Algebra 2 — Teoria dei Campi

Sommario

Queste pagine partono dalle slides del corso di Algebra 2 tenuto negli anni 2020/2021 dal prof. Alberto Canonaco (alberto.canonaco@unipv.it), che si possono ancora reperire all'indirizzo https://www-dimat.unipv.it/canonaco/2020-2021/alg2.html. Tuttavia è bene tenere conto che:

- Ci sono integrazioni con note e corsi degli anni successivi. Per questo motivo, la presentazione del materiale ha subito dei cambiamenti e delle dimostrazioni sono state cambiate.
- Sono stati inseriti alcuni richiami più o meno estesi ad argomenti di Algebra 1.
- La bibliografia è estesa.

Importante: qua e là c'è ancora qualche retaggio delle vecchie slides e a volte il discorso può essere troncato nel mezzo. Spesso le notazioni sono incoerenti. Eventuali errori sono da attribuire a chi sta mantenendo queste note e sta facendo integrazioni.

Testi di riferimento

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

[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/.

Indice

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.

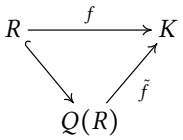
Proposizione 1.6. Sia R un anello con divisione e S un anello non banale. Allora ogni omomorfismo $f : R \to S$ è iniettivo.

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

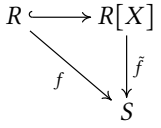
$$\deg(p + q) = \max\{\deg p, \deg q\}$$

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

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

[Scrivere del funtore di $(\ )_* : \mathbf{CRing} \to \mathbf{CRing}$.]

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.

[Inserire esempi.]

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. Implicazione $(1) \Rightarrow (2)$. 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. Implicazione $(2) \Rightarrow (1)$. 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.

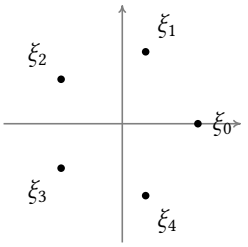


Figura 1. Le radici quinte di 1 sul piano di Argand-Gauss.

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:

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

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

Definizione 3.6 (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*.

Vediamo qualche esempio di estensione generata che sarà importante anche per il seguito.

Esempio 3.7. 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 3.8. Considerando l'inclusione $\mathbb{Q} \subseteq \mathbb{C}$, sai dire se $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}\right)$?

Proposizione 3.9. Sia $i : K \to L$ un'estensione e $\alpha_1, \dots, \alpha_n \in L$, con $n \geq 2$. Allora

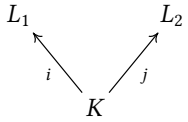
$$K\left(\alpha_1, \dots, \alpha_{n-1}, \alpha_n\right) = K\left(\alpha_1, \dots, \alpha_{n-1}\right)\left(\alpha_n\right).$$

Dimostrazione. Esercizio. □

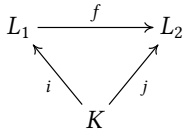
Cioè le estensioni finitamente generate possono essere introdotte iterativamente a partire dalla costruzione di estensione semplice.

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 3.10 (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

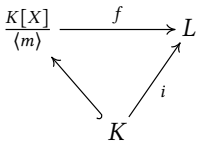


Per dire più concretamente come sono fatte un certo tipo di estensioni semplici serve un po' di lavoro preliminare.

Proposizione 3.11. 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



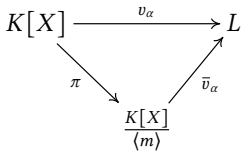
commuta e $f(X + \langle m \rangle) = \alpha$. In particolare, f ha immagine $K(\alpha)$ e quindi

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

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 3.12. 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 3.13. 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 3.14. 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 3.15. 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 3.16. [Riscrivere: introdurre un terzo campo L' e conteggiare il numero di morfismi di estensioni $K(\alpha) \to L'$ invece.] Sia $i : K \to L$ una estensione e $\alpha \in L$ con polinomio minimo $m \in K[X]$. Allora esiste una biezione

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

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. Vediamo qualche conseguenza di questo fatto.

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

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

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 $[L : F] = mn$. □

Osservazione 4.3.
- $[L : K]$ non va confuso con l'indice di $K < L$.
- $[L : K] > 0$ e $[L : K] = 1 \Leftrightarrow K = L$.

Esempio 4.4.
- $[\mathbb{C} : \mathbb{R}] = 2$ perché $\{1, i\}$ è una $\mathbb{R}$-base di $\mathbb{C}$.
- $[K(X) : K] = \infty$ perché $\{X^n : n \in \mathbb{N}\} \subset K[X] \subset K(X)$ è K-linearmente indipendente.

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

Esempio 4.5. 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 3.11.

Proposizione 4.6. 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 3.13 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 4.7. 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 4.8. Un'estensione $K \subseteq L$ è detta *algebrica* quando ogni elemento di L è algebrico su K.

Proposizione 4.9. 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. Proviamo le implicazioni $1 \Rightarrow 2$, $2 \Rightarrow 3$ e $3 \Rightarrow 1$.

$1 \Rightarrow 2$ 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

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

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

Proposizione 4.10. 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 $[F(\alpha) : F] < \infty$. □

5 Esercizi

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 4.6 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

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

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 $\alpha := \sqrt{2} + \sqrt{3}$.

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

   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 4.6 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. □

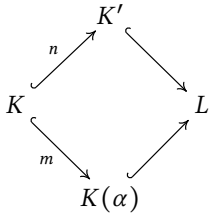
Esercizio 5.3 (Problema 399 di [Tsu])**.** Dimostra che $X^3 - 2$ è irriducibile sul campo $\mathbb{Q}(i)$.

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. $\left[K_f : K\right] \leq (\deg f)!$.

Dimostrazione. Procediamo 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. Quindi il polinomio f visto come elemento di $E[X]$ è fattorizzabile come

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

Quest'ultimo ha grado $\deg f - 1$ e quindi, per induzione esiste un campo di spezzamento $E \subseteq L := E(\alpha_2, \dots, \alpha_n)$ in cui $f_1 = (X - \alpha_2) \cdots (X - \alpha_n)$ con $\alpha_2, \dots, \alpha_n \in L$. Ecco la fattorizzazione in $L[X]$ di f:

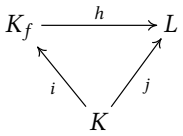
$$f = (X - \alpha_1) \cdots (X - \alpha_n).$$

Da costruzione, $L = E(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. 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 $h : K_f \to L$

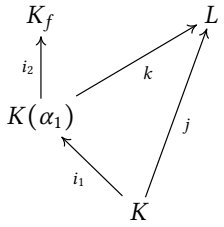


se e solo se f si spezza su L. In particolare, il campo di spezzamento di un polinomio non nullo è unico a meno di isomorfismi.

