CORSO DI ALGEBRA 2

FABRIZIO CASELLI

Contents

Premessa

Queste note sono gli appunti del docente per le lezioni e NON sostituiscono i libri consigliati e sono state redatte per venire incotro agli studenti in mancanza di un libro di testo unico seguito durante il corso. Contengono alcune (poche) cose non trattate in aula e mancano di tanti particolari che invece sono stati visti a lezione. Sfogliare e leggere più libri è sempre una buona prassi quando si studia matematica. È molto probabile che questi appunti contengano numerosi errori e chiedo ai miei studenti-lettori di segnalarmeli.

1. Richiami sui gruppi

L'algebra è la branca della matematica che si occupa dello studio di insiemi con operazioni che soddisfano certe condizioni. Solitamente si considerano insiemi concreti che godono di determinate proprietà in comune e si cerca di uniformarli in un'unica teoria che li racchiuda.

Esempio 1.1. Le trasformazioni lineari invertibili di uno spazio vettoriale, le isometrie di uno spazio metrico, le permutazioni di un insieme sono insiemi in cui è definita un'operazione (di composizione) che soddisfa certe condizioni. Questa osservazione porta in modo naturale alla definizione di gruppo vista nel corso del primo anno e che ora andiamo a richiamare.

Definizione. Sia A un insieme. Un'*operazione binaria* su A è una funzione $A \times A \to A$ che ad ogni coppia ordinata di elementi di A associa un elemento di A.

Definizione. Un insieme G si dice *gruppo* se è dotato di un'operazione binaria $(g, h) \mapsto gh$ tale che

- (esistenza dell'elemento neutro): esiste $e \in G$ tale che $ge = eg = g$ per ogni $g \in G$;
- (proprietà associativa): $(gh)k = g(hk)$ per ogni $g, h, k \in G$;
- (esistenza dell'elemento inverso) per ogni $g \in G$ esiste $h \in G$ tale che $gh = hg = e$.

Ricordiamo senza verificarlo che in un gruppo l'elemento neutro è unico, che l'inverso è unico, e che vale la legge di cancellazione, cioè se $g, g', h \in G$ sono tali che $gh = g'h$ o $hg = hg'$ allora $g = g'$.

Un gruppo G si dice *abeliano* se $gh = hg$ per ogni $h, g \in G$.

Non richiamiamo la definizione di sottogruppo, ma ricordiamo invece il seguente criterio.

Esercizio 1.2. Un sottoinsieme non vuoto H di un gruppo G è un sottogruppo se e solo se $gh^{-1} \in H$ per ogni $h, g \in H$.

La cardinalità di un gruppo finito si dice *ordine* del gruppo e un celebre teorema di Lagrange afferma che se H è un sottogruppo di un gruppo finito G allora l'ordine di H divide l'ordine di G.

Se g è un elemento di un gruppo G diciamo che g ha *ordine finito* se esiste $n > 0$ tale che $g^n = e$. Il più piccolo intero positivo n che soddisfa questa condizione si dice ordine (o periodo) di g e si indica con $o(g)$.

Osserviamo che se $g^n = e$ per qualche $n \in \mathbb{Z}$ allora $o(g)|n$. Infatti siano $q, r \in \mathbb{Z}$, con $0 \leq r < o(g)$ tali che $n = qo(g) + r$; allora

$$e = g^n = g^{o(g)q+r} = (g^{o(g)})^q g^r = g^r$$

e quindi, per minimalità di $o(g)$ abbiamo $r = 0$.

I gruppi più semplici che possiamo considerare, e che ci saranno più utili durante il corso sono i cosiddetti gruppi ciclici.

Definizione. Un gruppo G si dice *ciclico* se esiste un elemento $g \in G$ tale che

$$G = \{g^n : n \in \mathbb{Z}\}.$$

Scriviamo in tal caso $G = \langle g \rangle$.

Le potenze di un qualunque elemento di un gruppo qualsiasi formano sempre un sottogruppo ciclico. Se G è un gruppo diciamo che g è un generatore di G, o che g genera G se $G = \langle g \rangle$. Osserviamo che un gruppo ciclico può avere più di un generatore.

Esempio 1.3. L'insieme $G = \{1, -1, i, -i\} \subset \mathbb{C}^*$ con l'operazione di prodotto è un gruppo ciclico. E infatti ha due generatori i e $-i$ in quanto $G = \langle i \rangle = \langle -i \rangle$.

Lemma 1.4. *Se G è un gruppo ciclico generato da un elemento g di ordine finito allora G è finito e si ha $|G| = o(g)$.*

Proof. Poniamo $d = o(g)$ e consideriamo un elemento generico $h \in G$. Allora per definizione esiste $a \in \mathbb{Z}$ tale che $h = g^a$. Effettuando la divisione con resto (in $\mathbb{Z}$) di a per d abbiamo che esistono due interi q ed r con $0 \leq r \leq d-1$ tali che $a = qd + r$. Abbiamo quindi

$$h = g^a = g^{qd+r} = (g^d)^q g^r = g^r.$$

Deduciamo che gli elementi di G sono $e = g^0, g^1, \ldots, g^{d-1}$. Questi d elementi sono tutti distinti tra loro: infatti se $g^i = g^j$ con $0 \leq i < j \leq d-1$ allora $g^j = g^i g^{j-i}$ da cui, per la legge di cancellazione, avremmo $g^{j-i} = e$ contraddicendo l'ipotesi $o(g) = d$. □

Diamo per buoni i concetti di omomorfismi e di isomorfismi tra gruppi.

Esercizio 1.5. Due gruppi ciclici finiti aventi lo stesso ordine sono isomorfi.

Le classi resto modulo n formano, con l'operazione di somma, l'unico gruppo ciclico di ordine n, a meno di isomorfismo. Anche le radici n-esime dell'unità con l'operazione di prodotto formano un altro modello concreto per il gruppo ciclico di ordine n.

Ci poniamo ora alcune domande sulla struttura dei gruppi ciclici. Quanti sono i generatori? Quanti e quali i sottogruppi? Possiamo caratterizzare i gruppi ciclici in termini di sottogruppi?

Vediamo intanto quali e quanti sono i generatori di un gruppo ciclico.

Proposizione 1.6. *Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n. I generatori di G sono gli elementi della forma g^i con $0 < i < n$ e $MCD(i, n) = 1$. I generatori di un gruppo ciclico di ordine n sono quindi $\phi(n)$, dove ϕ indica la funzione di Eulero.*

Proof. Un elemento generico di G è della forma g^i con $0 \leq i < n$ in quanto g è un generatore ed ha ordine n. L'elemento g^i è a sua volta un generatore se e solo se ha ordine n. Sia $d = MCD(i, n)$. Abbiamo

$$(g^i)^{n/d} = (g^n)^{i/d} = e$$

e quindi l'ordine di g^i è al più n/d. Se $d > 1$, di conseguenza, g^i non può essere generatore di G.

Viceversa, se $d = 1$ sia m l'ordine di g^i. Allora $g^{mi} = e$ e quindi $n | mi$. E siccome $MCD(n, i) = 1$ deduciamo che $n | m$ e quindi, siccome l'ordine di un elemento di G non può superare n, abbiamo $n = m$. □

Proseguiamo studiando i sottogruppi di un gruppo ciclico.

Proposizione 1.7. *Sia $G = \langle g \rangle$ un gruppo ciclico, $|G| = n$ e d un divisore di n. Allora esiste un unico sottogruppo H di G di ordine d. Tale sottogruppo è ciclico ed è generato da $g^{n/d}$.*

Proof. Esistenza: l'elemento $g^{n/d}$ genera un sottogruppo di ordine d:

$$\langle g^{n/d} \rangle = \{g^{n/d}, g^{2n/d}, g^{3n/d}, \dots, g^{dn/d} = e\}.$$

Unicità. Sia H un sottogruppo di ordine d. Sia $i > 0$ minimo tale che $g^i \in H$. Mostriamo intanto che $i|n$. Altrimenti avremmo $k = MCD(i, n) < i$ e per l'identità di Bèzout esistono due interi a e b tali che $k = ai + bn$ e avremmo quindi $g^k = g^{ai+bn} = g^{ai} = (g^i)^a \in H$ contraddicendo la minimalità di i. Abbiamo quindi che H contiene le n/i potenze distinte di g^i. Lasciamo al lettore di verificare che H non può contenere altri elementi e quindi $n/i = d$. □

Corollario 1.8. *Per ogni $n > 0$ abbiamo*

$$n = \sum_{d|n} \phi(d).$$

Proof. Per le Proposizioni 1.6 e 1.7 gli elementi di ordine d in un gruppo ciclico di ordine n sono $\phi(d)$: essi sono infatti i generatori dell'unico sottogruppo ciclico di ordine d. Il risultato segue. □

L'ultima proprietà che vogliamo mostrare è lievemente più sottile e può essere vista come un'inversione della Proposizione 1.7.

Proposizione 1.9. *Sia G un gruppo finito di ordine n. Supponiamo che per ogni divisore d di n esista al più un sottogruppo di ordine d. Allora G è ciclico.*

Proof. Per ogni $d|n$ poniamo $m(d)$ il numero di elementi di G aventi ordine d. Abbiamo chiaramente

$$n = \sum_{d|n} m(d).$$

Se per assurdo il gruppo non fosse ciclico avremmo $m(n) = 0$ e quindi, confrontando l'identità qui sopra con il Corollario 1.8 esisterebbe $d|n$ tale che $m(d) > \phi(d)$. Sia quindi $g \in G$ un elemento di ordine d. Il sottogruppo $\langle g \rangle$ ha ordine d e contiene quindi esattamente $\phi(d)$ elementi di ordine d. Esiste quindi almeno un altro elemento g' di ordine d che non appartiene a $\langle g \rangle$. Il sottogruppo $\langle g' \rangle$ generato da g' è quindi un altro sottogruppo di ordine d e questo contraddice le ipotesi. □

2. Anelli commutativi

La principale struttura algebrica che vogliamo studiare in questo corso è quella di anello. Questa si ottiene uniformando ed astraendo delle strutture algebriche che ben conosciamo come $\mathbb{Z}$ (i numeri interi), $\mathbb{R}[X]$ (polinomi a coefficienti reali), $M(n; \mathbb{R})$ (matrici quadrate $n \times n$ a coefficienti reali): in questi esempi possiamo sommare, sottrarre, moltiplicare. Tuttavia non è possibile "dividere".

Definizione. Un *anello* è un insieme A con due operazioni binarie $+ : (a,b) \mapsto a+b$ e $\cdot : (a,b) \mapsto a \cdot b$ dette di somma e prodotto tali che

- (A è un gruppo additivo abeliano) A con l'operazione binaria $+$ forma un gruppo abeliano;
- (il prodotto è associativo) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ per ogni $a, b, c \in A$;
- (proprietà distributiva) $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot c$ per ogni $a, b, c \in A$.

Dato un anello A denotiamo con 0 l'elemento neutro rispetto alla somma e con $-a$ l'elemento inverso di a rispetto alla somma. Abbiamo le seguenti proprietà basilari.

Lemma 2.1. *Sia A un anello, $a, b \in A$. Allora*

- $-(-a) = a$;
- $a \cdot 0 = 0$;
- $-(a+b) = -a + (-b)$;
- $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$;

Dimostrazione. La prima segue dal fatto che in un gruppo l'inverso dell'inverso è l'elemento stesso. La seconda dal calcolo di $a \cdot (0+0)$ più la proprietà distributiva e la legge di cancellazione in un gruppo. La terza dal fatto che la somma è commutativa. La quarta dalla proprietà distributiva. □

Osservazione. Osserviamo che in un anello non vale la legge di cancellazione rispetto al prodotto: cioè non è vero che se $a \cdot b = a \cdot c$, anche con $a \neq 0$, allora $b = c$. Ed in particolare non è vero che se $a \cdot b = 0$ allora almeno uno tra a e b è 0. Ad esempio in $M(2, \mathbb{R})$ abbiamo

$$\begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} -3 & 2 \\ 4 & -2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}.$$

Definizione. Un anello A si dice *commutativo* se $a \cdot b = b \cdot a$ per ogni $a, b \in A$. Un anello A si dice *unitario* se esiste un elemento $u \in A$ tale che $u \cdot a = a \cdot u = a$ per ogni $a \in A$.

Lemma 2.2. *Se A è un anello unitario allora esiste un unico elemento $u \in A$ tale che $u \cdot a = a \cdot u = a$ per ogni $a \in A$. Tale elemento verrà semplicemente indicato con il simbolo 1.*

Dimostrazione. Se u' è un altro elemento che soddisfa la stessa condizione avremmo $uu' = u = u'$. □

Esempio 2.3. Abbiamo che $\mathbb{Z}$ è commutativo unitario, $2\mathbb{Z}$ è commutativo non unitario, $M(n, \mathbb{R})$ è unitario ma non commutativo, $M(n, 2\mathbb{Z})$ non è né commutativo né unitario.

Avvertenza: in questo corso con il termine anello indichiamo sempre un anello commutativo unitario, a meno che non venga diversamente indicato.

Esempio 2.4. Esiste un anello con un solo elemento, che sarà sia 0 che 1. Tale anello verrà detto *anello banale*. Osserviamo che non esistono altri anelli in cui $0 = 1$. Infatti, se A è un anello in cui $0 = 1$ e $a \in A$ allora $a = a \cdot 1 = a \cdot 0 = 0$ per il Lemma 2.1.

Notazione importante. Se $m \in \mathbb{Z}$ poniamo

$$ma = \begin{cases} a + a \cdots + a \, (m \text{ volte}) & \text{se } m > 0, \\ (-a) + (-a) + \cdots + (-a) (-m \text{ volte}) & \text{se } m < 0, \\ 0 & \text{se } m = 0. \end{cases}$$

L'elemento $m1$ verrà semplicemente indicato con m. Questa notazione non crea confusione in quanto chiaramente $m1 + n1 = (m + n)1$ e $m1 \cdot n1 = (mn)1$ e per ogni $a \in A$ abbiamo $m1 \cdot a = m \cdot a = ma$ (fare tutte le verifiche del caso!). Abbiamo quindi che l'elemento ma (se $m > 0$) può essere interpretato sia come la somma di m volte a che come il prodotto tra a e la somma di m volte 1.

Potrà ben accadere che se $m, n \in \mathbb{Z}$, abbiamo $m = n \in A$ anche se $m \neq n \in \mathbb{Z}$. Consideriamo ad esempio l'anello con due elementi $A = \{0, 1\}$. In questo anello tutte le operazioni sono univocamente determinate e in particolare $1 + 1 = 0$ (altrimenti $1 + 1 = 1$ e per la legge di cancellazione della somma avremmo $0 = 1$) Chi è $3 \in A$? Abbiamo per definizione $3 = 1 + 1 + 1 = 0 + 1 = 1 \in A$.

Alcune formule che siamo abituati ad utilizzare come le seguenti continuano a valere negli anelli (commutativi).

Proposizione 2.5. *Sia A un anello, $a, b \in A$, $n \in \mathbb{N}$. Abbiamo*

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

e

$$a^{n+1} - b^{n+1} = (a - b) \sum_{k=0}^{n} a^k b^{n-k}.$$

Dimostrazione. Entrambe sono di facile verifica: la prima per induzione utilizzando ad esempio la formula di Stifel, mentre per la seconda è sufficiente utilizzare la proprietà distributiva. Fare attenzione che entrambe le formule non valgono se il prodotto non è commutativo! □

Definizione. Se A è un anello, un *sottoanello* di A è un sottoinsieme che contiene 1 e che sia a sua volta un anello rispetto alle stesse operazioni di somma e prodotto di A.

