb{F}_{64}$. Il gruppo di Galois di $\mathbb{F}_4 \subseteq \mathbb{F}_{64}$ è C_3. [Scrivere di $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ con $m \mid n$ e del suo gruppo di Galois.]

$q = 5$ [Da rivedere.] $\alpha \in \mathbb{F}_{5^d} \Rightarrow f(\alpha) = \mathcal{F}(\alpha) - \alpha + \bar{3} \Rightarrow f(a) = \bar{3} \neq \bar{0}$ se $a \in \mathbb{F}_5$ e $f(\alpha + a) = f(\alpha)\ \forall\, \alpha \in \mathbb{F}_{5^d}$ e $\forall\, a \in \mathbb{F}_5 \Rightarrow \mathbb{F}_{5^d} = \mathbb{F}_5(\alpha)$ se α radice di $f \Rightarrow d = \deg(\mathrm{m}_{\alpha,\mathbb{F}_5})$ non dipende dalla radice α di $f \Rightarrow f$ irriducibile in $\mathbb{F}_5[X]$ (non ha radici in $\mathbb{F}_5$ e non può essere $f = gh$ in $\mathbb{F}_5[X]$ con $\deg(g) = 2$ e $\deg(h) = 3$) $\Rightarrow d = 5$. □

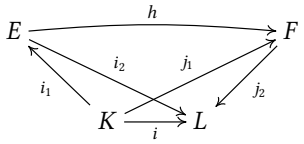
14 Corrispondenza di Galois

Definizione 14.1 (Campi intermedi)**.** Sia $i : K \to L$ un'estensione di campi. Un *campo intermedio* è il dato di un campo e di due estensioni

$$K \xrightarrow{i_1} E \xrightarrow{i_2} L$$

tali che $i = i_2 i_1$. Introduciamo anche una relazione tra due campi intermedi $K \xrightarrow{i_1} E \xrightarrow{i_2} L$ e $K \xrightarrow{j_1} F \xrightarrow{j_2} L$: diciamo che il primo è *contenuto* nel secondo

qualora esiste un omomorfismo $h : E \to F$ tale che $hi_1 = j_1$ e $j_2 h = i_2$.



(14.1)

Richiamiamo un risultato ricavato molto tempo fa, quello della formula (4.1). In generale, può non dire nulla sulla costituzione dei campi intermedi, ma può dare delle indicazioni sul grado dei campi intermedi o guidare ad una prima scrematura in certi casi. Richiamiamo questo fatto con il linguaggio della definizione di campo intermedio: se $i : K \to L$ è finito ed è assegnato il campo intermedio $K \xrightarrow{i_1} F \xrightarrow{i_2} L$, allora vale $[L : K] = [L : F][F : K]$.

Come sempre, quando si tratta di semplici inclusioni tutto il macchinario della definizione precedente passa inosservato: un campo intermedio è un campo F compreso tra due campi K e L, cioè $K \subseteq F \subseteq L$. Tuttavia, in un contesto generale può essere bene averci a che fare per almeno un po'. Ecco infatti la prima parte della corrispondenza di Galois.

[L'insieme dei campi intermedi insieme preordinato.]

Proposizione 14.2. Sia $i : K \to L$ un'estensione e $K \xrightarrow{i_1} E \xrightarrow{i_2} L$ e $K \xrightarrow{j_1} F \xrightarrow{j_2} L$ due campi intermedi. Se il primo è contenuto nel secondo, allora

$$\mathrm{Gal}\left(F \xrightarrow{j_2} L\right) \subseteq \mathrm{Gal}\left(E \xrightarrow{i_2} L\right).$$

In altre parole, abbiamo la funzione

$$\phi : \left\{\text{campi intermedi di } K \xrightarrow{i} L\right\} \to \left\{\text{sottogruppi di } \mathrm{Gal}\left(K \xrightarrow{i} L\right)\right\}$$
$$\phi\left(K \xrightarrow{i_2} E \xrightarrow{i_2} L\right) := \mathrm{Gal}\left(E \xrightarrow{i_2} L\right)$$

con le seguenti proprietà:

1. è una funzione antitòna
2. $\phi\left(K \xrightarrow{\mathrm{id}_K} K \xrightarrow{j} L\right) = \mathrm{Gal}\left(K \xrightarrow{j} L\right)$
3. $\phi\left(K \xrightarrow{i} L \xrightarrow{\mathrm{id}_L} L\right) = \{\mathrm{id}_L\}$.