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. [Rileggere ed espandere alcune parti.] 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. □

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.

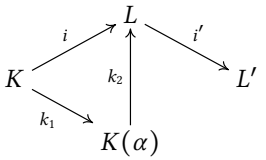
Dimostrazione. (1 ⇒ 2) Sia $f \in K[X]$ irriducibile e indichiamo con $\alpha \in L$ una delle sue radici. Siano $g \in K[X]$ monico e $c \in K^*$ tali che $f = cg$. Ora α è radice di g e g è irriducibile: quindi, grazie alla Proposizione 2.11, g è proprio il polinomio minimo di α. Assumendo (1), possiamo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

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

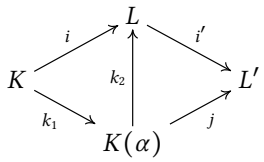
Proposizione 8.3. Un'estensione finita è normale se e solo se è il campo di spezzamento di un polinomio non nullo.

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. (⇒) Esercizio.
(⇐) 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:



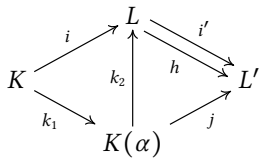
Qui introduciamo notazioni: k_1 manda $r \in K$ in $i(k)$ mentre k_2 è una mera inclusione insiemistica. Se $\beta \in L'$ è una delle radici di $m \in K[X]$, allora possiamo costruire un morfismo di estensioni $j : K(\alpha) \to L'$ da k_2 a $i'i$ che manda α in β:



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

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

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 $\gcd(f, g) = 1$, allora $\gcd(i_*(f), i_*(g)) = 1$, 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. $\gcd(f, f') = 1$.

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 $\gcd(f, f') = 1$, 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 $\gcd(f, f') = 1$ perché f è irriducibile. Quindi f è separabile. Viceversa, se f è separabile, allora $\gcd(f, f') = 1$, 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 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 $\alpha_1, \dots, \alpha_n \in L$ algebrici. Se i polinomi minimi degli α_i sono separabili, allora l'estensione $K \subseteq L$ è separabile.

Dimostrazione. Per induzione su n. Consideriamo l'estensione $K \subseteq L = K(\alpha_1)$ e $\beta \in L$. [Da scrivere.] □

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

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

Dimostrazione. [Da scrivere.] □

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 problemi in molti casi concreti.

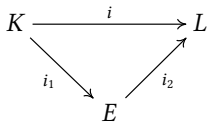
Definizione 10.2. Sia K un campo, e $f \in K[X]$ non nullo. Il *gruppo di Galois* di f su K è il gruppo di Galois di un campo di spezzamento per f. Viene indicato molto semplicemente come $\mathrm{Gal}(f)$.

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.

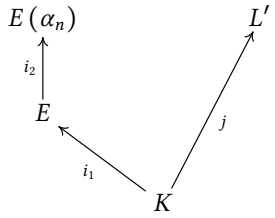
Il gruppo di Galois può essere un oggetto piuttosto difficile da calcolare in generale, mentre noi ci limiteremo ad una classe di estensioni per cui si possono avere degli strumenti e delle indicazioni. Il lemma che segue riguarda il numero di morfismi di estensioni da un'estensione finita.

Lemma 10.3. 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 $\leq [L : K]$. 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.

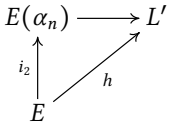
Dimostrazione. Andiamo per induzione su $n := [L : K]$. Il caso base, $n = 1$, significa che $L \cong K$ come campi e quindi il morfismo di estensioni da i a j è l'unico che può esserci, cioè ji^{-1}. Possiamo quindi supporre che $n > 0$ per il passo induttivo. In questo caso, a causa della Proposizione 4.9, esistono $\alpha_1, \dots, \alpha_n \in L$ algebrici tali che $L = K(\alpha_1, \dots, \alpha_n)$. Introduciamo il campo $E := K(\alpha_1, \dots, \alpha_{n-1})$, quindi in particolare $L = E(\alpha_n)$. 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 3.16, 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. [Riscrivere meglio e provare il se e solo se.] □

Proposizione 10.4 (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 $K \subseteq L$ è anche normale e separabile.

Dimostrazione. $\mathrm{Gal}_K(L)$ è il gruppo dei morfismi di estensione dall'estensione $K \subseteq L$ in sé. Quindi si applica il lemma di sopra. [Più dettagli.] □

Quindi il gruppo di Galois di un'estensione finita è finito: l'interesse per i gruppi di ordine finito risiede anche in questo. Esistono estensioni il cui gruppo di Galois è infinito.

Esempio 10.5 ($\mathbb{Q} \subseteq \overline{\mathbb{Q}}$)**.** [Scrivere.]

Definizione 10.6. Un'estensione è detta *di Galois* qualora è finita, normale e separabile. Equivalentemente, un'estensione è di Galois quando è separabile e campo di spezzamento di un qualche polinomio non nullo.

La Proposizione 10.4 fornisce 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 $\mathrm{Gal}_K(L)$.

Prima di fare i primi esempi, indugiamo sui gruppi di Galois di estensioni finite par farci un'idea su come siano fatti gli automorfismi di questo tipo di estensioni.

Lemma 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 $i_*(f)(\phi(\alpha)) = \phi(i_*(f)(\alpha))$. Quindi in particolare, gli zeri di f vengono mandati negli zeri di f.

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

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

□

Proposizione 10.8. Sia $i : K \to L$ un'estensione finitamente generata, cioè $L = K(\alpha_1, \dots, \alpha_n)$ per degli $\alpha_1, \dots, \alpha_n \in L$. Allora ogni $\phi \in \mathrm{Gal}_K(L)$ è univocamente determinato da $\phi(\alpha_1), \dots, \phi(\alpha_n)$.