Esempio 2.6. $\mathbb{Q}$ è un anello. Per ogni $n > 0$ e per ogni p numero primo abbiamo che i sottoinsiemi di $\mathbb{Q}$

$$\mathbb{Z}[1/n] = \left\{ \frac{a}{n^k} : \, a \in \mathbb{Z}, \, k \in \mathbb{N} \right\}$$

e

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : \, a, b \in \mathbb{Z}, \, p \not| b \right\}$$

sono anche dei sottoanelli.

Un esempio fondamentale è dato da $\mathbb{Z}_m$, l'insieme degli interi modulo m. Sappiamo già che $\mathbb{Z}_m$ è un gruppo abeliano (anzi ciclico) rispetto alla somma. Se $x \in \mathbb{Z}$, indicheremo solitamente ancora con x la sua classe in $\mathbb{Z}_m$. Se invece abbiamo bisogno di distinguere tra

l'elemento x e la sua classe utilizzeremo la notazione $[x]$ o $[x]_m$ per indicare la classe di x modulo m.

Vogliamo dare a $\mathbb{Z}_m$ la struttura di anello utilizzando il prodotto in $\mathbb{Z}$, vogliamo cioè poter definire il prodotto tra due classi come la classe del prodotto di due rappresentanti. L'unico problema che può insorgere è che tale prodotto non sia ben definito. Affrontiamo questo problema in un contesto più generale.

Definizione. Sia A un anello, $\mathcal{P} = \{A_i\}_{i\in I}$ una partizione di A e $\sim$ la relazione d'equivalenza associata a $\mathcal{P}$. Diciamo che $\mathcal{P}$ (o che $\sim$) è *compatibile* se per ogni $a, a', b, b' \in A$ tali che $a \sim a'$ e $b \sim b'$ si ha

$$a + b \sim a' + b',\ a \cdot b \sim a' \cdot b'.$$

Proposizione 2.7. *Sia A un anello e $\sim$ una relazione d'equivalenza compatibile. Allora l'insieme quoziente $A/\sim$ dato dalle classi di equivalenza è ancora un anello con le operazioni di somma e prodotto ereditate da A.*

Dimostrazione. Lasciata al lettore. □

Corollario 2.8. *$\mathbb{Z}_m$ è un anello.*

Dimostrazione. Sappiamo che $\mathbb{Z}_m$ è l'insieme quoziente rispetto alla relazione d'equivalenza data dalla congruenza modulo m. Basta quindi verificare che se $a \equiv a' \mod m$ e $b \equiv b' \mod m$ allora $a + b \equiv a' + b' \mod m$ e $ab \equiv a'b' \mod m$, e questo è una semplice verifica. □

L'anello $\mathbb{Z}_m$ ci offre un esempio per cui è necessario richiedere che l'elemento 1 faccia parte di un sottoanello. Infatti, ad esempio, se consideriamo l'anello $\mathbb{Z}_6$ possiamo osservare che il sottoinsieme $\{0, 3\}$ con le operazioni ristrette da $\mathbb{Z}_6$ è un anello unitario. Tuttavia non è un sottoanello perché non contiene 1.

3. Domini e campi

Definizione. Sia A un anello e $a \in A$, $a \neq 0$. Diciamo che a è un divisore dello 0 se esiste $b \in A$, $b \neq 0$ tale che $a \cdot b = 0$

Esempio 3.1. In $\mathbb{Z}_{12}$ abbiamo che 8 è un divisore dello 0. Infatti $8 \cdot 3 = 0$.

Definizione. Sia A un anello e $a \in A$, $a \neq 0$. Diciamo che a soddisfa la legge di cancellazione se per ogni $b, c \in A$ tali che $ab = ac$ si ha necessariamente $b = c$.

In questa definizione e spesso nel seguito, omettiamo il simbolo $\cdot$ per indicare il prodotto tra due elementi di un anello A.

Proposizione 3.2. *Sia A un anello e $a \in A$, $a \neq 0$. Allora a soddisfa la legge di cancellazione se e solo se non è un divisore dello 0.*

Dimostrazione. Supponiamo che a soddisfi la legge di cancellazione. Sia b tale che $ab = 0$; allora $ab = a \cdot 0$ e quindi, per la legge di cancellazione $b = 0$. Viceversa, se a non è divisore dello zero siano b, c tali che $ab = ac$. Ma allora $ab - ac = a(b - c) = 0$ da cui $b = c$. □

In questa dimostrazione e spesso nel seguito scriviamo $a - b$ anziché $a + (-b)$.

Proposizione 3.3. *Sia $a \in \mathbb{Z}$ e $a \neq 0 \in \mathbb{Z}_m$. Allora a è un divisore dello 0 in $\mathbb{Z}_m$ se e solo se a e m non sono coprimi.*

Proof. Se a e m sono coprimi e $b \in \mathbb{Z}$ è tale che $ab = 0 \in \mathbb{Z}_m$ abbiamo che $m|ab$ e quindi $m|b$ da cui $b = 0 \in \mathbb{Z}_m$.

Viceversa se a e m non sono coprimi abbiamo che esiste $d \in \mathbb{Z}$, $d \neq 0, 1 \in \mathbb{Z}_m$ tale che $d|a$ e $d|m$. Allora $m/d \neq 0 \in \mathbb{Z}_m$ e $a \cdot m/d = a/d \cdot m = 0 \in \mathbb{Z}_m$ e quindi a sarebbe un divisore dello 0 in $\mathbb{Z}_m$. □

Definizione. Un *dominio d'integrità*, o più semplicemente *dominio*, è un anello non banale in cui non ci sono divisori dello zero.

Corollario 3.4. *L'anello $\mathbb{Z}_m$ è un dominio se e solo se m è primo.*

Dimostrazione. Per la Proposizione 3.3 abbiamo che se m non è primo ogni divisore di m diverso da 1 e m è un divisore dello zero. Viceversa, se m è primo non esistono interi non multipli di m che non sono coprimi con m e quindi non esistono divisori dello zero. □

Definizione. Sia A un anello, $a \in A$. Diciamo che a è *invertibile*, o che è un'*unità*, se esiste $b \in A$ tale che $ab = 1$.

Proposizione 3.5. *L'insieme degli elementi invertibili di un anello A è un gruppo (con l'operazione di prodotto) che denotiamo con $\mathcal{U}(A)$.*

Proof. $1 = 1 \cdot 1$ e quindi $1 \in \mathcal{U}(A)$. Se a, a' sono invertibili siano b, b' tali che $ab = a'b' = 1$; allora aa' è invertibile in quanto $aa'(bb') = 1$ e quindi $\mathcal{U}(A)$ è chiuso rispetto al prodotto. L'esistenza dell'elemento inverso è tautologica e la proprietà associativa vale perché siamo in un anello. □

Esempio 3.6. Gli invertibili di $\mathbb{Z}[1/p]$, di $\mathbb{Z}_{(p)}$ di $\mathbb{Z}_m$ sono...

Proposizione 3.7. *Un elemento invertibile non è un divisore dello 0 e viceversa un divisore dello 0 non è invertibile. Se u è un elemento invertibile l'elemento inverso di u è unico e viene denotato con u^{-1}.*

Proof. Supponiamo per assurdo che u sia un elemento invertibile e un divisore dello 0. Allora esistono $v, a \in A$, $a \neq 0$ tali che $uv = 1$ e $ua = 0$. Allora $v0 = vua = a$ da cui $a = 0$ contraddicendo le ipotesi.

Per la seconda parte sia quindi u un elemento invertibile. Per la prima parte e la Proposizione 3.2 u soddisfa la legge di cancellazione e quindi, se esistono v e v' tali che $uv = uv' = 1$, abbiamo necessariamente $v = v'$. □

Definizione. Un *corpo* è un anello unitario (non necessariamente commutativo) in cui $0 \neq 1$ e in cui ogni elemento non nullo è invertibile. Un *campo* è un corpo commutativo.

Non avremo modo in questo corso di studiare la teoria dei corpi. Ci limitiamo nel prossimo esempio a costruire il più famoso corpo non commutativo.

Esempio 3.8. Consideriamo uno spazio vettoriale reale di dimensione 4 che denotiamo con Q avente per base gli elementi $1, i, j, k$. Ogni elemento di Q si esprime quindi formalmente in modo unico nella forma $a1 + bi + cj + dk$, con $a, b, c, d \in \mathbb{R}$. Su Q consideriamo il prodotto ottenuto imponendo che 1 sia l'elemento neutro, $i^2 = j^2 = k^2 = -1$ e $ij = -ji = k$, $jk = -kj = i$ e $ki = -ik = j$ ed estendendo in modo unico in modo che il prodotto sia un'operazione binaria "bilineare" (cioè tale che valga la proprietà distributiva). Abbiamo quindi

$$\begin{aligned}(a + bi + cj + dk)(a' + b'i + c'j + d'k) =&(aa' - bb' - cc' - dd') + (ab' + ba' + cd' - c'd)i \\ &+ (ac' + a'c + db' - d'b)j + (ad' + da' + bc' - b'c)k.\end{aligned}$$

Definiamo il coniugato di $\alpha = a + bi + cj + dk$ tramite $\bar{\alpha} := a - bi - cj - dk$ e osserviamo dalla formula precedente che la norma di α data da

$$N(\alpha) := \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$$

è sempre un numero reale non negativo, nullo solo se $\alpha = 0$. Abbiamo quindi che se $\alpha \neq 0$ allora α è invertibile e il suo inverso è dato da

$$\alpha^{-1} = \frac{a}{N(\alpha)} - \frac{b}{N(\alpha)}i - \frac{c}{N(\alpha)}j - \frac{d}{N(\alpha)}k = \frac{\bar{\alpha}}{N(\alpha)}.$$

L'insieme Q con le operazioni di somma e prodotto ha quindi una struttura di corpo e i suoi elementi vengono detti *quaternioni*.

Concludiamo questa sezione ricordando una classica costruzione di produzione di nuovi anelli. Se A e B sono anelli possiamo dare al prodotto cartesiano $A \times B$ la struttura di anello definendo la somma e il prodotto componente per componente. Osserviamo che il prodotto cartesiano di anelli non è quasi mai un dominio: infatti questo capita se e solo se uno dei due è un dominio e l'altro è l'anello banale con un elemento.

4. Omomorfismi, ideali e quozienti

In questa sezione gli anelli considerati sono commutativi ma non necessariamente unitari.

Definizione. Siano A e B due anelli. Un *omomorfismo* da A a B è una funzione

$$\varphi : A \to B$$

tale che, per ogni $a, a' \in A$ si ha $\varphi(a + a') = \varphi(a) + \varphi(a')$ e $\varphi(a \cdot a') = \varphi(a) \cdot \varphi(a')$. Se gli anelli A e B sono unitari si richiede anche che $\varphi(1) = 1$.

Esempio 4.1. (importante). Se A è un anello unitario allora esiste un unico omomorfismo $\varphi : \mathbb{Z} \to A$. Tale omomorfismo è dato da $\varphi(m) = m \in A$ per ogni $m \in \mathbb{Z}$ secondo la notazione introdotta precedentemente. È importante convincersi sia dell'esistenza che dell'unicità di tale omomorfismo.

Facciamo una prima osservazione.

Lemma 4.2. *Se $\varphi : A \to B$ w $\psi : B \to C$ sono omomorfismo di anelli, allora anche $\psi \circ \phi : A \to C$ è un omomorfismo di anelli.*

Dimostrazione. Semplice verifica. □

Lemma 4.3. *Se $\varphi : A \to B$ è un omomorfismo biunivoco di anelli allora anche φ^{-1} è un omomorfismo di anelli.*

Proof. Siano $b, b' \in B$ e siano $a, a' \in A$ tali che $\varphi(a) = b$ e $\varphi(a') = b'$. Allora abbiamo $\varphi(a + a') = b + b'$ e $\varphi(aa') = bb'$ e quindi

$$\varphi^{-1}(b + b') = a + a' = \varphi^{-1}(b) + \varphi^{-1}(b')$$

e analogamente con il $\cdot$ al posto del $+$. Osserviamo anche che se φ è un omomorfismo di anelli unitari si ha chiaramente anche $\varphi^{-1}(1) = 1$.

□

Un omomorfismo biunivoco si dice *isomorfismo*. Un isomorfismo può essere pensato semplicemente come un cambio di nome degli elementi, in quanto la struttura algebrica rimane esattamente la stessa.

Se A è un anello non unitario, un sottoanello di A è un sottoinsieme non vuoto che sia a sua volta un anello rispetto alle stesse operazioni di somma e prodotto definite in A.

Esempio 4.4. Se A è un sottoanello di B osserviamo che l'inclusione $\iota : A \to B$ data da $\iota(a) = a$ per ogni $a \in A$ è chiaramente un omomorfismo di anelli. La proiezione $\pi : \mathbb{Z} \to \mathbb{Z}_m$ è anche un esempio di omomorfismo (confronta con l'Esempio 4.1).

Definizione. Sia $\varphi : A \to B$ un omomorfismo di anelli. Il *nucleo* di φ è

$$\ker(\varphi) := \{a \in A : \varphi(a) = 0\}.$$

Osserviamo che se $\varphi : A \to B$ è un omomorfismo di anelli allora il nucleo $\ker(\varphi)$ è un sottogruppo additivo che soddisfa la seguente ulteriore proprietà: per ogni $x \in \ker(\varphi)$ e per ogni $a \in A$ si ha $ax \in \ker(\varphi)$. Ciò è del tutto evidente e segue direttamente dal fatto che φ è moltiplicativo. Assiomatizzando questo concetto diamo la seguente

Definizione. Sia A un anello. Un *ideale* di A è un sottoinsieme I che sia un sottogruppo additivo e tale che per ogni $x \in I$ e per ogni $a \in A$ si ha $ax \in I$.

Abbiamo quindi già osservato che

Proposizione 4.5. *Il nucleo di un omomorfismo è un ideale.*

Lemma 4.6. *Se I è un ideale di un anello A allora I è un sottoanello (non necessariamente unitario). Inoltre, se A è unitario e I un ideale di A allora sono equivalenti:*

- *I è un sottoanello unitario;*
- *$I = A$;*
- *I contiene un elemento invertibile.*

Dimostrazione. Un ideale è un sottogruppo additivo e chiuso rispetto al prodotto per definizione (rispetto al prodotto si richiede una proprietà più forte nella definizione di ideale).

Supponiamo ora che A sia unitario. Se I contiene un elemento u invertibile, allora contiene anche $u \cdot u^{-1} = 1$ e quindi è unitario. Se I è unitario contiene 1 e quindi contiene

$1 \cdot a = a$ per ogni $a \in A$ e quindi $I = A$. Infine, se $I = A$ allora I contiene chiaramente tutti gli elementi di A e in particolare quelli invertibili. □

Esempio 4.7. Gli ideali di $\mathbb{Z}$. Sappiamo già dal corso del primo anno che i sottogruppi additivi sono gli $m\mathbb{Z}$ al variare di $m > 0$; una semplice verifica mostra che questi sono anche ideali e quindi sono tutti gli ideali di $\mathbb{Z}$.

Sia A un anello e $\sim$ una relazione d'equivalenza: vogliamo ora vedere quando è possibile dare la struttura di anello in modo naturale all'insieme quoziente.