L'enunciato è più difficile a scriversi che a dimostrarsi.

Dimostrazione. Sia $\sigma \in \mathrm{Gal}\left(F \xrightarrow{j_2} L\right)$, cioè $\sigma j_2 = j_2$. Sia $h : E \to F$ tale che $hi_1 = j_1$ e $j_2 h = i_2$ (teniamo sempre presente il diagramma (14.1) visto che manteniamo la stessa notazione). Allora

$$\sigma i_2 = \underbrace{\sigma j_2}_{= j_2} h = j_2 h = i_2.$$

Cioè $\sigma \in \mathrm{Gal}\left(E \xrightarrow{i_2} L\right)$. Il resto è solo banale verifica. □

[Fare esempi su come varia il gruppo di Galois di un'estensione $K \subseteq L$ al quando varia K. Forse troppo presto?]

L'altra metà della corrispondenza di Galois ha bisogno di nuove nozioni. Le introdurremo all'interno di una Proposizione che ricorda tanto quella precedente in alcuni aspetti.

Lemma 14.3 (Campo fisso)**.** Sia L un campo e G un sottogruppo di automorfismi di L (quindi non necessariamente automorfismi di una fissata estensione $i : K \to L$). Allora

$$L^G := \{a \in L \mid \sigma(a) = a \text{ per ogni } \sigma \in G\}$$

è un sottocampo di L, che noi chiameremo *campo fisso* di G.

Dimostrazione. La verifica che L^G è sottocampo di L è banale routine. □

Proposizione 14.4. Sia $i : K \to L$ un'estensione e G un sottogruppo di $\mathrm{Gal}\left(K \xrightarrow{i} L\right)$. Allora si ha il campo intermedio

$$K \xrightarrow{i_G} L^G \hookrightarrow L$$

in cui $i_G(r) := i(r)$ e la seconda estensione è una banale inclusione insiemistica. Inoltre, la funzione

$$\psi : \left\{\text{sottogruppi di } \mathrm{Gal}\left(K \xrightarrow{i} L\right)\right\} \to \left\{\text{campi intermedi di } K \xrightarrow{i} L\right\}$$
$$\psi(H) := \left(K \xrightarrow{i_H} L^H \hookrightarrow L\right)$$

ha le seguenti proprietà:

1. è antitòna
2. $\psi(\{e\})$ è il campo intermedio $K \xrightarrow{i} L$ stesso
3. Se $G = \mathrm{Gal}\left(K \xrightarrow{i} L\right)$, allora abbiamo il campo intermedio $K \xrightarrow{i_G} L^G \hookrightarrow L$ in cui non necessariamente i_G è un isomorfismo.

Dimostrazione. Siano ora $r \in K$ e $\sigma \in G \subseteq \mathrm{Gal}\left(K \xrightarrow{i} L\right)$ qualsiasi, l'immagine di K sotto i è contenuta in L^G perché da definizione di gruppo di Galois di $i : K \to L$ si ha $\sigma(i(r)) = i(r)$. Qui il lavoro per il controllo dell'antitonia è semplice. Siano H_1 e H_2 sottogruppi di $\mathrm{Gal}\left(K \xrightarrow{i} L\right)$ tali che $H_1 \subseteq H_2$: gli elementi di L^{H_2} sono gli elementi di L fissati da ogni $\sigma \in H_2$, e quindi a maggior ragione da ogni automorfismo in H_1. [Il punto 3?] □

Lemma 14.5 (di E. Artin)**.** Sia L campo e G un gruppo finito di automorfismi di L. Allora

$$\left[L : L^G\right] \leq |G|.$$

In particolare, se G è finito, allora pure l'estensione $L^G \subseteq L$ lo sarà. Questo è il caso, per esempio, se G è sottogruppo del gruppo di Galois di un'estensione $K \to L$ finita.