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. □

Corollario 10.9. Sia $i : K \to L$ un'estensione finitamente generata, cioè $L = K(\alpha_1, \dots, \alpha_n)$ per degli $\alpha_1, \dots, \alpha_n \in L$. Allora $\mathrm{Gal}_K(L)$ è isomorfo ad un sottogruppo di S_n.

E qui è chiaro anche come mai ci sia un interesse verso i gruppi simmetrici S_n e i suoi sottogruppi: sostanzialmente gli elementi di $\mathrm{Gal}_K(L)$ sono permutazioni degli α_i. Ne riparleremo sicuramente in seguito, per ora facciamo degli esempi.

Esempio 10.10 (Gruppo di Galois di $\mathbb{Q} \subseteq \mathbb{Q}(i)$)**.** [Scrivere.]

11 Il teorema fondamentale

[Riscrivere la parte su come $\mathrm{Gal}_K(L)$ agisce sull'insieme delle radici.]

G gruppo, X G-insieme $\Rightarrow$

$$X^G := \{x \in X : gx = x \ \forall\, g \in G\} \subseteq X.$$

L campo, $G < \mathrm{Gal}(L) \Rightarrow$

$$L^G = \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall\, \sigma \in G\} \subseteq L$$

sottocampo (detto *campo fisso* di G).

Osservazione 11.1. $F \subseteq L$ sottocampo primo $\Rightarrow F \subseteq L^{\mathrm{Gal}(L)}$ (perché $L^{\mathrm{Gal}(L)} \subseteq L$ sottocampo) $\Rightarrow \mathrm{Gal}_F(L) = \mathrm{Gal}(L)$.

Teorema 11.2 (Artin)**.** L campo, $G < \mathrm{Gal}(L)$ finito $\Rightarrow [L : L^G] \leq |G|$.

Dimostrazione. $|G| = m$, $G = \{\sigma_1 = \mathrm{id}_L, \dots, \sigma_m\}$.

Dati $\alpha_1, \dots, \alpha_n \in L$ distinti con $n > m$, basta dimostrare che $\{\alpha_1, \dots, \alpha_n\}$ è linearmente dipendente su L^G. $v_j := (\sigma_1(\alpha_j), \dots, \sigma_m(\alpha_j)) \in L^m$ (per $j = 1, \dots, n$) distinti.

$\{v_1, \dots, v_n\}$ linearmente dipendente su L (perché $n > m$) $\Rightarrow$

$$W := \{(\beta_1, \dots, \beta_n) \in L^n : \sum_{j=1}^{n} \beta_j v_j = 0\}$$

L-sottospazio vettoriale non nullo di L^n.

$\sigma \in G$, $(\beta_1, \dots, \beta_n) \in W \Rightarrow (\sigma(\beta_1), \dots, \sigma(\beta_n)) \in W$: $(\beta_1, \dots, \beta_n) \in W \Leftrightarrow \sum_{j=1}^n \beta_j \sigma_i(\alpha_j) = 0 \ \forall\, i = 1, \dots, m \Rightarrow \sum_{j=1}^n \sigma(\beta_j)(\sigma \circ \sigma_i)(\alpha_j) = 0 \ \forall\, i = 1, \dots, m \Leftrightarrow (\sigma(\beta_1), \dots, \sigma(\beta_n)) \in W$ perché $\{\sigma \circ \sigma_1, \dots, \sigma \circ \sigma_m\} = G$.

$(\gamma_1, \dots, \gamma_n) \in W \setminus \{0\}$ ($\Rightarrow \exists\, j_0 \in \{1, \dots, n\}$ tale che $\gamma_{j_0} \neq 0$ e posso supporre $\gamma_{j_0} = 1$) con il minimo numero di componenti $\neq 0$.

$\sigma \in G \Rightarrow \delta_j := \gamma_j - \sigma(\gamma_j)$ tali che $(\delta_1, \dots, \delta_n) \in W$ e $\delta_j = 0$ se $\gamma_j = 0$ o $j = j_0 \Rightarrow (\delta_1, \dots, \delta_n) = 0$ per l'ipotesi su $(\gamma_1, \dots, \gamma_n) \Rightarrow \gamma_j = \sigma(\gamma_j) \in L^G$ (per $j = 1, \dots, n$) tali che $\sum_{j=1}^n \gamma_j \alpha_j = 0$ perché $\sum_{j=1}^n \gamma_j \sigma_1(\alpha_j) = 0$ e $\sigma_1 = \mathrm{id}_L$. □

L campo $\Rightarrow$ le funzioni

$$\phi : \{K : K \subseteq L \text{ sottocampo}\} \to \{G : G < \mathrm{Gal}(L)\} \quad K \mapsto \mathrm{Gal}_K(L)$$
$$\psi : \{G : G < \mathrm{Gal}(L)\} \to \{K : K \subseteq L \text{ sottocampo}\} \quad G \mapsto L^G$$

soddifano le seguenti proprietà:

1. $K' \subseteq K \subseteq L$ sottocampi $\Rightarrow \phi(K) \subseteq \phi(K')$ (cioè $\mathrm{Gal}_K(L) < \mathrm{Gal}_{K'}(L)$);
2. $G' < G < \mathrm{Gal}(L) \Rightarrow \psi(G) \subseteq \psi(G')$ (cioè $L^G \subseteq L^{G'}$);
3. $K \subseteq L$ sottocampo $\Rightarrow K \subseteq \psi(\phi(K))$ (cioè $K \subseteq L^{\mathrm{Gal}_K(L)}$);
4. $G < \mathrm{Gal}(L) \Rightarrow G \subseteq \phi(\psi(G))$ (cioè $G < \mathrm{Gal}_{L^G}(L)$).

Segue formalmente che valgono queste ulteriori proprietà:

5. $K \subseteq L$ sottocampo $\Rightarrow \phi(K) = \phi(\psi(\phi(K)))$ (cioè $\mathrm{Gal}_K(L) = \mathrm{Gal}_{L^{\mathrm{Gal}_K(L)}}(L)$) perché $\phi(K) \subseteq \phi(\psi(\phi(K)))$ per iv e $K \subseteq \psi(\phi(K))$ per iii, quindi $\phi(\psi(\phi(K))) \subseteq \phi(K)$ per i;
6. $G < \mathrm{Gal}(L) \Rightarrow \psi(G) = \psi(\phi(\psi(G)))$ (cioè $L^G = L^{\mathrm{Gal}_{L^G}(L)}$).