Lemma 4.8. *Sia $I \subset A$ un sottoinsieme non vuoto.*

(1) *La relazione su A data da $x \sim_I y$ se $x - y \in I$ è una relazione d'equivalenza se e solo se I è un sottogruppo additivo;*
(2) *Se I è un sottogruppo additivo la relazione d'equivalenza $\sim_I$ è compatibile se e solo se I è un ideale.*

Dimostrazione. (1) Supponiamo che $\sim_I$ sia d'equivalenza e siano $x, y \in I$. Dobbiamo mostrare che $x - y \in I$ per l'Esercizio 1.2. Per costruzione $x \sim_I 0$ e anche $y \sim_I 0$ e quindi, per transitività abbiamo $x \sim_I y$, cioè $x - y \in I$. Viceversa, se I è un sottogruppo abeliano allora le tre proprietà di una relazione d'equivalenza sono una semplice verifica (da fare!). (2) Supponiamo che $\sim_I$ sia compatibile. Dobbiamo mostrare che se $a \in A$ e $x \in I$ allora $ax \in I$. La compatibilità ci assicura che $ax = a0$ in quanto $x \sim_I 0$ e quindi $ax \sim_I 0$, cioè $ax \in I$. Viceversa, se I è un ideale, siano $a, a', b, b' \in A$ tali che $a \sim_I a'$ e $b \sim_I b'$ cioè tali che $a - a' \in I$ e $b - b' \in I$. Allora

- $(a + b) - (a' + b') = (a - a') + (b - b') \in I$ e quindi $a + b \sim_I a' + b'$;
- $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I$ e quindi $ab \sim_I a'b'$.

□

Per la Proposizione 2.7 e il Lemma 4.8, se I è un ideale di un anello A, possiamo quindi dare una struttura di anello all'insieme quoziente $A/\sim_I$. Vale anche il viceversa:

Proposizione 4.9. *Una relazione $\sim$ su un anello A è una relazione d'equivalenza compatibile se e solo se esiste un ideale I tale che la relazione $\sim$ coincide con la relazione $\sim_I$.*

Dimostrazione. Abbiamo già mostrato nel Lemma 4.8 che se I è un ideale allora la relazione $\sim_I$ è una relazione d'equivalenza compatibile. Viceversa, sia $\sim$ una relazione d'equivalenza compatibile. Consideriamo il sottoinsieme I di A dato da

$$I = \{x \in A : x \sim 0\}.$$

Mostriamo che I è un ideale. Si ha chiaramente $0 \in I$ e, se $x, y \in I$ allora $x + y \sim 0 + 0 = 0$ perché $\sim$ è compatibile. Inoltre, dalla condizione $-x + x = 0$, segue anche che $-x \in I$. Infine, se $a \in A$ abbiamo che $a \cdot x \sim a \cdot 0 = 0$ e quindi $a \cdot x \in I$.

Mostriamo infine che le relazioni $\sim$ e $\sim_I$ coincidono. Dati $x, y \in A$ si ha $x \sim y$ se e solo se $x - y \sim 0$ per la compatibilità di $\sim$ (basta sottrarre y in entrambi i membri). E questa

ultima condizione ci dice che $x - y \in I$ per definizione di I, e quest'ultima è per definizione equivalente a $x \sim_I y$.

□

La Proposizione 4.9 ci porta a dimostrare la seguente affermazione.

Corollario 4.10. *L'applicazione $I \mapsto \sim_I$ è una corrispondenza biunivoca tra ideali di A e relazioni d'equivalenza compatibili su A.*

Dimostrazione. Rimane solo da controllare che $I \mapsto \sim_I$ è iniettiva, e questo segue dal fatto che I può essere ricostruito dalla conoscenza di $\sim_I$: infatti $I = \{x \in A : x \sim_I 0\}$. □

Abbiamo quindi che se I è un ideale l'insieme quoziente $A/\sim_I$ ha una naturale struttra di anello ereditata da quella di A (cioè ottenuta effettuando le operazioni utilizzando i rappresentanti): tale anello verrà più semplicemente denotato con A/I e ci riferiremo ai suoi elementi come "laterali" rispetto ad I. Diremo inoltre anche che due elementi $a, b \in A$ sono congruenti modulo I e scriviamo $a \equiv b \mod I$, se $a \sim_I b$ o equivalentemente $a - b \in I$ o, ancora equivalentemente, se a e b rappresentano lo stesso elemento in A/I.

L'anello A/I viene detto *anello quoziente* (dell'anello A modulo l'ideale I).

Ideali e sottoanelli possono essere caratterizzati anche in termini di omomorfismi.

Proposizione 4.11. *Sia A un anello e $B \subset A$. Allora*

- *B è un ideale se e solo se B è il nucleo di un omomorfismo di dominio A.*
- *B è un sottoanello se e solo se B è immagine di un omomorfismo di codominio A.*

Dimostrazione. Abbiamo già osservato che i nuclei sono ideali. Se I è ideale allora $\pi : A \to A/I$ ha nucleo I.

È una semplice verifica mostrare che l'immagine di un omomorfismo (tra anelli unitari) è un sottoanello (unitario). Per mostrare che un sottoanello B è immagine di un omomorfismo è sufficiente considerare l'inclusione $\iota : B \to A$ la cui immagine è chiaramente B. □

Facciamo ora la seguente osservazione che conosciamo già nella teoria dei gruppi e degli spazi vettoriali

Proposizione 4.12. *Sia $\varphi : A \to B$ un omomorfismo di anelli. Allora φ è iniettivo se e solo se* $\ker(\varphi) = \{0\}$.

Dimostrazione. Se φ è iniettivo $\ker(\varphi)$ non può contenere più di un elemento e quindi contiene solo lo 0 di A. Viceversa, se $\ker(\varphi) = \{0\}$ siano $a, a' \in A$ tali che $\varphi(a) = \varphi(a')$; allora $\varphi(a - a') = 0$ e quindi $a - a' \in \ker(\varphi)$ e concludiamo che $a = a'$. □

Siamo ora pronti ad enunciare il risultato di gran lunga più importante che riguarda la teoria degli omomorfismi.

Teorema 4.13 (Primo fondamentale di omomorfismo)**.** *Sia $\varphi : A \to B$ un omomorfismo tra anelli (unitari). Allora φ induce un isomorfismo tra $A/ker(\varphi)$ e $Im(\varphi)$.*

Dimostrazione. Per ogni $a \in A$ denotiamo con $[a]$ la classe di a nel quoziente $A/\ker(\varphi)$. L'applicazione indotta $\psi : A/ker(\varphi) \to B$ è data da $\psi([a]) = \varphi(a)$. Mostriamo che è ben posta: sia $a' \in A$ tale che a e a' siano congruenti modulo $\ker(\varphi)$: questo vuol dire che esiste $x \in \ker(\varphi)$ tale che $a - a' = x$. Ma allora

$$\psi([a'] = \psi([a - x]) = \varphi(a - x) = \varphi(a) - \varphi(x) = \varphi(a) = \psi([a])$$

per cui la ψ è ben posta. Il fatto che ψ sia un omomorfismo segue dal fatto che i calcoli li possiamo fare utilizzando i rappresentanti utilizzando la φ e quindi ψ è un omomorfismo perché φ lo è. Infatti:

$$\psi([a] + [b]) = \psi([a + b]) = \varphi(a + b) = \varphi(a) + \varphi(b) = \psi([a]) + \psi([b])$$

e similmente con il $\cdot$ al posto del $+$.

Mostriamo che ψ è iniettiva: si ha $\psi([a]) = 0$ se e solo se $\varphi(a) = 0$ cioè se e solo se $a \in \ker(\varphi)$ e quindi abbiamo $[a] = 0$. La suriettività su $Im(\varphi)$ è ovvia. □

Vediamo ora qualche proprietà degli ideali.

Lemma 4.14. *Sia $\{I_j\}_{j\in J}$ una qualunque collezione di ideali di un anello A indicizzata da un insieme J. Allora*

$$\bigcap_{j\in J} I_j$$

è ancora un ideale di A.

Dimostrazione. Esercizio. □

Il Lemma 4.14 ci permette di dare la seguente definizione.

Definizione. Sia S un sottoinsieme di un anello A. L'ideale (S) generato da S è l'intersezione di tutti gli ideali che contengono S.

Proposizione 4.15. *Sia S un sottoinsieme non vuoto di un anello unitario A. Allora*

$$(S) = \{a_1 s_1 + \cdots + a_k s_k : k \in \mathbb{N}, a_1, \ldots, a_k \in A, s_1, \ldots, s_k \in S\}.$$

Dimostrazione. Sia $I = \{a_1 s_1 + \cdots + a_k s_k : k \in \mathbb{N}, a_1, \ldots, a_k \in A, s_1, \ldots, s_k \in S\}$. È chiaro che se un ideale contiene S allora deve contenere tutti gli elementi di I. Basta quindi osservare che gli elementi di S sono anche elementi di I (e questo è ovvio, basta scegliere $k = 1$, $a_1 = 1$ e s_1 un elemento arbitrario di S) e che I è un ideale. Infatti, la differenza di elementi di I

$$(a_1 s_1 + \cdots + a_k s_k) - (a'_1 s'_1 + \cdots + a'_h s'_h) = a_1 s_1 + \cdots + a_k s_k + (-a'_1)s'_1 + \cdots + (-a'_h)s'_h$$

è quindi ancora una "combinazione lineare finita" di elementi di S a coefficienti in A, cioè è ancora un elemento di I e quindi I è un sottogruppo additivo. L'altra verifica viene lasciata per esercizio. □

Osservazione. Questa proposizione non vale se l'anello A non è unitario. Perché? Come modificheresti la descrizione di (S) in questo contesto più generale?

In un anello unitario l'ideale generato da un insieme $S = \{s\}$ con un solo elemento viene detto *principale* e viene denotato semplicemente con (s) e si ha quindi:

$$(s) = \{as : a \in A\}$$

abbiamo cioè che (s) è costituito da tutti i "multipli in A di s". Osserviamo anche che $(s) = A$ se e solo se s è invertibile.

Lemma 4.16. *Siano I, J ideali di un anello A. Allora l'insieme*

$$I + J := \{x + y : x \in I,\, y \in J\}$$

è ancora un ideale detto ideale somma dgli ideali I e J.

Dimostrazione. Tutte le verifiche sono elementari. □

Osserviamo che se I è un ideale di un anello A e B è un sottoanello di A che contiene I allora I è anche un ideale di B.

Teorema 4.17 (Secondo fondamentale di omomorfismo)**.** *Se I, J sono ideali di un anello A allora*

$$\frac{I + J}{I} \cong \frac{J}{I \cap J}.$$

Dimostrazione. Per quanto osservato prima abbiamo che I è un ideale in $I + J$ e $I \cap J$ è un ideale in J e possiamo quindi considerarne i quozienti. Consideriamo la funzione $\varphi : J \to \frac{I+J}{I}$ data da $\varphi(y) = [y]_I$, la classe di y in $\frac{I+J}{I}$. Il fatto che φ sia un omomorfismo deriva dal fatto che le operazioni in $\frac{I+J}{I}$ possono essere effettuate sui rappresentanti. Vediamo che φ è suriettiva: un elemento di $\frac{I+J}{I}$ è dato da $[x + y]_I$ per opportuni $x \in I$ e $y \in J$. Ma in tal caso abbiamo che $[x + y]_I = [y]_I$ in quanto $[x]_I = 0$. E abbiamo quindi che $[x + y]_I = \varphi(y)$. Per completare la dimostrazione basta osservare che $\ker(\varphi)$ è dato dagli elementi nel dominio, cioè in J, che appartengono alla classe nulla modulo I, cioè che stanno anche in I: abbiamo quindi $\ker(\varphi) = J \cap I$ e il risultato segue dal primo teorema fondamentale di omomorfismo. □

Vediamo un esempio di applicazione. Consideriamo l'anello (non unitario) J dato dai polinomi a coefficienti interi nella variabile X il cui termine noto sia divisibile per 3 (verificare che si tratta di un anello). Consideriamo inoltre in J l'ideale H dato da tutti i polinomi di J che hanno tutti i coefficienti pari (e qui verificare che si tratta di un ideale). Vogliamo descrivere J/H. Osserviamo che J è anche un ideale in $\mathbb{Z}[X]$ e ponendo

$$I = \{f \in \mathbb{Z}[X] : \text{tutti i coefficienti di } f \text{ sono pari}\}$$

osserviamo che I è un ideale in $\mathbb{Z}[X]$ e che $H = I \cap J$. Per il secondo teorema di omomorfismo abbiamo quindi

$$J/H = \frac{J}{I \cap J} \cong \frac{I + J}{I}.$$

Ma chi è $I + J$? Osserviamo che $1 = (-2) + 3 \in I + J$ e quindi $I + J = \mathbb{Z}[X]$ e quindi concludiamo che J/H è isomorfo a $\mathbb{Z}[X]/I$, cioè sono polinomi "a coefficienti in $\mathbb{Z}_2$".

Esercizio 4.18. Sia $\varphi : A \to B$ un omomorfismo di anelli. Mostrare che la controimmagine di un ideale di B è sempre un ideale di A, mentre non è sempre vero che l'immagine di un ideale di A sia un ideale di B.

Vogliamo ora vedere che legame c'è tra ideali di A e ideali di B quando siamo in presenza di un omomorfismo suriettivo $A \to B$.

Proposizione 4.19. *Sia $\varphi : A \to B$ un omomorfismo di anelli suriettivo. Allora φ induce una biiezione tra ideali di A che contengono $\ker(\varphi)$ e ideali di B. Similmente φ induce una biiezione tra sottoanelli di A che contengono $\ker(\varphi)$ e sottoanelli di B.*

Dimostrazione. Se J è un ideale di B allora la controimmagine $\varphi^{-1}(J)$ chiaramente contiene $\ker(\varphi)$ e mostriamo che si tratta anche di un ideale. Infatti, se $x, x' \in \varphi^{-1}(J)$ abbiamo $\varphi(x - x') = \varphi(x) - \varphi(x') \in J$ e quindi $\varphi^{-1}(J)$ è un sottogruppo additivo. Inoltre, se $a \in A$, abbiamo $\varphi(ax) = \varphi(a)\varphi(x) \in J$ e quindi $ax \in \varphi^{-1}(J)$ e possiamo concludere che $\varphi^{-1}(J)$ è un ideale.

Mostriamo ora che $J \mapsto \varphi^{-1}(J)$ è una corrispondenza biunivoca: che tale funzione sia iniettiva segue direttamente dal fatto che φ è suriettiva (non serve neanche sapere che φ è un omomorfismo). Per mostrare che è suriettiva basta mostrare che se I è un ideale di A che contiene $\ker(\varphi)$ allora $\varphi(I)$ è un ideale di B e che $\varphi^{-1}(\varphi(I)) = I$. Infatti, se $x, x' \in I$ allora $\varphi(x) - \varphi(x') = \varphi(x - x') \in \varphi(I)$ perché $x - x' \in I$. Inoltre, se $b = \varphi(a) \in B$ allora $\varphi(x) \cdot \varphi(a) = \varphi(xa) \in \varphi(I)$ e quindi $\varphi(I)$ è un ideale. Inoltre, se $x \in \varphi^{-1}(\varphi(I))$ allora esiste $y \in I$ tale che $\varphi(x) = \varphi(y)$: ma allora $\varphi(x - y) = 0$ e quindi $x - y \in \ker(\varphi)$ e quindi $x \in I$.