Dimostrazione. Consideriamo un generico gruppo finito $G = \{\sigma_1 = \mathrm{id}_L, \dots, \sigma_m\}$ di cardinalità m. Dobbiamo quindi mostrare che L come spazio vettoriale su L^G ha dimensione $\leq m$. Per quanto visto nel corso di Algebra Lineare, è sufficiente mostrare che ogni sottoinsieme $\{\alpha_1, \dots, \alpha_n\}$ di L con $m < n$ è linearmente dipendente. [Vedi il capitolo 3 di [Mil].] □

Proposizione 14.6. Sia G un gruppo finito di automorfismi di un campo L. Allora

$$G = \mathrm{Gal}\left(L^G \subseteq L\right).$$

Vale a dire ogni gruppo finito di automorfismi di campi è il gruppo di Galois di qualche estensione.

Dimostrazione. Abbiamo tutti gli strumenti per farlo.

$$\underbrace{\left[L : L^G\right] \leq |G|}_{\text{Lemma 14.5}} \leq \underbrace{\left|\mathrm{Gal}\left(L^G \subseteq L\right)\right| \leq \left[L : L^G\right]}_{\text{Proposizione 10.16}}.$$

G e $\mathrm{Gal}\left(L^G \subseteq L\right)$ hanno la stessa cardinalità finita, e quindi sono uguali. □

15 Esercizi 2

Esercizio 15.1 (Esercizio sul gruppo di Galois di $X^n - 2$)**.** $n > 1$, $\alpha := \sqrt[n]{2} \in \mathbb{R}_{>0}$, $\omega := e^{(2\pi i)/n} \in \mathbb{C}$, $G := \mathrm{Gal}_{\mathbb{Q}}(X^n - 2)$.

1. $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \omega)$ campo di spezzamento di $X^n - 2$.
2. n primo $\Rightarrow |G| = n\varphi(n) = n(n-1)$.
3. $n = 4$ o $6 \Rightarrow |G| = n\varphi(n)$.
4. $n = 8 \Rightarrow |G| < n\varphi(n)$.
5. $|G| = n\varphi(n) \Rightarrow G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$ con $\theta : \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n)$ isomorfismo.

Svolgimento. 1. Le radici in $\mathbb{C}$ di $X^n - 2$ sono $\alpha\omega^j$ per $j = 0, \dots, n-1 \Rightarrow$ il campo di spezzamento in $\mathbb{C}$ di $X^n - 2$ su $\mathbb{Q}$ è $L := \mathbb{Q}(\alpha\omega^j : j = 0, \dots, n-1) = \mathbb{Q}(\alpha, \omega)$.