Da v e vi segue anche che $\phi|_{\mathrm{im}(\psi)} : \mathrm{im}(\psi) \to \mathrm{im}(\phi)$ è biunivoca con inversa $\psi|_{\mathrm{im}(\phi)} : \mathrm{im}(\phi) \to \mathrm{im}(\psi)$, dove $\mathrm{im}(\psi) = \{L^G : G < \mathrm{Gal}(L)\}$ e $\mathrm{im}(\phi) = \{\mathrm{Gal}_K(L) : K \subseteq L \text{ sottocampo}\}$.

Teorema 11.3. 1. $G < \mathrm{Gal}(L)$ finito $\Rightarrow [L : L^G] = |G|$, $L^G \subseteq L$ di Galois e $G = \mathrm{Gal}_{L^G}(L)$.
2. $K \subseteq L$ estensione finita $\Rightarrow |\mathrm{Gal}_K(L)| \leq [L : K]$ e vale l'uguaglianza $\Leftrightarrow K \subseteq L$ di Galois $\Leftrightarrow K = L^{\mathrm{Gal}_K(L)}$.

Corollario 11.4.

$$\{K : K \subseteq L \text{ di Galois}\} \to \{G : G < \mathrm{Gal}(L) \text{ finito}\} \quad K \mapsto \mathrm{Gal}_K(L)$$
$$\{G : G < \mathrm{Gal}(L) \text{ finito}\} \to \{K : K \subseteq L \text{ di Galois}\} \quad G \mapsto L^G$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre $K \subseteq L$ di Galois $\Rightarrow |\mathrm{Gal}_K(L)| = [L : K]$.

Dimostrazione. Sappiamo già che:

1' $G < \mathrm{Gal}(L)$ finito $\Rightarrow [L : L^G] \leq |G|$;
2' $K \subseteq L$ estensione finita $\Rightarrow |\mathrm{Gal}_K(L)| \leq [L : K]$ e vale l'uguaglianza $\Leftrightarrow K \subseteq L$ di Galois.

1. Per 1' $[L : L^G] \leq |G| < \infty$.
   Per iv $G < \mathrm{Gal}_{L^G}(L)$, e quindi $|G| \leq |\mathrm{Gal}_{L^G}(L)|$.
   Per 2' $|\mathrm{Gal}_{L^G}(L)| \leq [L : L^G]$.
   Dunque $[L : L^G] = |G| = |\mathrm{Gal}_{L^G}(L)|$ (per cui $G = \mathrm{Gal}_{L^G}(L)$) e, ancora per 2', $L^G \subseteq L$ di Galois.
2. Per iii $K \subseteq L^{\mathrm{Gal}_K(L)}$.
   Per 2' $|\mathrm{Gal}_K(L)| \leq [L : K] < \infty$.
   Per 1 $L^{\mathrm{Gal}_K(L)} \subseteq L$ di Galois e $[L : L^{\mathrm{Gal}_K(L)}] = |\mathrm{Gal}_K(L)|$.
   Dunque, se $K = L^{\mathrm{Gal}_K(L)}$, allora $K \subseteq L$ è di Galois.
   Viceversa, se $K \subseteq L$ è di Galois, allora, sempre per 2', $[L : K] = |\mathrm{Gal}_K(L)| = [L : L^{\mathrm{Gal}_K(L)}]$, da cui segue $K = L^{\mathrm{Gal}_K(L)}$. □

Ricordiamo che, fissato un campo L,

$$\{K : K \subseteq L \text{ di Galois}\} \to \{G : G < \mathrm{Gal}(L) \text{ finito}\} \quad K \mapsto \mathrm{Gal}_K(L)$$
$$\{G : G < \mathrm{Gal}(L) \text{ finito}\} \to \{K : K \subseteq L \text{ di Galois}\} \quad G \mapsto L^G$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre $K \subseteq L$ di Galois $\Rightarrow |\mathrm{Gal}_K(L)| = [L : K]$.

Teorema 11.5 (Il teorema fondamentale)**.** $K \subseteq L$ estensione di Galois, $G := \mathrm{Gal}_K(L)$. Allora

$$\{F : K \subseteq F \subseteq L \text{ sottocampo}\} \to \{H : H < G\} \quad F \mapsto \mathrm{Gal}_F(L)$$
$$\{H : H < G\} \to \{F : K \subseteq F \subseteq L \text{ sottocampo}\} \quad H \mapsto L^H$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre, se $K \subseteq F \subseteq L$ è un sottocampo, allora

1. $F \subseteq L$ di Galois e $|\mathrm{Gal}_F(L)| = [L : F]$;
2. $K \subseteq F$ normale $\Leftrightarrow H := \mathrm{Gal}_F(L) \lhd G \Rightarrow \mathrm{Gal}_K(F) \cong G/H$.

Dimostrazione.
- La prima parte e il punto 1 seguono da quanto già visto, tenendo conto che $K \subseteq F \subseteq L$ sottocampo $\Rightarrow F \subseteq L$ di Galois (perché $K \subseteq L$ di Galois).
- Per dimostrare il punto 2, ricordiamo che $K \subseteq F$ è normale (e quindi di Galois) $\Leftrightarrow F$ è G-stabile.
- $K \subseteq F$ normale $\Rightarrow f : G \to \mathrm{Gal}_K(F)$, $\sigma \mapsto \sigma|_F$ ben definita. Chiaramente f omomorfismo e $\ker(f) = H$, per cui $H \lhd G$ e $G/H \cong \mathrm{im}(f)$ per il primo teorema di isomorfismo. Inoltre

$$|\mathrm{im}(f)| = |(G/H)| = \frac{|G|}{|H|} = \frac{|[L : K]|}{|[L : F]|} = [F : K] = |\mathrm{Gal}_K(F)|,$$

  $\Rightarrow f$ suriettiva e $\mathrm{Gal}_K(F) \cong G/H$.
- $H \lhd G \Rightarrow \sigma(\alpha) \in F \ \forall\, \sigma \in G$ e $\forall\, \alpha \in F$ (quindi $K \subseteq F$ normale): $\sigma(\alpha) \in F = L^H$ $\Leftrightarrow \tau(\sigma(\alpha)) = \sigma(\alpha) \ \forall\, \tau \in H \Leftrightarrow (\sigma^{-1}\tau\sigma)(\alpha) = \alpha \ \forall\, \tau \in H$, vero perché $\sigma^{-1}\tau\sigma \in H$ e $\alpha \in F = L^H$.