La dimostrazione per i sottoanelli è del tutto analoga. □

Un'immediata conseguenza della Proposizione 4.19, applicata al caso in cui $B = A/I$ e φ è la proiezione canonica, è che gli ideali di un anello quoziente A/I sono tutti e soli della forma J/I dove J è un ideale che contiene I e similmente con i sottoanelli anziché gli ideali.

Esempio 4.20. Gli ideali di $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ sono dati dai quozienti $I/m\mathbb{Z}$ dove I è un ideale di $\mathbb{Z}$ che contiene $m\mathbb{Z}$. E siccome gli ideali di $\mathbb{Z}$ sono tutti e soli della forma $n\mathbb{Z}$ abbiamo che gli ideali di $\mathbb{Z}_m$ sono dati da

$$\frac{d\mathbb{Z}}{m\mathbb{Z}}$$

al variare di d tra i divisori di m. I possibili quozienti sono quindi

$$\frac{\mathbb{Z}/m\mathbb{Z}}{d\mathbb{Z}/m\mathbb{Z}}$$

e il prossimo risultato ci dà anche la struttura algebrica di questi quozienti "doppi".

Teorema 4.21 (Terzo fondamentale di omomorfismo)**.** *Siano I, J ideali di un anello A, $I \subset J$. Allora*

$$A/J \cong \frac{A/I}{J/I}.$$

Dimostrazione. Denotiamo con $[a]_I$ e con $[a]_J$ la classe di congruenza di a modulo I e modulo J rispettivamente. Definiamo $\varphi : A/I \to A/J$ ponendo $\varphi([a]_I) = [a]_J$. Verifichiamo intanto che φ è ben posta: infatti, se $[a]_I = [a']_I$ allora $a - a' \in I$ e quindi anche $a - a' \in J$ e di conseguenza $[a]_J = [a']_J$. Il fatto che φ sia un omomorfismo di anelli allora segue dal fatto che le operazioni sono definite sui rappresentanti.

Osserviamo che φ è suriettiva: se $[a]_J \in A/J$ allora abbiamo che $[a]_J$ è l'immagine di $[a]_I$. Il nucleo di φ, infine, è dato da tutte le classi $[a]_I$ tali che $[a]_J = 0$, cioè è dato da tutte le classi modulo I rappresentate da elementi di J, per cui abbiamo $\ker(\varphi) = J/I$ e il risultato segue dal primo teorema fondamentale di omomorfismo. □

Conseguenza immediata di questo teorema è che i quozienti di $\mathbb{Z}_m$ sono quindi tutti isomorfi a $\mathbb{Z}_d$ al variare di d tra i divisori di m.

Vogliamo ora vedere un'ultima importante applicazione del primo teorema di omomorfismo.

Teorema 4.22 (Cinese del resto)**.** *Siano n, m interi positivi. Allora*

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

come anelli se e solo se MCD$(n, m) = 1$.

Dimostrazione. Se $\mathrm{MCD}(n, m) = d > 1$ abbiamo che ogni elemento di $\mathbb{Z}_n \times \mathbb{Z}_m$ ha ordine divisore di mn/d: infatti, se $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$ abbiamo

$$\frac{mn}{d}(a, b) = \Big(\frac{m}{d}na, \frac{n}{d}mb\Big) = (0, 0) = 0.$$

Ne segue che $\mathbb{Z}_n \times \mathbb{Z}_m$ come gruppo additivo non è ciclico e quindi non può essere isomorfo a $\mathbb{Z}_{nm}$.

Supponiamo ora che $\mathrm{MCD}(n, m) = 1$ e consideriamo l'unico omomorfismo (vedi Esempio 4.1)

$$\varphi : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m.$$

Questo omomorfismo è dato da $\varphi(z) = ([z]_n, [z]_m)$. Possiamo anche osservare che φ è un omomorfismo in quanto le proiezioni di $\mathbb{Z}$ su $\mathbb{Z}_m$ lo sono per ogni m. Osserviamo ora che $\ker(\varphi)$ è dato dagli interi multipli sia di m che di n, ed essendo questi primi tra loro, abbiamo $\ker(\varphi) = mn\mathbb{Z}$. Per il primo teorema di omomorfismo abbiamo quindi che $\mathbb{Z}_{nm}$ è isomorfo a $Im(\varphi)$. Ma siccome $\mathbb{Z}_{nm}$ ha nm elementi deduciamo che anche $Im(\varphi)$ ha nm elementi e quindi $Im(\varphi) = \mathbb{Z}_n \times \mathbb{Z}_m$.

□

Un problema tipico nei sistemi di congruenze è quello di determinare la controimmagine di un elemento in $\mathbb{Z}_n \times \mathbb{Z}_m$ tramite l'unico omomorfismo $\varphi : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ (definito nella dimostrazione del Teorema 4.22). Il teorema cinese del resto ci dice che tale controimmagine è data da una classe resto modulo nm.

Esempio 4.23. Per il teorema cinese del resto abbiamo $\mathbb{Z}_{15} \times \mathbb{Z}_{28} \cong \mathbb{Z}_{420}$ come anelli. Vogliamo trovare $\varphi^{-1}(7, 20)$, cioè l'unico elemento $k \in \mathbb{Z}_{420}$ che sia soluzione del sistema

$$\begin{cases} k \equiv 7 & \mod 15 \\ k \equiv 20 & \mod 28 \end{cases}$$

Più in generale, se dobbiamo risolvere il sistema

$$\begin{cases} k \equiv a & \mod m \\ k \equiv b & \mod n \end{cases}$$

con $MCD(n, m) = 1$, si cercano r ed s tali che $1 = rm + sn$ (identità di Bèzout) e poi basta porre $k = sna + rmb$. Infatti è chiaro che tale k è soluzione e per il teorema cinese sappiamo che questa è l'unica soluzione modulo nm. Nel nostro caso abbiamo $1 = 7 \cdot 28 - 13 \cdot 15$ e quindi

$$k = 7 \cdot 7 \cdot 28 - 13 \cdot 15 \cdot 20 = 412 \mod 420.$$

Riscopriamo quindi un risultato che già conosciamo dal primo anno

Corollario 4.24. *Consideriamo la cosiddetta ϕ di Eulero $\phi : \mathbb{N}_+ \to \mathbb{N}_+$ data da*

$$\phi(n) = |\{k \in \{1, 2, \dots, n\} : MCD(k, n) = 1\}|.$$

Allora $\phi(nm) = \phi(n)\phi(m)$ per ogni n, m tali che $MCD(n, m) = 1$.

Dimostrazione. Ricordiamo che gli elementi invertibili in $\mathbb{Z}_n$ sono proprio $\phi(n)$ e quindi gli elementi invertibili di $\mathbb{Z}_n \times \mathbb{Z}_m$ sono $\phi(n)\phi(m)$ e il risultato segue. □

Il teorema cinese del resto può anche essere enunciato in una forma più generale aumentando il numero dei fattori. Se $n_1, \dots, n_r$ sono a due a due coprimi allora

$$\mathbb{Z}_{n_1 \cdots n_r} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} :$$

la dimostrazione è esattamente la stessa, oppure si può dimostrare per induzione su r (provare!). In questo caso, la soluzione del sistema dato da $k \equiv k_i \mod n_i$ per ogni $i = 1, \dots, r$, può essere esplicitamente espressa nel modo seguente: sia $s_i \in \mathbb{Z}$ tale che $n_1 \cdots n_{i-1} s_i n_{i+1} \cdots n_r \equiv 1 \mod n_i$ (cioè s_i rappresenta l'inverso di $n_1 \cdots n_{i-1} n_{i+1} \cdots n_r$ modulo n_i. Allora la soluzione è data da

$$k = \sum_{i=1}^{r} k_i n_1 \cdots n_{i-1} s_i n_{i+1} \cdots n_r.$$

Completiamo questa sezione generalizzando il teorema cinese ad un anello qualunque. Prima però abbiamo bisogno di introdurre anche l'operazione di prodotto tra ideali.

Lemma 4.25. *Siano I, J ideali di un anello A. Allora il prodotto*

$$IJ = \{x_1 y_1 + \cdots + x_k y_k : k \in \mathbb{N},\, x_1, \dots, x_k \in I,\, y_1, \dots, y_k \in J\}$$

è ancora un ideale.

Dimostrazione. Siano $x_1y_1 + \cdots + x_ky_k, x'_1y'_1 + \cdots + x'_hy'_h \in IJ$. Allora

$$(x_1y_1 + \cdots + x_ky_k) - (x'_1y'_1 + \cdots + x'_hy'_h) = x_1y_1 + \cdots + x_ky_k + (-x'_1)y'_1 \cdots + (-x'_h)y'_h \in IJ$$

e per ogni $a \in A$ abbiamo

$$a(x_1y_1 + \cdots + x_ky_k) = (ax_1)y_1 + \cdots + (ax_k)y_k \in IJ.$$

□

Osserviamo che in generale $IJ \subseteq I \cap J$ e può ben accadere che $IJ \neq I \cap J$: ad esempio, in $\mathbb{Z}$ se $I = 6\mathbb{Z}$ e $J = 10\mathbb{Z}$ abbiamo $IJ = 60\mathbb{Z}$ mentre $I \cap J = 30\mathbb{Z}$.

Teorema 4.26 (Cinese del resto, forma generale)**.** *Sia A un anello unitario e siano I, J ideali tali che $I + J = A$. Allora $IJ = I \cap J$ e*

$$\frac{A}{I \cap J} \cong \frac{A}{I} \times \frac{A}{J}.$$

Dimostrazione. Sia $x + y = 1$ con $x \in I$ e $y \in J$. Sappiamo già che $IJ \subset I \cap J$. Sia ora $z \in I \cap J$. Abbiamo $z = z(x + y) = zx + zy \in IJ$ per cui $I \cap J \subset IJ$.

Inoltre se $[a]_I \in A/I$ allora $[a]_I = [a(x + y)]_I = [ay]_I$ con $ay \in J$. Similmente con J al posto di I. Ogni elemento di $A/I \times A/J$ è quindi della forma $([y']_I, [x']_J)$ con $x' \in I$ e $y' \in J$ e quindi l'omomorfismo $a \mapsto ([a]_I, [a]_J)$ è suriettivo in quanto $x' + y' \mapsto ([y']_I, [x']_J)$. □

Esempio 4.27. In $\mathbb{R}[X]$ consideriamo gli ideali principali $I = (X^2 + 1)$ e $J = (X + 1)$. Abbiamo $1 = \frac{1}{2}(X^2+1)+\frac{1}{2}(-X^2+1)$ per cui le ipotesi del teorema cinese sono soddisfatte. Si ha $I \cap J = IJ = ((X + 1)(X^2 + 1))$ e quindi

$$\mathbb{R}[X]/(X^3 + X^2 + X + 1) \cong \mathbb{R}[X]/(X^2 + 1) \times \mathbb{R}[X]/(X + 1).$$

5. La caratteristica di un dominio

Proposizione 5.1. *Se A è un dominio e $m \in \mathbb{N}$ sono equivalenti*

- *$m = 0 \in A$;*
- *esiste $a \in A$, $a \neq 0$, tale che $ma = 0$;*
- *per ogni $a \in A$ si ha $ma = 0$.*

Dimostrazione. La dimostrazione di questo fatto è immediata ricordando che ma pensato come la somma di m volte a è uguale a $m \cdot a$, dove con il simbolo m intendiamo la somma di m volte 1. □

Se A è un dominio la caratteristica $car(A)$ di A è

- 0 se le condizioni equivalenti della Proposizione 5.1 sono soddisfatte solo per $m = 0$;
- il più piccolo intero positivo m che soddisfa la Proposizione 5.1, se tale intero esiste.

Osservazione. La caratteristica di un dominio è sempre 0 o un numero primo. Infatti, se $car(A) = m = ab$, con $a, b < m$, la condizione $ab = 0$ implicherebbe $a = 0$ oppure $b = 0$, contraddicendo la minimalità di m.

Se $car(A)$ è p allora A contiene un (unico) sottoanello isomorfo a $\mathbb{Z}_p$; se $car(A)$ è 0 allora A contiene un (unico) sottoanello isomorfo a $\mathbb{Z}$; in entrambi i casi questi sottoanelli sono dati dalle immagini dell'unico omomorfismo $\varphi : \mathbb{Z} \to A$.

Se K è un campo e $car(K) = 0$ allora K contiene un (unico) sottocampo isomorfo a $\mathbb{Q}$: questo è dato dagli elementi della forma $ab^{-1} \in A$ al variare di $a, b \in \mathbb{Z}$, $b \neq 0$.

Teorema 5.2. *Un campo finito K di caratteristica p ha p^l elementi, per qualche $l > 0$.*

Dimostrazione. Abbiamo che K contiene un sottocampo isomorfo a $\mathbb{Z}_p$. In particolare K è anche uno spazio vettoriale su $\mathbb{Z}_p$ (convincersi che tutte le proprietà della definizione di spazio vettoriale sono soddisfatte). Essendo K finito abbiamo che K ha dimensione finita su $\mathbb{Z}_p$. Se tale dimensione è l allora ogni elemento si esprime in un unico modo come combinazione lineare a coefficienti in $\mathbb{Z}_p$ degli elementi di una base (costituita quindi da l elementi). Concludiamo che, avendo p scelte per il primo coefficiente, p per il secondo e ... p per l' l-esimo abbiamo in tutto p^l elementi. □

6. Estensioni quadratiche

Se A è un anello e $d \in A$, vogliamo estendere l'anello A (cioè costruire un anello più grande contenente A) aggiungendo un elemento che al quadrato dia d, cioè una "radice quadrata" di d. Se chiamiamo tale elemento ε, nel nostro nuovo anello, che denotiamo con $A[\sqrt{d}]$, avremo tutti gli elementi della forma $a + b\varepsilon$ al variare di $a, b \in A$:

$$A[\sqrt{d}] = \{a + b\varepsilon,\ a, b \in A\}.$$

Le scritture $a + b\varepsilon$ vanno per ora interpretate come simboli. Abbiamo quindi che $A[\sqrt{d}]$ è in biiezione con $A \times A$, ma gli daremo una struttura diversa di anello. Preferiamo usare la notazione ε anziché $\sqrt{d}$ per non cadere nella tentazione di scrivere "$\sqrt{4} = 2$", cosa che sarebbe sbagliata in $\mathbb{Z}[\sqrt{4}]$!

Poniamo

$$(a + b\varepsilon) + (a' + b'\varepsilon) = (a + a') + (b + b')\varepsilon$$

e

$$(a + b\varepsilon) \cdot (a' + b'\varepsilon) = (aa' + bb'd) + (ab' + a'b)\varepsilon.$$

Proposizione 6.1. *$A[\sqrt{d}]$ con le operazioni di somma e prodotto definite sopra è un anello.*

Dimostrazione. Semplici verifiche. □

Gli anelli $A[\sqrt{d}]$ vengono detti *estensioni quadratiche* di A e penseremo sempre ad A come un sottoanello di $A[\sqrt{d}]$ (cioè quello costituito dagli elementi della forma $a + 0\varepsilon$). L'anello $\mathbb{Z}[\sqrt{-1}]$ viene più spesso denotato con $\mathbb{Z}[i]$ e si chiama anello degli interi gaussiani. Osserviamo anche che $\mathbb{R}[\sqrt{-1}]$ altri non è che $\mathbb{C}$, il campo dei numeri complessi. Prima di andare a mostrare altri esempi facciamo un'osservazione di carattere aritmetico.