2. $\mathbb{Q} \subseteq L$ di Galois, $G = \mathrm{Gal}_{\mathbb{Q}}(L) \Rightarrow |G| = [L : \mathbb{Q}]$.
   $X^n - 2$ irriducibile per Eisenstein $\Rightarrow \mathrm{m}_{\alpha,\mathbb{Q}} = X^n - 2 \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^n - 2) = n$.
   $\mathrm{m}_{\omega,\mathbb{Q}} = \Phi_n \Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n) = n - 1$.
   $\mathrm{mcd}(n, n-1) = 1 \Rightarrow [L : \mathbb{Q}] = n(n-1)$.
3. $\varphi(4) = \varphi(6) = 2 \Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) = 2 \Rightarrow n = \mathrm{mcm}(n, 2) \mid [L : \mathbb{Q}] \leq 2n$ $\Rightarrow [L : \mathbb{Q}] = 2n = n\varphi(n)$ (altrimenti $[L : \mathbb{Q}] = n \Rightarrow \omega \in L = \mathbb{Q}(\alpha) \subset \mathbb{R}$, assurdo).
4. $\omega = \sqrt{2}(1+i)/2$, $\omega^2 = i \Rightarrow \sqrt{2}\omega = 1 + i = 1 + \omega^2 \Rightarrow \omega$ radice di $X^2 - \sqrt{2}X + 1 \in \mathbb{Q}(\alpha)[X]$ (perché $\sqrt{2} = \alpha^4$) $\Rightarrow [L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2 \cdot 8 = 16 < 32 = 8\varphi(8)$.
5. $H := \mathrm{Gal}_{\mathbb{Q}(\alpha)}(L) < G$ tale che $|H| = |G|/[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(n)$, $H' := \mathrm{Gal}_{\mathbb{Q}(\omega)}(L) \lhd G$ (perché $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ normale) tale che $|H'| = |G|/[\mathbb{Q}(\omega) : \mathbb{Q}] = n$ e $H \cap H' = \{1\} \Rightarrow |(HH')| = n\varphi(n) = |G| \Rightarrow G = HH' \Rightarrow G = H' \rtimes H$.
   $H' = \{\sigma_{\bar{j}} : \bar{j} \in \mathbb{Z}/n\mathbb{Z}\}$ con $\sigma_{\bar{j}}(\alpha) = \alpha\omega^j$ (e $\sigma_{\bar{j}}(\omega) = \omega$) $\Rightarrow \sigma_{\bar{j}} = \sigma_{\bar{1}}^j$ $\forall\, \bar{j} \in \mathbb{Z}/n\mathbb{Z} \Rightarrow H' = \langle \sigma_{\bar{1}} \rangle \cong C_n$.
   $H \cong G/H' \cong \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong \mathbb{Z}/n\mathbb{Z}^* \Rightarrow G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$ con $\theta : \mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^*$ omomorfismo iniettivo (quindi isomorfismo) perché $\tau \in H \Rightarrow \exists\, \bar{l} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che $\tau(\omega) = \omega^l$ (e $\tau(\alpha) = \alpha$) $\Rightarrow \tau\sigma_{\bar{1}}\tau^{-1} = \sigma_{\bar{l}} = \sigma_{\bar{1}}$ $\Leftrightarrow \tau = 1$ □

Esercizio 15.2 (Polinomi con gruppo di Galois S_n)**.** K campo, $0 \neq f \in K[X]$ tale che $\deg(f) = n > 0$ e $\mathrm{Gal}_K(f) \cong S_n$;
α radice di f (in un campo di spezzamento L di f su K).

1. f è irriducibile in $K[X]$.
2. $n > 2 \Rightarrow \mathrm{Gal}_K(K(\alpha)) = \{1\}$.
3. $n > 3 \Rightarrow \alpha^n \notin K$.

Svolgimento. 1. $\mathrm{Gal}_K(f) \cong S_n \Rightarrow$ le radici $\alpha = \alpha_1 \dots, \alpha_n \in L$ di f sono distinte e $\forall\, i = 1, \dots, n\ \exists\, \sigma \in \mathrm{Gal}_K(f)$ tale che $\sigma(\alpha) = \alpha_i \Rightarrow \alpha_i$ radice di $\mathrm{m}_{\alpha,K} \Rightarrow f \mid \mathrm{m}_{\alpha,K} \Rightarrow f$ irriducibile.

2. $\sigma \in \mathrm{Gal}_K(K(\alpha)) \Rightarrow \exists\, i = 1, \dots, n$ tale che $\sigma(\alpha) = \alpha_i$, e basta dimostrare $i = 1$. Per assurdo $i = 2 \Rightarrow K(\alpha) \subseteq L$ campo di spezzamento di $\prod_{i=3}^{n}(X - \alpha_i)$ $\Rightarrow [L : K] = [L : K(\alpha)][K(\alpha) : K] \leq (n-2)!n < n!$, assurdo perché $[L : K] \geq |\mathrm{Gal}_K(L)| = n!$.

3. Per assurdo $\alpha^n = a \in K \Rightarrow$ posso supporre $f = X^n - a \Rightarrow L = K(\alpha, \omega)$ con $\langle \omega \rangle = \{\beta \in L : \beta^n = 1\} < L^* \Rightarrow [L : K] \leq [K(\alpha) : K][K(\omega) : K] \leq n(n-1) < n!$, assurdo. □