□

Esempio 11.6. $K := \mathbb{Q}$ e $L := \mathbb{Q}(\sqrt[3]{2}, \omega)$ con $1 \neq \omega \in \mathbb{C}$ tale che $\omega^3 = 1$.

- $\mathbb{Q} \subset L$ di Galois (è campo di spezzamento di $X^3 - 2$) e $G := \mathrm{Gal}_{\mathbb{Q}}(L) = \mathrm{Gal}(L)$ tale che $|G| = [L : \mathbb{Q}] = 6$.

- $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ non normale $\Rightarrow \mathrm{Gal}_{\mathbb{Q}(\sqrt[3]{2})}(L) < G$ non normale $\Rightarrow G \cong S_3$.
- $\exists! H \lhd G$ non banale (di ordine 3) $\Rightarrow [L : L^H] = 3$, $\mathbb{Q} \subset L^H$ normale e $\mathrm{Gal}_{\mathbb{Q}}\left(L^H\right) \cong G/H \cong C_2 \Rightarrow L^H = \mathbb{Q}(\omega)$.
- G ha anche 3 sottogruppi non normali non banali (di ordine 2), che corrispondono a $\mathbb{Q}(\omega^i \sqrt[3]{2})$ per $i = 0, 1, 2$.

Osservazione 11.7.
- $K \subseteq L$ di Galois $\Rightarrow |\{F : K \subseteq F \subseteq L \text{ sottocampo}\}| < \infty$ perché coincide con $|\{H : H < \mathrm{Gal}_K(L)\}|$.
- $K \subseteq L$ finita $\Rightarrow |\mathrm{Gal}_K(L)| \leq [L : K] < \infty \Rightarrow L^{\mathrm{Gal}_K(L)} \subseteq L$ di Galois e $|\mathrm{Gal}_K(L)| = [L : L^{\mathrm{Gal}_K(L)}] \mid [L : K]$ (perché $K \subseteq L^{\mathrm{Gal}_K(L)} \subseteq L$, quindi $[L : K] = [L : L^{\mathrm{Gal}_K(L)}][L^{\mathrm{Gal}_K(L)} : K]$).

12 Campi finiti

K campo finito $\Rightarrow \mathrm{char}(K) = p$ primo.

$0 < n := [K : \mathbb{F}_p] < \infty \Rightarrow K \cong \mathbb{F}_p^n$ come $\mathbb{F}_p$-spazio vettoriale (quindi $K \cong C_p^n$ come gruppo abeliano) $\Rightarrow |K| = p^n$.

Teorema 12.1. $\forall\, p$ primo e $\forall\, n > 0$ $\exists!$ a meno di isomorfismo un campo $\mathbb{F}_{p^n}$ di ordine p^n; inoltre $\mathbb{F}_{p^n}$ è campo di spezzamento di $X^{p^n} - X$ su $\mathbb{F}_p$.

Dimostrazione. $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ campo di spezzamento di $X^{p^n} - X \Rightarrow$

$R := \{\alpha \in \mathbb{F}_{p^n} : \alpha \text{ radice di } X^{p^n} - X\} = \{\alpha \in \mathbb{F}_{p^n} : \mathcal{F}^n(\alpha) = \alpha\}$ sottocampo di $\mathbb{F}_{p^n} \Rightarrow \mathbb{F}_{p^n} = \mathbb{F}_p(R) = R$.

$(X^{p^n} - X)' = -1$ non ha radici $\Rightarrow X^{p^n} - X$ non ha radici multiple $\Rightarrow \left|\mathbb{F}_{p^n}\right| = |R| = \deg(X^{p^n} - X) = p^n$.

K altro campo di ordine $p^n \Rightarrow \alpha^{p^n - 1} = 1\ \forall\, \alpha \in K^*$ (per il teorema di Lagrange) $\Rightarrow$ ogni elemento di K è radice di $X^{p^n} - X \Rightarrow \prod_{\alpha \in K}(X - \alpha) \mid (X^{p^n} - X) \Rightarrow X^{p^n} - X = \prod_{\alpha \in K}(X - \alpha) \Rightarrow \mathbb{F}_p \subseteq K$ campo di spezzamento di $X^{p^n} - X$. □

Se $n, m > 0$, esiste un'estensione $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n \mid m$:

$\Rightarrow$ $d := [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] \Rightarrow \mathbb{F}_{p^m} \cong \mathbb{F}_{p^n}^d$ (come $\mathbb{F}_{p^n}$-spazi vettoriali) $\Rightarrow p^m = \left|\mathbb{F}_{p^m}\right| = \left|\mathbb{F}_{p^n}^d\right| = (p^n)^d = p^{nd} \Rightarrow m = nd$;

$\Leftarrow$ $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} = \mathcal{F}^n(\alpha) = \alpha\} \subseteq \mathbb{F}_{p^m}$ perché, se $\mathcal{F}^n(\alpha) = \alpha$, allora $\mathcal{F}^m(\alpha) = (\mathcal{F}^n)^{m/n}(\alpha) = \alpha$.

Corollario 12.2. $n \mid m \Rightarrow \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ di Galois e $\mathrm{Gal}_{\mathbb{F}_{p^n}}\left(\mathbb{F}_{p^m}\right) = \langle \mathcal{F}^n \rangle \cong C_{m/n}$.

Dimostrazione. $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ è di Galois perché campo di spezzamento di $X^{p^m} - X$ (e $\mathbb{F}_{p^n}$ è perfetto) $\Rightarrow \left|\mathrm{Gal}_{\mathbb{F}_{p^n}}\left(\mathbb{F}_{p^m}\right)\right| = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = m/n$.