Lemma 6.2. *Sia $A = \mathbb{Z}, \mathbb{Q}$. Siano $d \in A$ un non quadrato in A e $a, b \in A$ tali che $a^2 = db^2$. Allora $a = b = 0$.*

Dimostrazione. Osserviamo che ogni numero razionale positivo $q \in \mathbb{Q}$ si scrive in modo unico nella forma

$$q = \prod_p p^{m_p}$$

dove $m_p \in \mathbb{Z}$. Ad esempio $\frac{25}{18} = 2^{-1}3^{-2}5^2$. Chiamiamo l'esponente m_p la molteplicità di p in q. Dalla definizione deduciamo che un numero razionale è un quadrato se e solo se tutti gli esponenti m_p sono pari. Essendo d un non quadrato esiste un primo p tale che la molteplicità di p in d è dispari.

Supponiamo per assurdo che $a \neq 0$. Segue immediatamente che anche $b \neq 0$. La molteplicità di p in a^2 è necessariamente pari e similmente la molteplicità di p in db^2 è necessariamente dispari e questo è assurdo. Ne segue che $a = 0$ e quindi essendo $d \neq 0$ (d non è un quadrato) anche $b = 0$. □

Esempio 6.3. Osserviamo che $\mathbb{Z}[\sqrt{2}]$ è un dominio: dobbiamo mostrare che se $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ sono tali che $\alpha\beta = 0$ e $\alpha \neq 0$ allora $\beta = 0$. Infatti se $\alpha = a + b\varepsilon$ e $\beta = a' + b'\varepsilon$ abbiamo $aa' + 2bb' = 0$ e $ab' + a'b = 0$. Siccome $\alpha \neq 0$ si ha $a \neq 0$ oppure $b \neq 0$. Se $a = 0$ abbiamo $b' = -a'b/a$ e sostituendo nell'altra equazione otteniamo

$$aa' - 2ba'b/a = 0$$

da cui, moltiplicando per $a'a$ otteniamo $(aa')^2 = 2(ba')^2$ e quindi per il Lemma 6.2 abbiamo $a' = 0$ e quindi anche $b' = -a'b/a = 0$ e quindi $\beta = 0$. Similmente si può procedere se $b \neq 0$ e quindi concludiamo che in ogni caso $\beta = 0$.

Esempio 6.4. Osserviamo che $\mathbb{Q}[\sqrt{2}]$ è un campo. Dobbiamo mostrare che ogni elemento non nullo è invertibile. Per il Lemma 6.2 sappiamo che se $\alpha = a+\varepsilon b \neq 0$ allora $a^2-2b^2 \neq 0$. Consideriamo quindi l'elemento

$$\beta = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\varepsilon.$$

Un semplice calcolo mostra che $\alpha\beta = 1$ per cui $\beta = \alpha^{-1}$.

Esempio 6.5. $\mathbb{Z}[\sqrt{4}]$ non è un dominio: infatti $(2 + \varepsilon)(2 - \varepsilon) = 0$.

Strumenti fondamentali nello studio delle estensioni quadratiche sono il coniugio e la norma.

Definizione. Sia $\alpha = a + \varepsilon b \in A[\sqrt{d}]$. Poniamo $\bar{\alpha} = a - \varepsilon b \in A[\sqrt{d}]$ e chiamiamo $\bar{\alpha}$ il *coniugato* di α. La *norma* di α è definita da $N(\alpha) = a^2 - db^2$.

Proposizione 6.6. *Il coniugio $\alpha \mapsto \bar{\alpha}$ è un automorfismo di $A[\sqrt{d}]$ come anello.*

Dimostrazione. È chiaro che il coniugio, essendo un'involuzione, è biunivoco. Dobbiamo quindi mostrare che si tratta di un omomorfismo di anelli. Si ha facilmente $\bar{1} = 1$. Se $\alpha = a + b\varepsilon$ e $\beta = a' + b'\varepsilon$ abbiamo

$$\bar{\alpha} + \bar{\beta} = a - b\varepsilon + a' - b'\varepsilon = (a + a') - \varepsilon(b + b') = \overline{\alpha + \beta}$$

e

$$\bar{\alpha}\bar{\beta} = (aa' + dbb') - (ab' + a'b)\varepsilon = \overline{\alpha\beta}.$$

□

È facile verificare che la norma $N : A[\sqrt{d}] \to A$ non è un omomorfismo di anelli: in particolare non è vero che $N(\alpha) + N(\beta) = N(\alpha + \beta)$. Vale tuttavia il seguente risultato.

Proposizione 6.7. *Per ogni $\alpha, \beta \in A[\sqrt{d}]$ si ha $N(\alpha) = \alpha\bar{\alpha}$ e $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Dimostrazione. La prima parte è una semplice verifica: se $\alpha = a + \varepsilon b$ abbiamo $\alpha\bar{\alpha} = (a + \varepsilon b)(a - \varepsilon b) = a^2 - db^2$.

La seconda parte è una conseguenza della prima e del fatto che il coniugio è un omomorfismo. Infatti:

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = N(\alpha)N(\beta).$$

□

Nel caso degli interi gaussiani abbiamo che se $\alpha = a+ib$ allora $N(\alpha) = a^2+b^2$. Deduciamo la seguente osservazione sui numeri interi: se c e d sono somma di due quadrati, allora esistono $\alpha, \beta \in \mathbb{Z}[i]$ tali che $N(\alpha) = c$ e $N(\beta) = d$. Abbiamo quindi che cd è la norma di $\alpha\beta$ e quindi è anch'esso la somma di due quadrati. Abbiamo quindi che il prodotto di due numeri che sono somma di due quadrati è a sua volta una somma di due quadrati.

Volendo generalizzare questa proprietà si ha il seguente fatto che non dimostriamo: se $n = 1, 2, 4, 8$ allora il prodotto di due numeri che sono somma di n è quadrati è ancora una somma di n quadrati. Tale affermazione è falsa per ogni $n \neq 1, 2, 4, 8$.

Ma torniamo allo studio della struttura algebrica di $A[\sqrt{d}]$.

Proposizione 6.8. *$A[\sqrt{d}]$ è un dominio se e solo se A lo è e l'unico elemento di norma nulla è 0.*

Dimostrazione. Sia $A[\sqrt{d}]$ un dominio. Allora chiaramente anche A, che è un sottoanello, deve essere un dominio. Sia inoltre α tale che $N(\alpha) = 0$. Ma per la Proposizione 6.7 $N(\alpha) = \alpha\bar{\alpha} = 0$ e quindi abbiamo che $\alpha = 0$.

Viceversa, se $\alpha\beta = 0$ allora abbiamo $N(\alpha)N(\beta) = 0$, sempre per la Proposizione 6.7. Siccome A è un dominio abbiamo che $N(\alpha) = 0$ oppure $N(\beta) = 0$ e quindi $\alpha = 0$ oppure $\beta = 0$. □

Questa proposizione è coerente con i nostri primi esempi: infatti $\mathbb{Z}[\sqrt{4}]$ non è un dominio perché l'elemento $2 + \varepsilon$ ha norma nulla. Osserviamo che se $d = 0$ non abbiamo mai un dominio (e infatti in questo caso $N(\varepsilon) = 0$)

Osserviamo che se d è un quadrato in A allora $A[\sqrt{d}]$ non è mai un dominio: infatti in tal caso, se $a^2 = d$ abbiamo che l'elemento $a + \varepsilon$ ha norma nulla. Il seguente risultato ci assicura che in $\mathbb{Z}$ e in $\mathbb{Q}$ vale anche il viceversa.

Corollario 6.9. *Se $A = \mathbb{Z}, \mathbb{Q}$ abbiamo che $A[\sqrt{d}]$ è un dominio se e solo se d non è un quadrato in A.*

Dimostrazione. Abbiamo osservato sopra che se d è un quadrato allora $A[\sqrt{d}]$ non è un dominio. Supponiamo quindi che d non è un quadrato. Se $A[\sqrt{d}]$ non fosse un dominio avremmo un elemento non nullo di norma nulla, cioè esisterebbero $a, b \in A$ non entrambi nulli, tali che $a^2 - db^2 = 0$. Ma questo contraddice il Lemma 6.2. □

Viene spontaneo chiedersi se questo corollario vale in qualunque dominio A. La risposta è no ed è fornita dal seguente esempio piuttosto complicato.

Esempio 6.10. Consideriamo l'anello quoziente $A = \mathbb{C}[x, y, z]/(x^2 - yz^2)$. In $A[\sqrt{y}]$ esistono elementi di norma nulla $(x + \varepsilon z)$ e quindi non è un dominio, ma l'elemento y non è un quadrato in A (perché?).

Concludiamo questo studio in un anello qualunque caratterizzando gli elementi invertibili in $A[\sqrt{d}]$.

Proposizione 6.11. *Un elemento $\alpha \in A[\varepsilon]$ è invertibile se e solo se lo è $N(\alpha)$ in A. E in tal caso $\alpha^{-1} = \bar{\alpha}/N(\alpha)$.*

Dimostrazione. Se α è invertibile abbiamo $\alpha\alpha^{-1} = 1$ e quindi $N(\alpha)N(\alpha^{-1}) = N(1) = 1$ per la moltiplicatività della norma e quindi $N(\alpha)$ è invertibile in A. Viceversa se $N(\alpha)$ è invertibile in A definiamo

$$\beta = \bar{\alpha}N(\alpha)^{-1}$$

ed $\alpha\beta = \alpha\bar{\alpha}N(\alpha)^{-1} = N(\alpha)N(\alpha)^{-1} = 1$ per cui $\beta = \alpha^{-1}$. □

Esercizio 6.12. Determinare gli elementi invertibili in $\mathbb{Z}[\sqrt{d}]$ con $d \leq -1$.

Consideriamo ora il caso particolare in cui l'anello che andiamo a estendere è un campo K. Abbiamo.

Lemma 6.13. *Sia K un campo e $d \in K$. Allora d non è un quadrato in K se e solo se in $K[\sqrt{d}]$ l'unico elemento di norma nulla è 0.*

Dimostrazione. Se $d = a^2$ è un quadrato in K abbiamo che $N(a + \varepsilon) = 0$. Viceversa se un elemento $\alpha \neq 0$ ha norma nulla esistono $a, b \in K$ non entrambi nulli tali che $a^2 - db^2 = 0$. Essendo non entrambi nulli abbiamo in particolare $b \neq 0$ (altrimenti anche $a = 0$) e quindi $d = (ab^{-1})^2$ è un quadrato. □

Corollario 6.14. *$K[\sqrt{d}]$ è un campo se e solo se d non è un quadrato in K. In particolare $\mathbb{C}$ è un campo.*

Questo corollario ci dà un metodo per costruire nuovi campi finiti partendo da un campo K e da un elemento di K che non è un quadrato. Quali e quanti sono i quadrati in un campo finito? Osserviamo che se $a^2 = b^2$ allora $(a + b)(a - b) = 0$ e quindi $a = \pm b$. In caratteristica 2 abbiamo quindi $a = b$ e l'applicazione $a \mapsto a^2$ è iniettiva. In un campo finito con caratteristica $\neq 2$ la funzione $a \mapsto a^2$ non è iniettiva e quindi neanche suriettiva e abbiamo elementi che non sono quadrati.

Proposizione 6.15. *Se $|K| = q$ dispari allora in K si hanno $(q+1)/2$ quadrati e $(q-1)/2$ non quadrati.*

Dimostrazione. Per quanto osservato prima l'applicazione $K^* \to K^*$ data da $x \mapsto x^2$ è 2:1 e quindi i quadrati sono $\frac{q-1}{2} + 1$. □

La Proposizione 6.15 ci permette di costruire ricorsivamente campi con p^{2^n} elementi per ogni primo p dispari. Infatti per $n = 0$ abbiamo il campo $\mathbb{Z}_p$ e supponendo di aver già costruito un campo K con $p^{2^{n-1}}$ elementi possiamo trovare in K un elemento d che non è un quadrato per quanto visto nella Proposizione 6.15 e quindi costruire un'estensione quadratica di K che avrà quindi $(p^{2^{n-1}})^2 = p^{2^n}$ elementi.

7. Radici di -1 in campi finiti

Anche alla luce dell'importanza delle radici quadrate vista nella sezione precedente, ci proponiamo in questa di studiare il problema dell'esistenza di un elemento che al quadrato dia -1 in un campo finito K. Questo studio, oltre ad essere interessante di per sé, tornerà utile più avanti nel corso.

Se K ha caratteristica 2 abbiamo $-1 = 1$ e quindi -1 ammette radice quadrata. Consideriamo quindi il caso $|K| = q$ dispari. Il nostro principale obiettivo sarà di dimostrare il seguente risultato.

Teorema 7.1. *Sia K un campo finito con q elementi, q dispari. Allora esiste in K un elemento che al quadrato dà -1 se e solo se $q \equiv 1 \mod 4$.*

Un verso della dimostrazione è un'immediata applicazione della teoria dei gruppi. Supponiamo infatti che $a \in K$ sia tale che $a^2 = -1$. Abbiamo in questo caso che l'ordine (o periodo) di a nel gruppo K^* è 4. Siccome K^* ha $q - 1$ elementi abbiamo che $4|q - 1$ o, equivalentemente, $q \equiv 1 \mod 4$.

Ci rimane da dimostrare che se $q \equiv 1 \mod 4$ allora esiste una radice quadrata di -1. Premettiamo il seguente risultato.

Proposizione 7.2. *Se K è un campo finito il prodotto di tutti gli elementi non nulli di K è -1.*

Dimostrazione. Nel prodotto di tutti gli elementi non nulli di K ogni elemento verrà semplificato dal proprio inverso, con l'eccezione di quegli elementi che coincidono con il proprio inverso, cioè gli elementi a tali che $a = a^{-1}$. Ma se $a = a^{-1}$ allora $a^2 - 1 = (a+1)(a-1) = 0$ e quindi $a = \pm 1$. Abbiamo quindi che in tale prodotto gli unici elemento che rimangono dopo aver fatto un numero finito di semplificazioni sono 1 e -1 e quindi il prodotto è proprio -1. □

Corollario 7.3 (Teorema di Wilson)**.** *Se p è un numero primo allora $(p-1)! \equiv -1 \mod p$.*

Dimostrazione. Si tratta semplicemente del teorema precedente nel caso $K = \mathbb{Z}_p$. □

Siamo ora pronti a dimostrare la seconda parte del nostro teorema principale.

Dimostrazione. [proseguimento] Dobbiamo verificare che se $q \equiv 1 \mod 4$ allora esiste una radice quadrata di -1. Osserviamo che $a \neq -a$ per ogni $a \in K^*$ (perché?). Andiamo

quindi a riscrivere gli elementi non nulli di K "accoppiando" ogni elemento a con il suo opposto $-a$. Abbiamo

$$K = \{0, a_1, -a_1, a_2, -a_2, \dots, a_{\frac{q-1}{2}}, -a_{\frac{q-1}{2}}\}$$

dove gli elementi $0, a_1, -a_1, a_2, -a_2, \dots, a_{\frac{q-1}{2}}, -a_{\frac{q-1}{2}}$ sono tutti distinti. Avremo quindi, utilizzando la Proposizione 7.2,

$$-1 = \prod_{a \in K^*} a = \prod_{i=1}^{\frac{q-1}{2}} a_i(-a_i) = (-1)^{\frac{q-1}{2}} \prod_{i=1}^{\frac{q-1}{2}} a_i^2 = \Big(\prod_{i=1}^{\frac{q-1}{2}} a_i\Big)^2,$$

e il teorema è completamente dimostrato. □

8. Divisibilità

In questa sezione ci occupiamo di questioni di divisibilità tra elementi di un dominio. La divisibilità in un anello che non è un dominio è un concetto un po' "patologico" e quindi preferiamo non trattarlo. Iniziamo dalla seguente definizione, che di certo non ha niente di sorprendente.