$\mathbb{F}_{p^n} = \{\alpha \in \mathbb{F}_{p^m} : \mathcal{F}^n(\alpha) = \alpha\} \Rightarrow \mathcal{F}^n \in \mathrm{Gal}_{\mathbb{F}_{p^n}}\left(\mathbb{F}_{p^m}\right)$, e basta dimostrare $\mathrm{ord}(\mathcal{F}^n) \geq m/n$, cioè $\mathrm{ord}(\mathcal{F}) \geq m$ in $\mathrm{Gal}\left(\mathbb{F}_{p^m}\right)$, vero perché $0 < i < m \Rightarrow \left|\{\alpha \in \mathbb{F}_{p^m} : \mathcal{F}^i(\alpha) = \alpha^{p^i} = \alpha\}\right| \leq p^i < p^m \Rightarrow \mathcal{F}^i \neq \mathrm{id}_{\mathbb{F}_{p^m}}$. □

p primo, $n > 0$, $q := p^n$, $0 \neq f \in \mathbb{F}_q[X]$, $G := \mathrm{Gal}_{\mathbb{F}_q}(f)$.

- f irriducibile, $d := \deg(f) \Rightarrow \mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di f ($\Rightarrow G \cong C_d$):

  $\alpha \in \overline{\mathbb{F}}_p$ radice di $f \Rightarrow [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d \Rightarrow \mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$.

- in generale $f = \prod_{i=1}^{k} f_i$ con f_i irriducibile, $d_i := \deg(f_i)\ \forall\, i = 1,\dots,k \Rightarrow d := \mathrm{mcm}(d_1,\dots,d_k)$ tale che $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di f ($\Rightarrow G \cong C_d$):
  per il punto precedente $\mathbb{F}_{q^{d_i}}$ è campo di spezzamento di f_i su $\mathbb{F}_q$, quindi f si spezza su $\mathbb{F}_{q^{d'}} \Leftrightarrow \mathbb{F}_{q^{d_i}} \subseteq \mathbb{F}_{q^{d'}}\ \forall\, i = 1,\dots,k \Leftrightarrow d_i \mid d'\ \forall\, i = 1,\dots,k \Leftrightarrow d \mid d'$.

  $n > 0$, $\mathrm{char}(K) \nmid n$, $K \subseteq L$ campo di spezzamento di $X^n - 1$.

- $(X^n - 1)' = nX^{n-1} \neq 0$ ha solo la radice 0 (che non è radice di $X^n - 1$) $\Rightarrow$ $X^n - 1$ non ha radici multiple in $L \Rightarrow R := \{\alpha \in L : \alpha^n = 1\}$ tale che $|R| = n$.
- $R < L^* \Rightarrow R$ ciclico $\Rightarrow \exists\, \omega \in R$ tale che $R = \langle\omega\rangle$ (quindi $\mathrm{ord}(\omega) = n$ in L^*, e si dice che ω è una radice n-esima *primitiva* dell'unità; per esempio $\omega = e^{(2\pi i)/n}$ se $K \subseteq \mathbb{C}$).
- $L = K(R) = K(\omega) \Rightarrow |\mathrm{Gal}_K(L)| = |R'|$ con $R' := \{\alpha \in L : \mathrm{m}_{\omega,K}(\alpha) = 0\} \subseteq R$ (perché $\mathrm{m}_{\omega,K} \mid (X^n - 1)$).
- $\mathrm{m}_{\omega,K}$ si spezza su L e non ha radici multiple $\Rightarrow |\mathrm{Gal}_K(L)| = \deg(\mathrm{m}_{\omega,K}) = [L : K] \Rightarrow K \subseteq L$ di Galois.
- La funzione $\mathrm{Gal}_K(L) \to \mathrm{Aut}(R) < S(R)$, $\sigma \mapsto \sigma|_R$ è ben definita e è un omomorfismo iniettivo di gruppi.
- $\mathrm{Gal}_K(X^n - 1) = \mathrm{Gal}_K(L) \cong G < \mathbb{Z}/n\mathbb{Z}^* \cong \mathrm{Aut}(R) \Rightarrow G$ abeliano e $|G| \mid \varphi(n)$.

$\alpha \in R' \Rightarrow \exists\, \sigma \in \mathrm{Gal}_K(L)$ tale che $\alpha = \sigma(\omega) \Rightarrow \mathrm{ord}(\alpha) = \mathrm{ord}(\omega) = n \Rightarrow \exists\, \bar{j} \in \mathbb{Z}/n\mathbb{Z}^*$ tale che $\alpha = \omega^j \Rightarrow$

$$\mathrm{m}_{\omega,K} = \prod_{\alpha \in R'} (X - \alpha) \mid \Phi_n := \prod_{\bar{j} \in \mathbb{Z}/n\mathbb{Z}^*} (X - \omega^j) \in L[X],$$

dove Φ_n è detto n-esimo *polinomio ciclotomico*. Chiaramente

$$\Phi_n \mid (X^n - 1) = \prod_{\bar{j} \in \mathbb{Z}/n\mathbb{Z}} (X - \omega^j)$$

e $\deg(\Phi_n) = \varphi(n)$.

Teorema 12.3. 1. $\Phi_n \in K[X]$.
2. $K = \mathbb{Q} \Rightarrow \Phi_n \in \mathbb{Q}[X]$ irriducibile.

Corollario 12.4. $\mathrm{m}_{\omega,\mathbb{Q}} = \Phi_n$ e $\mathrm{Gal}_{\mathbb{Q}}(X^n - 1) \cong \mathbb{Z}/n\mathbb{Z}^*$.

13 Discriminante

- K campo, $0 \neq f \in K[X]$, $K \subseteq L$ campo di spezzamento di f.
- $n := \deg(f)$, $\alpha_1,\dots,\alpha_n \in L$ radici di $f \Rightarrow$

$$\delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in L$$

  è ben definito a meno del segno (dipende dall'ordine delle radici), e chiaramente $\delta \neq 0 \Leftrightarrow f$ non ha radici multiple.
- Il *discriminante* di f è $\Delta = \Delta(f) := \delta^2 \in L$ (ben definito e tale che $\Delta \neq 0 \Leftrightarrow f$ non ha radici multiple).