Definizione. Sia A un dominio, $a, b \in A$. Diciamo che a *divide* b o che a è un *divisore* di b, o che b è un *multiplo* di a se esiste $x \in A$ tale che $b = ax$.

Questa definizione è in contrasto con la definizione di divisore dello zero data precedentemente. Tuttavia in questo contesto ci troviamo in un dominio per cui non esistono divisori dello zero nel senso vecchio, mentre ogni elemento di A divide 0 nel senso nuovo. In ogni caso, in un dominio, entrambi i concetti sono banali, e quindi non avremo occasione di utilizzarli, evitando fraintendimenti.

Vediamo alcune proprietà elementari che riguardano la relazione di divisibiltià.

Lemma 8.1. *Siano $a, b, c \in A$, $u \in A$ invertibile.*

- *se $a|b$ e $b|c$ allora $a|c$;*
- *$u|a$;*
- *$a|u$ se e solo se a è invertibile;*
- *$a|0$*
- *$0|a$ se e solo se $a = 0$;*
- *se $a|b$ e $a|c$ allora a divide ogni combinazione lineare di b e c, cioè ogni elemento del tipo $xb + yc$, con $x, y \in A$.*
- *se a divide b e $b + c$ allora $a|c$.*

Dimostrazione. Le verifiche sono tutte elementari e sono quindi lasciate al lettore volenteroso. □

Parlando di problemi di divisibilità viene naturale introdurre la seguente relazione

Definizione. Sia A un dominio, $a, b \in A$. Diciamo che a e b sono *associati* se esiste un elemento invertibile $u \in A$ tale che $a = ub$.

Osserviamo che "essere associati" è una relazione di equivalenza. Infatti $a = 1 \cdot a$ (riflessiva), se $a = ub$ allora $b = u^{-1}a$ (simmetrica), se $a = ub$ e $b = u'c$ allora $a = uu'c$ (transitiva).

Il seguente risultato ci permette sempre di sostituire un elemento con un suo associato per questioni di divisibilità.

Proposizione 8.2. *Sia A un dominio e $a, b, c \in A$. Allora*

- *a e b sono associati se e solo se $a|b$ e $b|a$;*
- *se a e b sono associati allora $a|c$ se e solo se $b|c$;*
- *se a e b sono associati allora $c|a$ se e solo se $c|b$.*

Dimostrazione. Se a e b sono associati abbiamo $a = ub$ e quindi $b|a$ e anche $b = u^{-1}a$ e quindi $a|b$. Viceversa, se $a|b$ e $b|a$ esistono $x, y \in A$ tali che $b = ax$ e $a = by$. Ne segue $a = axy$ da cui $xy = 1$ (perché siamo in un dominio!) e quindi x e y sono invertibili.

Gli altri due punti seguono direttamente dal primo e dalla transitività della relazione di divisibilità. Infatti, ad esempio, se $a|c$ e gli elementi a e b sono associati allora $b|a$ e quindi $b|c$. □

Ogni elemento $a \in A$ si può sempre scrivere come prodotto di due elementi di A: infatti, se u è un qualunque elemento invertibile possiamo scrivere $a = (au) \cdot u^{-1}$. Diremo che una tale fattorizzazione è *banale*. In certi casi è possibile scrivere una fattorizzazione non banale, cioè utilizzando fattori che non siano invertibili, in altri ciò non è possibile. È questo il senso della prossima definizione.

Definizione. Un elemento $a \in A$, non nullo e non invertibile si dice *riducibile* se esistono $b, c \in A$ entrambi non invertibili tali che $a = bc$. O, equivalentemente, se ammette una fattorizzazione non banale.

Osserviamo che la condizione a non invertibile nella definizione di elemento riducibile può essere omessa: se infatti un elemento invertibile a fosse il prodotto di due elementi $a = bc$, allora anche b e c sarebbero automaticamente invertibili (perché?).

Definizione. Un elemento non nullo, non invertibile e non riducibile si dice *irriducibile*. In altre parole un elemento non nullo a è irriducibile se in ogni sua fattorizzazione $a = bc$ con $b, c \in A$ si ha che almemo uno tra b e c, cioè a ammette solo le fattorizzazioni banali descritte sopra.

Non dovrebbe sorprendere il seguente risultato.

Proposizione 8.3. *Siano a e b associati. Allora a irriducibile se e solo se b lo è.*

Dimostrazione. Sia a irriducibile, vogliamo mostrare che anche b lo è. Altrimenti abbiamo che $b = 0$, b è invertibile, oppure b è riducibile. Abbiamo $a = bu$ con u invertibile e quindi $b = 0$ implica $a = 0$ e b invertibile implica a invertibile. Se b è riducibile abbiamo $b = cd$ dove c e d sono non nulli e non invertibili. Ma allora $a = bu = c(du)$ e quindi anche a è riducibile (essendo c e du non invertibili). □

Facciamo quindi una osservazione sulle classi di associatura. Abbiamo che lo 0 forma una classe di associatura da solo. Tutti gli elementi invertibili formano una classe di associatura. Le altre classi sono quindi formate o da tutti elementi irriducibili o da tutti elementi riducibili.

Esempio 8.4. In $\mathbb{Z}$ gli invertibili sono ± 1 e quindi le classi di associatura sono date da $\{0\}$ oppure da $\{n, -n\}$, $n > 0$. Gli elementi irriducibili sono tutti quelli della forma $\pm p$, dove p è un numero primo: infatti se proviamo a scrivere p o $-p$ come prodotto di due numeri interi, allora necessariamente uno è invertibile, cioè 1 o -1.

Esempio 8.5. In $\mathbb{Z}[i]$ gli elementi invertibili sono $\pm 1, \pm i$ e questi quattro elementi formano la classe di associatura degli elementi invertibili. Abbiamo quindi che ogni classe di associatura diversa dalla classe costituita dal solo 0 contiene esattamente quattro elementi. Infatti, se $\alpha \in \mathbb{Z}[i]$ abbiamo che la classe di α è data da $\{\alpha, -\alpha, \alpha i, -\alpha i\}$. Ad esempio, se $\alpha = 1 + i$ abbiamo che la classe di α è $\{1 + i, -1 - i, -1 + i, -1 - i\}$. Osserviamo infine che $1 + i$ (e quindi anche gli altri tre elementi della sua classe di associatura) è irriducibile.

Un'ultima osservazione sugli elementi associati:

Proposizione 8.6. *Siano $a, b \in A$. Allora $a|b$ se e solo se $(a) \supseteq (b)$. In particolare a e b sono associati se e solo se $(a) = (b)$.*

Dimostrazione. Se $a|b$ allora $b = ac$ e quindi $b \in (a)$ e di conseguenza $(b) \subseteq (a)$. □

Nell'anello dei numeri interi siamo abituati a non distinguere i due termini "primo" e "irriducibile". In realtà in generale le due nozioni non sono coincidenti, anche se lo saranno in molti esempi importanti, tra cui $\mathbb{Z}$. Vediamo intanto la definizione di elemento primo.

Definizione. Sia A un dominio e $x \in A$, x non nullo e non invertibile. Diciamo che x è un elemento *primo* se per ogni $a, b \in A$ tali che $x|ab$ si ha necessariamente $x|a$ oppure $x|b$.

Vediamo intanto che la nozione di elemento primo è sempre più forte di elemento irriducibile.

Lemma 8.7. *Sia A un dominio e $x \in A$ primo. Allora x è irriducibile.*

Dimostrazione. Supponiamo per assurdo che x sia riducibile, cioè $x = bc$ dove b e c sono entrambi non invertibili. Allora abbiamo che x divide b o c. Supponiamo che $x|b$: ma allora $b = xy$ da cui $x = xyc$ e quindi $yc = 1$ e concludiamo che c è invertibile. □

Esempio 8.8. Il Lemma 8.7 non vale in anelli che non sono domini (in cui, comunque, è anche poco sensato parlare di queste proprietà). Infatti in $\mathbb{Z}_{12}$ abbiamo che $3 = 3 \cdot 9$ e quindi non è irriducibile. Tuttavia si può verificare che 3 soddisfa le condizioni della definizione di elemento primo.

Esempio 8.9. Il viceversa del Lemma 8.7 non vale. Ad esempio, in $\mathbb{Z}[\sqrt{-5}]$ abbiamo $(1 + \varepsilon)(1 - \varepsilon) = 2 \cdot 3$ e quindi, in particolare, $(1 + \varepsilon)|2 \cdot 3$. Ma $N(1 + \varepsilon) = 6$ e $N(2) = 4$ e $N(3) = 9$ e quindi $1 + \varepsilon$ non divide né 2, né 3. Tuttavia $1 + \varepsilon$ è un elemento irriducibile. Infatti, se così non fosse avremmo α, β con $N(\alpha) = 2$ e $N(\beta) = 3$ tali che $\alpha\beta = 1 + \epsilon$. Ma elementi di norma 2 o 3 non esistono.

9. Domini euclidei e domini ad ideali principali

Andiamo ora a studiare alcune particolari famiglie di domini che soddisfano particolari condizioni sulla divisibilità.

Definizione. Un *anello (o dominio) euclideo* è un dominio A in cui è definita una funzione $\rho : A \to \mathbb{Z}$ che soddisfa le seguenti condizioni

- $\rho(0) < \rho(a)$ per ogni $a \in A$, $a \neq 0$;
- per ogni $a, b \in A$, $b \neq 0$ esistono $q, r \in A$ tali che $a = bq + r$ con $\rho(r) < \rho(b)$;
- per ogni $a, b \in A$ non nulli, $\rho(a) \leq \rho(ab)$.

Esempio 9.1. I campi sono anelli euclidei scegliendo ad esempio ρ identicamente uguale a 1 su $A \setminus \{0\}$ e $\rho(0) = 0$.

L'anello $\mathbb{Z}$ è chiaramente un anello euclideo utilizzando $\rho =$ "valore assoluto" e la tradizionale divisione con il resto.

Andiamo ora a studiare altri esempi.

Proposizione 9.2. *Il dominio $\mathbb{Z}[\sqrt{d}]$ con $d = -1, \pm 2$ è un anello euclideo ponendo $\rho(\alpha) = |N(\alpha)|$ per ogni $\alpha \in \mathbb{Z}[\sqrt{d}]$.*

Dimostrazione. La prima e la terza proprietà della definizione sono di verifica immediata (nel caso $d = 2$ utilizzando il Lemma 6.2). Per dimostrare la seconda proprietà sfruttiamo il fatto che $\mathbb{Z}[\sqrt{d}]$ è contenuto in $\mathbb{Q}[\sqrt{d}]$ che è un campo. Siano quindi $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, con $\beta \neq 0$ e consideriamo l'elemento $\alpha\beta^{-1} \in \mathbb{Q}[\sqrt{d}]$. Abbiamo $\alpha\beta^{-1} = x_1 + x_2\varepsilon$, con $x_1, x_2 \in \mathbb{Q}$. Scegliamo ora $a_1, a_2 \in \mathbb{Z}$ tali che $|a_i - x_i| \leq 1/2$ e poniamo $q := a_1 + a_2\varepsilon$ e $r := \alpha - \beta q$. Per costruzione abbiamo $\alpha = \beta q + r$ e dobbiamo quindi mostrare che $\rho(r) < \rho(\beta)$.

Ora,

$$r = \alpha - \beta q = \beta(\alpha\beta^{-1} - q) = \beta((x_1 + x_2\varepsilon) - (a_1 + a_2\varepsilon)) = \beta((x_1 - a_1) + (x_2 - a_2)\varepsilon))$$

$$\begin{aligned}
\rho(r) &= |N(r)| = |N(\beta)||N((x_1 - a_1) + (x_2 - a_2)\varepsilon)| \\
&= |N(\beta)||(x_1 - a_1)^2 - d(x_2 - a_2)^2| \\
&\leq |N(\beta)|(|(x_1 - a_1)^2| + |d||(x_2 - a_2)^2|) \\
&\leq |N(\beta)|(\frac{1}{4} + 2\frac{1}{4}) \\
&< |N(\beta)| \\
&= \rho(\beta).
\end{aligned}$$

□

Esempio 9.3. In $\mathbb{Z}[\sqrt{2}]$ vogliamo effettuare la "divisione con resto" tra $\alpha = 3 + 2\varepsilon$ e $\beta = 1 + 2\varepsilon$. Osserviamo che $\rho(\beta) = |N(\beta)| = |1 - 8| = 7$. Procediamo come nella dimostrazione della Proposizione 9.2. Abbiamo

$$\alpha\beta^{-1} = \frac{1}{N(\beta)}\alpha\bar{\beta} = -\frac{1}{7}(3 + 2\varepsilon)(1 - 2\varepsilon) = -\frac{1}{7}(-5 - 4\varepsilon) = \frac{5}{7} + \frac{4}{7}\varepsilon \in \mathbb{Q}[\sqrt{2}].$$

Abbiamo quindi $q = 1 + \varepsilon$ e

$$r = \alpha - \beta q = 3 + 2\varepsilon - (1 + 2\varepsilon)(1 + \varepsilon) = 3 + 2\varepsilon - (5 + 3\varepsilon) = 2 - \varepsilon$$

e osserviamo che effettivamente $\alpha = \beta q + r$ e che $\rho(r) = 2 < \rho(\beta)$.

Vediamo qualche proprietà di carattere generale.

Lemma 9.4. *Sia A un dominio euclideo, sia $\rho_0 = \min\{\rho(a) : a \in A, a \neq 0\}$ e $a \in A$. Allora*

$$a \text{ è invertibile} \iff \rho(a) = \rho_0.$$

Proof. Supponiamo che $\rho(a) = \rho_0$. Effettuando la divisione di 1 per a troviamo q, r tali che $1 = qa + r$. Per minimalità di $\rho(a)$ abbiamo $r = 0$ e quindi a è invertibile.

Viceversa, sia b invertibile e a tale che $\rho(a) = \rho_0$. Per la prima parte dell'esercizio abbiamo che a è invertibile e abbiamo quindi

$$a = b \cdot (b^{-1}a), \;\; b = a(a^{-1}b).$$

Per definizione di dominio euclideo abbiamo quindi $\rho(a) \leq \rho(b)$ e viceversa e quindi $\rho(a) = \rho(b) = \rho_0$. □

Diamo ora la seguente definizione:

Definizione. Sia A un dominio e $a, b, d \in A$. Diciamo che d è un *massimo comun divisore* tra a e b se $d|a$ e $d|b$ e inoltre d è un multiplo di ogni elemento che divide sia a che b.

Osserviamo che possono esistere elementi $a, b \in A$ che non ammettono massimo comun divisore. Infatti, torniamo all'esempio di $\mathbb{Z}[\sqrt{-5}]$; abbiamo $(1 + \varepsilon)(1 - \varepsilon) = 2 \cdot 3 = 6$ e vogliamo mostrare che non esiste un massimo comun divisore tra 6 e $2 + 2\varepsilon$. Infatti, se d fosse un massimo comun divisore tra 6 e $2 + 2\varepsilon$ avremmo che sia $1 + \epsilon$ che 2 dividono d. Siccome $N(1 + \epsilon) = 6$ e $N(2) = 4$, $N((1 + \epsilon)2)) = 24$ e $N(6) = 36$ abbiamo quindi $N(d) = 12$: ma si può verficare facilmente che non ci sono elementi di norma 12.