Osservazione 13.1. $\sigma(\delta) = \varepsilon(\sigma|_R)\delta$ (con $R := \{\alpha_1, \dots, \alpha_n\}$) $\forall\, \sigma \in \mathrm{Gal}_K(f) = \mathrm{Gal}_K(L)$:

posso supporre $\delta \neq 0$ (quindi $|R| = n$), e allora per definizione di segno di una permutazione in $S(R) \cong S_n$

$$\sigma(\delta) = \prod_{1\le i<j\le n} (\sigma(\alpha_i) - \sigma(\alpha_j)) = \prod_{1\le i<j\le n} (\sigma|_R(\alpha_i) - \sigma|_R(\alpha_j)) = \varepsilon(\sigma|_R)\delta.$$

Proposizione 13.2. K perfetto $\Rightarrow \Delta = \Delta(f) \in K$. Se inoltre $\mathrm{char}(K) \neq 2$, f non ha radici multiple e identifico $\mathrm{Gal}_K(f)$ a un sottogruppo di $S_n \cong S(R)$, allora $\mathrm{Gal}_K(f) \subseteq A_n \Leftrightarrow \delta \in K \Leftrightarrow \Delta$ è un quadrato in K.

Dimostrazione.
- $K \subseteq L$ di Galois $\Rightarrow K = L^{\mathrm{Gal}_K(L)}$. Dunque, dato $\alpha \in L$, $\alpha \in K \Leftrightarrow \sigma(\alpha) = \alpha\ \forall\, \sigma \in \mathrm{Gal}_K(L) = \mathrm{Gal}_K(f)$.
- $\sigma(\Delta) = \sigma(\delta^2) = \sigma(\delta)^2 = (\varepsilon(\sigma|_R)\delta)^2 = \varepsilon(\sigma|_R)^2\delta^2 = \delta^2 = \Delta\ \forall\, \sigma \in \mathrm{Gal}_K(f) \Rightarrow \Delta \in K$.
- $\mathrm{Gal}_K(f) \subseteq A_n \Rightarrow \sigma(\delta) = \delta\ \forall\, \sigma \in \mathrm{Gal}_K(f) \Rightarrow \delta \in K$.
- $\delta \in K$, f senza radici multiple $\Rightarrow \delta \in K^*$ e $\forall\, \sigma \in \mathrm{Gal}_K(f)\ \delta = \sigma(\delta) = \varepsilon(\sigma|_R)\delta \Rightarrow \varepsilon(\sigma|_R)_K = 1_K \Rightarrow \varepsilon(\sigma|_R) = 1$ (cioè $\mathrm{Gal}_K(f) \subseteq A_n$) se $\mathrm{char}(K) \neq 2$.
- Chiaramente $\delta \in K \Leftrightarrow \Delta = \delta^2$ è un quadrato in K.

□

- Si può dimostrare che $\Delta(f)$ è esprimibile come polinomio valutato nei coefficienti di f.
- $\Delta(X^2 + aX + b) = a^2 - 4b$:

  $X^2 + aX + b = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta \Rightarrow a = -\alpha - \beta$, $b = \alpha\beta$;

  $\delta = \alpha - \beta \Rightarrow \Delta = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = a^2 - 4b$.
- $\Delta(X^3 + aX + b) = -4a^3 - 27b^2$:

  $X^3 + aX + b = (X - \alpha)(X - \beta)(X - \gamma) = X^3 - (\alpha + \beta + \gamma)X^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)X - \alpha\beta\gamma \Rightarrow \alpha + \beta + \gamma = 0$, $a = \alpha\beta + \alpha\gamma + \beta\gamma$, $b = -\alpha\beta\gamma \Rightarrow a = -(\alpha^2 + \alpha\beta + \beta^2)$, $b = \alpha\beta(\alpha + \beta)$;

  $\delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = (\alpha - \beta)(2\alpha + \beta)(\alpha + 2\beta) = 2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3 \Rightarrow \Delta = (2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3)^2 = 4\alpha^6 + 12\alpha^5\beta - 3\alpha^4\beta^2 - 26\alpha^3\beta^3 - 3\alpha^2\beta^4 + 12\alpha\beta^5 + 4\beta^6 = -4a^3 - 27b^2$.

K perfetto, $\mathrm{char}(K) \neq 2$, $\deg(f) = 3$, f irriducibile in $K[X] \Rightarrow \mathrm{Gal}_K(f) \cong \begin{cases} C_3 & \text{se } \Delta(f) \text{ è un quadrato in } K \\ S_3 & \text{altrimenti.} \end{cases}$

Esempio 13.3.
- $f = X^3 - 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (non ha radici in $\mathbb{Q}$) $\Rightarrow \Delta = -4(-3)^3 - 27 \cdot 1^2 = 81 = 9^2 \Rightarrow \mathrm{Gal}_{\mathbb{Q}}(f) \cong C_3$.
- $f = X^3 + 3X + 1$ irriducibile in $\mathbb{Q}[X]$ (non ha radici in $\mathbb{Q}$) $\Rightarrow \Delta = -4 \cdot 3^3 - 27 \cdot 1^2 = -135 < 0 \Rightarrow \mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$.

Osservazione 13.4. $\mathrm{char}(K) \neq 3$, $f(X) = X^3 + aX^2 + bX + c \in K[X] \Rightarrow$ con la sostituzione $X = Y - a/3$ si ottiene $f(X) = f(Y - a/3) =: g(Y)$ con $g(Y) = Y^3 + a'Y + b' \in K[Y]$. Chiaramente $\alpha \in L$ (campo di spezzamento di f su K) è radice di $g \Leftrightarrow \alpha - a/3$ è radice di $f \Rightarrow L$ è campo di spezzamento di g su $K \Rightarrow \mathrm{Gal}_K(f) \cong \mathrm{Gal}_K(g)$.

14 Esercizi di riepilogo

Esercizio 14.1. Determinare il gruppo di Galois G di $f := X^5 - X + 3$ su $\mathbb{F}_q$ per $q = 2, 3, 4, 5$.

Svolgimento. In ogni caso $G \cong C_d$ se $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ campo di spezzamento di f, e $d = \operatorname{mcm}(d_1, \dots, d_r)$ se $f = \prod_{i=1}^r f_i$ con $f_1, \dots, f_r$ irriducibili.