Osserviamo che se a, b ammettono un massimo comun divisore d allora l'insieme degli elementi che sono un massimo comun divisore tra a e b formano la classe di associatura di d: infatti se d' è associato a d allora soddisfa necessariamente le condizioni della definizione di massimo comun divisore e viceversa, se d' è un massimo comun divisore allora d' è associato a d: tutto segue facilmente dalla Proposizione 8.2.

Parlando di massimo comun divisore scriveremo quindi $\mathrm{MCD}(a, b) = d$ per indicare che gli elementi a e b ammettono un massimo comun divisore e che l'insieme dei massimi comun divisori di a e b è dato dalla classe di associatura di d.

Osserviamo che se b è un divisore di a allora $b = \mathrm{MCD}(a, b)$. In particolare, per $a = 0$ abbiamo $\mathrm{MCD}(0, b) = b$.

Proposizione 9.5. *Siano $a, b, c, d, x \in A$ tali che $a = bx + c$. Allora $d = MCD(a, b)$ se e solo se $d = MCD(b, c)$.*

Dimostrazione. Per simmetria basta mostrare che $d = \mathrm{MCD}(a, b)$ implica $d = \mathrm{MCD}(b, c)$. Infatti $d|b$ e $d|c = a - bx$. Inoltre, se $d'|b$ e $d'|c$ allora $d'|a$ e quindi $d'|d$ perché $d = \mathrm{MCD}(a, b)$. □

Corollario 9.6. *Sia A un dominio euclideo, $a, b \in A$. Allora esiste $d \in A$ tale che $MCD(a, b) = d$.*

Dimostrazione. Procediamo per induzione su $\min(\rho(a), \rho(b))$ e supponiamo senza perdere generalità che tale minimo sia $\rho(b)$. Il passo base dell'induzione consiste nel considerare il caso $b = 0$: è infatti questo l'unico elemento che minimizza la ρ per definizione. E in tal caso abbiamo già osservato che $\mathrm{MCD}(a, 0) = a$.

Passiamo quindi al passo induttivo e assumiamo pertanto $\rho(b) > \rho(0)$, cioè $b \neq 0$. Effettuiamo una divisione euclidea: abbiamo $a = qb+r$ con $\rho(r) < \rho(b)$. Abbiamo che $\mathrm{MCD}(b, r)$ esiste per ipotesi induttiva e per la Proposizione 9.5 abbiamo che anche $\mathrm{MCD}(a, b)$ esiste ed eguaglia $\mathrm{MCD}(b, r)$. □

Osserviamo che la dimostrazione di questo corollario ci fornisce anche un algoritmo ricorsivo per calcolare il MCD tra due elementi in un dominio euclideo che ricalca l'algoritmo euclideo delle divisioni successive nel caso dei numeri interi.

Definizione. Un dominio A si dice ad *ideali principali* se ogni suo ideale è principale. Diciamo in tal caso per brevità che A è un PID (principal ideal domain).

Teorema 9.7. *Un dominio euclideo è un dominio a ideali principali.*

Dimostrazione. Sia A un dominio euclideo e sia I un ideale di A. Dobbiamo mostrare che I è principale. Se $I = \{0\}$ questo è ovvio. Sia quindi $I \neq (0)$ e $d \neq 0$ un elemento di I tale che

$$\rho(d) \leq \rho(x), \quad \text{per ogni } x \in I,\ x \neq 0,$$

cioè d minimizza la ρ fra tutti gli elementi non nulli di I. Se $x \in I$, effettuando la divisione di x per d, abbiamo $x = qd+r$ per cui $r \in I$, con $\rho(r) < \rho(d)$. Per minimalità di d abbiamo che $r = 0$ e quindi $I = (d)$. □

Conseguenza: $\mathbb{Z}[X]$ non è un dominio euclideo. Infatti non è neanche un PID: abbiamo già visto che l'ideale $(2, X)$ non è principale.

Proposizione 9.8. *Sia A un dominio $a, b, d \in A$ tali che $(a, b) = (d)$. Allora (esiste un massimo comun divisore tra a e b e) $d = MCD(a, b)$.*

Dimostrazione. Siccome $(a, b) = (d)$ abbiamo che d è un divisore sia di a che di b. Inoltre, se $d'|a$ e $d'|b$ allora ogni elemento di (a, b) è diviso da d'. In particolare anche d e quindi $d = \mathrm{MCD}(a, b)$. □

Corollario 9.9. *Se A è un PID e $a, b \in A$ allora esiste $MCD(a, b)$ e $(a, b) = (MCD(a, b))$.*

Dimostrazione. Immediata dalla Proposizione 9.8. Infatti l'ideale (a, b) è principale e quindi esiste d tale che $(a, b) = (d)$. La Proposizione 9.8 ci assicura quindi che $d = \mathrm{MCD}(a, b)$. □

Attenzione: non è vero che se $d = MCD(a, b)$ allora $(a, b) = (d)$: ad esempio in $\mathbb{Z}[X]$ si può verificare che $1 = \mathrm{MCD}(2, X)$ e tuttavia $1 \notin (2, X)$.

Proposizione 9.10. *In qualunque dominio A, se $a|bc$ e $(a, b) = (1)$ allora $a|c$.*

Dimostrazione. Gli elementi di (a, b) sono quelli della forma $ar + bs$, $r, s, \in A$, per cui abbiamo in particolare $1 = ar + bs$ e moltiplicando per c concludiamo. □

Corollario 9.11. *In un PID (e quindi in ogni anello euclideo) gli irriducibili sono primi.*

Dimostrazione. Sia a irriducibile e $a|bc$. Siccome a è irriducibile i divisori di a sono solo gli elementi invertibili e gli associati di a. Si ha quindi $\mathrm{MCD}(a, b) = 1$ oppure $\mathrm{MCD}(a, b) = a$. Nel primo caso abbiamo anche $(a, b) = (1)$ dal Corollario 9.9 e concludiamo quindi dalla Proposizione 9.10 che $a|c$. Nel secondo caso abbiamo direttamente $a|b$. □

Esempio 9.12. Se d è dispari ≤ -3 allora $\mathbb{Z}[\sqrt{d}]$ non è euclideo. Infatti 2 è irriducibile (ha infatti norma 4 e non esistono elementi di norma 2). 2 però non è primo perché divide $(1 + \epsilon)(1 - \epsilon) = 1 - d$, ma non divide nessuno dei due fattori. Oppure si può verificare che l'ideale $(2, 1 + \epsilon)$ non è principale.

Definizione. Sia A un dominio e $a \in A$. Diciamo che a ammette una *scomposizione in fattori irriducibili* o una *fattorizzazione in elementi irriducibili* se esistono $r \in \mathbb{N}$ e $p_1, \ldots, p_r$ irriducibili tali che $a = p_1 \cdots p_r$.

Ci poniamo ora il problema dell'unicità della scomposizione in fattori irriducibili di un elemento. È chiaro ad esempio che in $\mathbb{Z}$ le fattorizzazioni di 6 date da $2 \cdot 3 = (-2) \cdot (-3) = 3 \cdot 2 = (-3) \cdot (-2)$ vanno considerate come la "stessa" fattorizzazione. Abbiamo quindi la seguente

Definizione. Sia A un dominio e $a \in A$. Diciamo che a ammette un'unica scomposizione in fattori irriducibili se ha una scomposizione in fattori irriducibili, e se $a = p_1 \cdots p_r = q_1 \cdots q_s$ sono due tali scomposizioni allora $r = s$ e, a meno di riordinare i fattori di una delle due, abbiamo p_i associato a q_i per ogni $i = 1, \ldots, r$.

Definizione. Un dominio A si dice *a fattorizzazione unica*, o *fattoriale*, se ogni elemento $a \in A$ non nullo e non invertibile ammette un'unica scomposizione in fattori irriducibili. Diciamo per brevità in tal caso che A è un UFD (unique factorization domain).

Teorema 9.13. *Se A è un PID allora è anche un UFD.*

Dimostrazione. (*Unicità.*) Vediamo in questa dimostrazione l'unicità. L'esistenza la vediamo più tardi trattando separatamente il caso euclideo, sensibilmente meno complicato. L'unicità deriva semplicemente dal fatto che ogni elemento irriducibile è anche primo. Infatti, supponiamo che $a = p_1 \cdots p_r = q_1 \cdots q_s$ e procediamo per induzione su $\min(r, s)$: se tale min è 1 abbiamo $p_1 = q_1 \cdots q_s$. Ma un elemento irriducibile non si può fattorizzare nel prodotto di due o più irriducibili e quindi abbiamo $s = 1$ e quindi le due espressioni si riducono a $p_1 = q_1$ e non abbiamo niente da dimostrare. Altrimenti, se tale minimo è > 1 abbiamo che $p_1 | q_1 \cdots q_s$ e quindi p_1 divide almeno uno tra $q_1, \ldots, q_s$. A meno di riordinare e rinominare i fattori q_i, possiamo assumere che p_1 divida q_1. Ma siccome q_1 è irriducibile questo implica che p_1 e q_1 sono associati, cioè esiste u invertibile tale che $p_1 = q_1 u$. Quindi, a meno di sostituire q_1 con $q_1 u$ e q_2 con $q_2 u^{-1}$, abbiamo $p_1 = q_1$ e quindi $p_1 \cdots p_r = q_1 q_2 q_3 \cdots q_s$ da cui segue $p_2 \cdots p_r = q_2 q_3 \cdots q_s$. Abbiamo quindi l'uguaglianza

tra due scomposizioni in fattori irriducibili con $r-1$ e $s-1$ fattori e quindi, per ipotesi induttiva, abbiamo che $r-1=s-1$, (cioè $r=s$) e che, a meno dell'ordine, p_i è associato a q_i per ogni $i=2,\dots,r$. □

Lemma 9.14. *Sia A un dominio euclideo e siano $b,c\in A$ non nulli e non invertibili. Allora $\rho(b)<\rho(bc)$.*

Dimostrazione. Ricordiamo dalla dimostrazione del Teorema 9.7 che ogni ideale di A non nullo è generato da un qualunque suo elemento che minimizza ρ tra gli elementi non nulli dell'ideale stesso. Dalla definizione di dominio euclideo abbiamo $\rho(b)\leq\rho(bc)$ e se per assurdo avessimo $\rho(b)=\rho(bc)$ avremmo che $(bc)=(b)$ da cui bc e b sono associati per la Proposizione 8.6 e quindi c è invertibile. □

Osserviamo che se un dominio euclideo è un campo allora $\rho(x)=\rho_0$ per ogni $x\neq 0$ per il Lemma 9.4. In particolare, se un dominio euclideo A non è un campo allora esiste $a\in A$ tale che $\rho(a)>\rho_0$.

Lemma 9.15. *Sia A un dominio euclideo che non è un campo e ρ_0 come nel Lemma 9.4. Sia ρ_1 tale che*

$$\rho_1=\min\{\rho(a):\ a\in A,\ a\neq 0,\ a\ \textit{non invertibile}\}.$$

Sia x tale che $\rho(x)=\rho_1$. Allora x è irriducibile.

Proof. Supponiamo per assurdo che x non sia irriducibile. Per il Lemma 9.4 abbiamo che x è riducibile e quindi esisterebbero b,c non invertibili tali che $x=bc$. Per il Lemma 9.14 avremmo $\rho(b)<\rho(x)$ e $\rho(c)<\rho(x)$. La minimalità di $\rho(x)$ implicherebbe tuttavia che b e c sono invertibili o nulli, contraddicendo l'ipotesi. □

Teorema 9.16. *Un anello euclideo A è un dominio a fattorizzazione unica.*

Dimostrazione. (*Esistenza.*)Mostriamo per induzione su $\rho(a)$ che ogni elemento a non nullo e non invertibile ammette una scomposizione in fattori irriducibili. Il minimo valore che può assumere $\rho(a)$ è ρ_1, come definito nel Lemma 9.15: in tal caso il lemma stesso ci garantisce che a è irriducibile e quindi non c'è niente da dimostrare.

Vediamo ora il passo induttivo, e assumiamo quindi $\rho(a)>\rho_1$. Se a è irriducibile non c'è niente da dimostrare. Altrimenti esistono b,c non nulli e non invertibili tali che $a=bc$. Il Lemma 9.14 ci garantisce quindi $\rho(b),\rho(c)<\rho(a)$ e per ipotesi induttiva sia b che c ammettono quindi una scomposizione in fattori irriducibili e il prodotto di queste ultime ci fornisce una scomposizione in fattori irriducibili per a. □

Per i PID la dimostrazione dell'esistenza è decisamente più delicata. Premettiamo un lemma che in una terminologia che non spieghiamo dice che un PID è un anello *nöetheriano.*

Lemma 9.17. *Sia A un PID e $d_1,d_2,\dots$ una successione di elementi di A tali che $d_{i+1}|d_i$ per ogni $i>0$. Allora esiste j_0 tale che gli elementi d_j, $j\geq j_0$ sono tutti associati fra loro.*

Dimostrazione. Consideriamo gli ideali generati dai d_i: abbiamo

$$(d_1)\subseteq(d_2)\subseteq(d_3)\subseteq\cdots.$$

Si verifica facilmente che l'unione di una successione di ideali ognuno contenuto nel successivo è ancora un ideale. Esiste quindi un elemento d tale che

$$\bigcup_{i>0}(d_i) = (d).$$

Sia quindi j_0 tale che $d \in (d_{j_0})$: abbiamo che per ogni $j \geq j_0$ $d_j \in (d)$ e quindi $d|d_j$; ma abbiamo anche $d \in (d_{j_0}) \subseteq (d_j)$ e quindi $d_j|d$ e concludiamo che tutti gli elementi d_j con $j \geq j_0$ sono associati a d. □

Dimostrazione. (*Esistenza per PID.*) Sia $a \in A$ non nullo e non invertibile. Mostriamo intanto che esiste p irriducibile tale che $p|a$. Infatti, se a non è irriducibile abbiamo che $a = d_1a_1$ con d_1 e a_1 non invertibili e non associati ad a. Se d_1 è irriducibile abbiamo completato, altrimenti possiamo fattorizzare $d_1 = d_2a_2$ e così via. Se ad un certo punto troviamo un d_i irriducibile abbiamo completato altrimenti otteniamo un assurdo perché avremmo ottenuto una successione infinita $d_1, d_2, \ldots$ che contraddice il Lemma 9.17.

Sia ora p_1 irriducibile tale che $a = p_1a_1$. Se a_1 è irriducibile abbiamo completato, altrimenti esiste p_2 irriducibile tale che $a_1 = p_2a_2$ e quindi $a = p_1p_2a_2$. Se ad un certo punto troviamo un elemento a_i irriducibile abbiamo finito altrimenti osserviamo che gli elementi a_i contraddirebbero il Lemma 9.17. □

Faccio presente in conclusione che esistono dei PID che non sono domini euclidei anche se trovare dei controesempi è piuttosto complicato. Un esempio è dato da $\mathbb{Z}[\omega]$, dove ω è un numero complesso radice del polinomio $x^2 - x + 5 = 0$, cioè ad esempio $\omega = \frac{1+\sqrt{19}i}{2}$. Una descrizione esplicita di $\mathbb{Z}[\omega]$ è data da

$$\mathbb{Z}[\omega] = \{a + b\frac{1+\sqrt{19}i}{2} : a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Si ha in effetti che $\mathbb{Z}[\omega]$ è un PID che non è un dominio euclideo, ma la verifica è piuttosto lunga e tecnica e quindi la omettiamo.