$q = 2$ f non ha radici (perché $f(\bar{0}) = f(\bar{1}) = \bar{1}$), ma è divisibile per $X^2 + X + 1$ (l'unico irriducibile di grado 2 in $\mathbb{F}_2[X]$) e risulta $f = (X^2+X+1)(X^3+X^2+1)$ $\Rightarrow d = \operatorname{mcm}(2, 3) = 6$.

$q = 3$ $f = X^5 - X = X(X-1)(X+1)(X^2+1) \Rightarrow d = 2$.

$q = 4$ $\mathbb{F}_{2^6=4^3}$ campo di spezzamento di f su $\mathbb{F}_2 \Rightarrow$ anche su $\mathbb{F}_4 \Rightarrow d = 3$.

$q = 5$ $\alpha \in \mathbb{F}_{5^d} \Rightarrow f(\alpha) = \mathcal{F}(\alpha) - \alpha + \bar{3} \Rightarrow f(a) = \bar{3} \neq \bar{0}$ 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 $\deg(h) = 3$) $\Rightarrow d = 5$. □

Esercizio 14.2 (Esercizio sul gruppo di Galois di $X^n - 2$)**.** $n > 1$, $\alpha := \sqrt[n]{2} \in \mathbb{R}_{>0}$, $\omega := e^{(2\pi i)/n} \in \mathbb{C}$, $G := \operatorname{Gal}_{\mathbb{Q}}(X^n - 2)$.

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 $\theta : \mathbb{Z}/n\mathbb{Z}^* \to \operatorname{Aut}(C_n)$ 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, $G = \operatorname{Gal}_{\mathbb{Q}}(L) \Rightarrow |G| = [L : \mathbb{Q}]$.
   $X^n - 2$ irriducibile per Eisenstein $\Rightarrow \mathrm{m}_{\alpha,\mathbb{Q}} = X^n - 2 \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^n - 2) = n$.
   $\mathrm{m}_{\omega,\mathbb{Q}} = \Phi_n \Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n) = n - 1$.
   $\operatorname{mcd}(n, n-1) = 1 \Rightarrow [L : \mathbb{Q}] = n(n-1)$.
3. $\varphi(4) = \varphi(6) = 2 \Rightarrow [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) = 2 \Rightarrow n = \operatorname{mcm}(n, 2) \mid [L : \mathbb{Q}] \leq 2n$ $\Rightarrow [L : \mathbb{Q}] = 2n = n\varphi(n)$ (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. $H := \operatorname{Gal}_{\mathbb{Q}(\alpha)}(L) < G$ tale che $|H| = |G|/[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(n)$, $H' := \operatorname{Gal}_{\mathbb{Q}(\omega)}(L) \lhd G$ (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 $\sigma_{\bar{j}}(\omega) = \omega$) $\Rightarrow \sigma_{\bar{j}} = \sigma_{\bar{1}}^j$ $\forall\, \bar{j} \in \mathbb{Z}/n\mathbb{Z} \Rightarrow H' = \langle \sigma_{\bar{1}} \rangle \cong C_n$.
   $H \cong G/H' \cong \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong \mathbb{Z}/n\mathbb{Z}^* \Rightarrow G \cong C_n \rtimes_\theta \mathbb{Z}/n\mathbb{Z}^*$ con $\theta : \mathbb{Z}/n\mathbb{Z}^* \to \operatorname{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^*$ 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 14.3 (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. □

Esercizio 14.4 (Gruppi di Galois di polinomi biquadratici)**.** Determinare campo di spezzamento $\mathbb{Q} \subseteq L$ e gruppo di Galois G di f su $\mathbb{Q}$ nei seguenti casi:

1. $f = X^4 - 4X^2 + 2$;
2. $f = X^4 - 4X^2 - 2$.

Svolgimento. 1. f irriducibile per Eisenstein.
$f(X) = g(X^2)$ con $g(Y) := Y^2 - 4Y + 2$ che ha radici $2 \pm \sqrt{2} \in \mathbb{R}_{>0} \Rightarrow$ le radici di f sono $\pm\alpha, \pm\beta$ con $\alpha := \sqrt{2 + \sqrt{2}}, \beta := \sqrt{2 - \sqrt{2}} \in \mathbb{R}_{>0} \Rightarrow L = \mathbb{Q}(\alpha, \beta)$.
$\alpha^2 - 2 = \sqrt{2} = \alpha\beta \Rightarrow \beta = (\alpha^2 - 2)/\alpha \in \mathbb{Q}(\alpha) \Rightarrow L = \mathbb{Q}(\alpha) \Rightarrow |G| = [L : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 4$.
$\exists\, \sigma \in G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ tale che $\sigma(\alpha) = \beta$ (perché β radice di $\mathrm{m}_{\alpha,\mathbb{Q}} = f$) $\Rightarrow$

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

$\Rightarrow \sigma^2 \neq \mathrm{id}_L \Rightarrow G \cong C_4$.

2. f irriducibile per Eisenstein.
$f(X) = g(X^2)$ con $g(Y) := Y^2 - 4Y - 2$ che ha radici $2 \pm \sqrt{6} \in \mathbb{R} \Rightarrow$ le radici di f sono $\pm\alpha, \pm\beta i$ con $\alpha := \sqrt{\sqrt{6} + 2}, \beta := \sqrt{\sqrt{6} - 2} \in \mathbb{R}_{>0} \Rightarrow L = \mathbb{Q}(\alpha, \beta i)$.
$\alpha\beta = \sqrt{2} \Rightarrow \alpha\beta i = \sqrt{2}i \Rightarrow L = \mathbb{Q}(\alpha, \sqrt{2}i)$.
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 4$, $[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}] = \deg(\mathrm{m}_{\sqrt{2}i,\mathbb{Q}}) = 2$ (perché $\mathrm{m}_{\sqrt{2}i,\mathbb{Q}} = X^2 + 2$) $\Rightarrow$

$$\mathrm{mcm}(4, 2) = 4 \mid |G| = [\mathbb{Q}(\alpha, \sqrt{2}i) : \mathbb{Q}] \leq 4 \cdot 2 = 8$$

e non può essere $[\mathbb{Q}(\alpha, \sqrt{2}i) : \mathbb{Q}] = 4$ (perché $\sqrt{2}i \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$) $\Rightarrow |G| = 8$.
$G \cong G' < S_4 \Rightarrow G \cong D_4$. □