10. I primi gaussiani e somme di quadrati

In questa sezione affrontiamo dei problemi classici di teoria dei numeri che possono essere risolti utilizzando la teoria dei domini euclidei, ed in particolare il fatto che $\mathbb{Z}[i]$ è un dominio euclideo.

Cominciamo studiando la divisibilità negli interi gaussiani. Facciamo qualche osservazione nel caso di interi standard: siano $n, m, a, b \in \mathbb{Z}$. Allora

- $n|m$ in $\mathbb{Z}[i]$ se e solo se $n|m$ in $\mathbb{Z}$;
- $n|\, a + bi$ se e solo se $n|a$ e $n|b$.

Quando un primo p rimane primo in $\mathbb{Z}[i]$? Osserviamo che $2 = (1 + i)(1 - i)$ e quindi 2 non è primo in $\mathbb{Z}[i]$, mentre 3 rimane primo anche in $\mathbb{Z}[i]$ (ad esempio perché non esistono elementi di norma 3).

Lemma 10.1. *Un primo p rimane primo in $\mathbb{Z}[i]$ se e solo se non è somma di 2 quadrati.*

Dimostrazione. Se $p = a^2 + b^2$ allora $p = (a + bi)(a - bi)$ e quindi p non è primo in $\mathbb{Z}[i]$ (osservando che $a + bi$ e $a - bi$ non sono invertibili).

Viceversa, se $p = \alpha\beta$ con α e β non invertibili allora $N(\alpha) = N(\beta) = p$ e quindi p, essendo una norma, è somma di quadrati. □

Siamo ora pronti a caratterizzare i primi p che rimangono primi in $\mathbb{Z}[i]$.

Teorema 10.2. *Un primo $p \in \mathbb{N}$ rimane primo in $\mathbb{Z}[i]$ se e solo se $p \equiv 3 \mod 4$.*

Dimostrazione. Se $p = 2$ abbiamo già osservato che p non è primo in $\mathbb{Z}[i]$.

Osserviamo ora che quadrati in $\mathbb{Z}_4$ sono $0 = 0^2 = 2^2$ e $1 = 1^2 = 3^2$ e quindi la somma di due quadrati non può essere $\equiv 3 \mod 4$. Per il Lemma 10.1 concludiamo che se $p \equiv 3 \mod 4$ allora p rimane primo in $\mathbb{Z}[i]$.

Se $p \equiv 1 \mod 4$ sappiamo che -1 è un quadrato $\mod p$ per il Teorema 7.1 applicato al campo $\mathbb{Z}_p$ e quindi esiste n tale che $n^2 = -1 + kp$, da cui $p|n^2 + 1 = (n + i)(n - i)$. Ma p non divide né $n + i$ né $n - i$, non dividendone la parte immaginaria e quindi p non è primo. □

Corollario 10.3. *Un primo p è somma di due quadrati se e solo se $p = 2$ oppure $p \equiv 1 \mod 4$. Inoltre, se $p = 2$, esiste un'unica classe di associatura i cui elementi hanno norma 2, mentre se $p \equiv 1 \mod 4$ esistono esattamente due classi di associatura, una coniugata dell'altra, i cui elementi hanno norma p.*

Dimostrazione. Ci rimane da dimostrare solo l'ultima parte: se $p = 2$ gli elementi di norma 2 sono $\pm 1 \pm i$ e questi sono tutti associati tra di loro.

Se $p \equiv 1 \mod 4$ e supponiamo che esistano due elementi $x + iy$ e $a + ib$ di norma p, cioè tali che $(x + iy)(x - iy) = (a + ib)(a - ib) = p$; per l'unicità della scomposizione in fattori primi (gli elementi $(x + iy)$, $(x - iy)$, $(a + ib)$, $(a - ib)$ hanno tutti norma p e sono quindi irriducibili), abbiamo che $a + ib$ è associato ad uno tra $(x + iy)$ e $(x - iy)$. Abbiamo quindi al più due classi di associatura i cui elementi hanno norma p. Osserviamo inoltre che x ed y sono coprimi perché $p = N(x + iy) = x^2 + y^2$ è divisibile per $\mathrm{MCD}(x, y)^2$, e che almeno uno di essi ho valore assoluto ≥ 2: in particolare $x \neq \pm y$ e $x, y \neq 0$. Concludiamo che $x + iy$ e $x - iy$ non sono associati: gli associati di $x + iy$ sono $-x - iy$, $-y + ix$, $y - ix$ e questi elementi sono tutti distinti da $x - iy$. □

Per il Corollario 10.3 abbiamo che per ogni $p \equiv 1 \mod 4$ esiste un unico elemento $a + ib \in \mathbb{Z}[i]$ con $a < b$ tale che $a^2 + b^2 = N(a + ib) = p$. Denotiamo questo elemento con π_p. Abbiamo ad esempio $\pi_5 = 1 + 2i$ e $\pi_{29} = 2 + 5i$. Siamo ora pronti a classificare gli elementi primi di $\mathbb{Z}[i]$.

Teorema 10.4. *L'insieme $\mathcal{P}$ di elementi di $\mathbb{Z}[i]$ dato da*

$$\mathcal{P} = \{1 + i\} \cup \{p : p \equiv 3 \mod 4\} \cup \{\pi_p, \bar{\pi}_p, p \equiv 1 \mod 4\}$$

è un insieme di rappresentanti delle classi di associatura degli elementi primi di $\mathbb{Z}[i]$.

Dimostrazione. Sappiamo già dal Corollario 10.3 che gli elementi di $\mathcal{P}$ sono primi e a due a due non associati. Dobbiamo mostrare che non ci sono altri elementi primi. Sia quindi

$\alpha \in \mathbb{Z}[i]$ irriducibile. Ricordando che il coniugio è un automorfismo abbiamo che anche $\bar{\alpha}$ è irriducibile e quindi

$$N(\alpha) = \alpha\bar{\alpha}$$

e quest'ultima è la scomposizione in fattori irriducibili di $N(\alpha)$.

Ora, se $N(\alpha)$ è pari abbiamo $1+i|N(\alpha)$ e quindi $1+i$ è associato ad α o ad $\bar{\alpha}$.

Similmente, se $N(\alpha)$ è divisibile per p, con $p \equiv 1 \mod 4$ abbiamo $\pi_p|N(\alpha)$ e quindi π_p è associato ad α o ad $\bar{\alpha}$.

Infine, se $N(\alpha)$ è divisibile per p, con $p \equiv 3 \mod 4$ abbiamo che $p|N(\alpha)$ e quindi p è associato ad α o ad $\bar{\alpha}$.

□

Vogliamo ora dedurre il seguente classico risultato di teoria dei numeri.

Teorema 10.5 (Fermat)**.** *Un numero intero positivo è somma di due quadrati se e solo se nella sua scomposizione in fattori irriducibili i numeri primi* $\equiv 3 \mod 4$ *compaiono con esponente pari.*

Dimostrazione. Le somme di due quadrati sono le norme di interi gaussiani e quindi basta mostrare che un numero intero positivo n è la norma di un intero gaussiano se e solo se nella sua scomposizione in fattori irriducibili i numeri primi $\equiv 3 \mod 4$ compaiono con esponente pari.

Sia quindi $n = N(\alpha)$ e scomponiamo α in fattori irriducibili in $\mathbb{Z}[i]$: abbiamo, a meno di associati,

$$\alpha = (1+i)^a \prod_{p\equiv 1} \pi_p^{a_{p,1}} \bar{\pi}_p^{a_{p,2}} \prod_{p\equiv 3} p^{a_p},$$

dove gli esponenti sono opportuni interi non negativi quasi tutti nulli (cioè quelli non nulli sono in numero finito). Ne segue

$$n = N(\alpha) = 2^a \prod_{p\equiv 1} p^{a_{p,1}+a_{p,2}} \prod_{p\equiv 3} p^{2a_p},$$

da cui n è della forma desiderata. Supponiamo ora che n abbia tale forma, cioè che

$$n = 2^a \prod_{p\equiv 1} p^{a_p} \prod_{p\equiv 3} p^{2a_p}.$$

Poniamo

$$\alpha = (1+i)^a \prod_{p\equiv 1} \pi_p^{a_p} \prod_{p\equiv 3} p^{a_p}$$

e abbiamo chiaramente $N(\alpha) = n$ e quindi n è somma di due quadrati.

□

Un'altra applicazione classica riguarda le terne pitagoriche.

Definizione. Siano a, b, c interi positivi. Diciamo che (a, b, c) è una *terna pitagorica* se $a < b$ e $a^2 + b^2 = c^2$. Tale terna pitagorica si dice *primitiva* se $\mathrm{MCD}(a, b) = 1$.

Osserviamo che se (a, b, c) è una terna pitagorica primitiva allora (na, nb, nc) è una terna pitagorica. Viceversa se (a, b, c) è una terna pitagorica e $d = \mathrm{MCD}(a, b)$ allora d è un divisore di c e si ha che $(a/d, b/d, c/d)$ è una terna pitagorica primitiva. Sarà quindi sufficiente limitare la nostra attenzione alle terne pitagoriche primitive.

Lemma 10.6. *Se (a, b, c) è una terna pitagorica primitiva e p è un primo che divide c, allora $p \equiv 1 \mod 4$.*

Dimostrazione. Se $p = 2$ abbiamo che a e b sono entrambi dispari (se fossero entrambi pari la terna non sarebbe primitiva). Allora $c^2 \equiv 0 \mod 4$ mentre $a^2 \equiv b^2 \equiv 1 \mod 4$, e queste condizioni sono incompatibili. Possiamo quindi assumere che c sia dispari e quindi che uno tra a e b è pari e l'altro è dispari.

Supponiamo ora che $p|c$ con $p \equiv 3$. Ricordiamo che tale elemento p è primo in $\mathbb{Z}[i]$ e quindi, siccome $p|c^2 = (a+ib)(a-ib)$, abbiamo che p divide almeno uno tra $a+ib$ e $a-ib$: ma in entrambi i casi abbiamo $p|a$ e $p|b$ per l'osservazione fatta all'inizio della sezione, contraddicendo l'ipotesi che (a, b, c) è primitiva. □

Teorema 10.7. *Sia c intero positivo. Allora esiste una terna pitagorica primitiva della forma (a, b, c) se e solo se c è prodotto di primi $\equiv 1 \mod 4$. In tal caso, se i primi distinti che compaiono nella fattorizzazione di c sono m, esistono esattamente 2^{m-1} terne pitagoriche primitive distinte della forma (a, b, c).*

Dimostrazione. Per il Lemma 10.6 sappiamo già che la condizione su c è necessaria. Supponiamo ora che

$$c = \prod_{p \equiv 1} p^{a_p}.$$

Possiamo quindi scrivere la decomposizione di c in fattori irriducibili in $\mathbb{Z}[i]$:

$$c = \prod_{p \equiv 1} \pi_p^{a_p} \bar{\pi}_p^{a_p}$$

e quindi quella di c^2:

$$c^2 = \prod_{p \equiv 1} \pi_p^{2a_p} \bar{\pi}_p^{2a_p}$$

e ponendo $\alpha = \prod_{p \equiv 1} \pi_p^{2a_p} = a + ib$ abbiamo $c^2 = \alpha\bar{\alpha} = N(\alpha)$ da cui $c^2 = a^2 + b^2$. Supponiamo ora che esista un numero primo p tale che $p|a$ e $p|b$. Per ipotesi sappiamo che $p \equiv 1$ e quindi sia π_p che $\bar{\pi}_p$ dividono $\alpha = a + ib$. Ma α non contiene fattori irriducibili coniugati e quindi otterremmo una contraddizione.

Per mostrare l'ultima parte della dimostrazione denotiamo con $p_1, \ldots, p_m$ i primi distinti che dividono c. Per ogni sottoinsieme $S \subseteq \{p_1, p_2, \ldots, p_m\}$ poniamo

$$\alpha_S = \prod_{p \in S} \pi_p^{2a_p} \prod_{p \notin S} \bar{\pi}_p^{2a_p}.$$

L'elemento α nella prima parte della dimostrazione corrisponde ad $S = \{p_1, p_2, \ldots, p_m\}$. Mostriamo ora che se (a, b, c) è una terna pitagorica primitiva allora $a + ib$ è associato ad

uno tra gli α_S e che se $S, S' \subseteq \{p_1, \dots, p_m\}$ allora α_S è associato ad $\alpha_{S'}$ se e solo se $S = S'$ e α_S è associato al coniugato di $\alpha_{S'}$ se e solo se S e S' sono complementari.

Supponiamo quindi che (a, b, c) sia una terna pitagorica primitiva. Allora

$$(a + ib)(a - ib) = \prod_{p \equiv 1} \pi_p^{2a_p} \bar{\pi}_p^{2a_p}.$$

Si ha $\pi_p | a + ib$ se e solo se $\bar{\pi}_p | a - ib$ (perché il coniugio è un automorfismo) e similmente scambiando π_p con $\bar{\pi}_p$. Inoltre non può accadere che π_p e $\bar{\pi}_p$ dividano entrambi $a + ib$ perché in tal caso avremmo $p|a$ e $p|b$. Ne segue che $\pi_p^{2a_p}$ divide $a+ib$ e $\bar{\pi}_p$ non divide $a+ib$ o viceversa, e concludiamo che $a + ib = \alpha_S$ per qualche S.

L'ultima parte segue dall'unicità della scomposizione in fattori irriducibili.

Esempio 10.8. Esiste una sola terna pitagorica primitiva della forma $(a, b, 5)$, una della forma $(a, b, 13)$, una della forma $(a, b, 17)$ e una della forma $(a, b, 25)$; tali terne sono $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$, $(7, 24, 25)$.

Esistono invece due terne pitagoriche della forma $(a, b, 65)$: sono $(33, 56, 65)$ e $(16, 63, 65)$. Vediamo come abbiamo ottenuto queste due terne. Si ha $65 = 5 \cdot 13 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)$ e questa è la scomposizione in irriducibili, da cui abbiamo

$$65^2 = (2 + i)^2(2 - i)^2(3 + 2i)^2(3 - 2i)^2.$$

Seguendo la dimostrazione del teorema dobbiamo calcolare $\alpha = (2 + i)^2(3 + 2i)^2$ e $\beta = (2 + i)^2(3 - 2i)^2$. Otteniamo $\alpha = -33 + 56i$ e $\beta = 63 - 16i$.

□

11. Polinomi

Definizione. Sia A un anello e X un simbolo. Un polinomio f a coefficienti in A nella variabile X è una scrittura simbolica del tipo

$$f = a_0X^0 \dot{+} a_1X^1 \dot{+} a_2X^2 \dot{+} \cdots = \dot{\sum_i} a_iX^i$$

dove $a_1, a_2, \dots \in A$ e per cui esiste $n_0 \in \mathbb{N}$ tale che $a_n = 0$ per ogni $n \geq n_0$. Indichiamo con $A[X]$ l'insieme dei polinomi a coefficienti in A nella variabile X. In questa notazione il simbolo $\dot{+}$ va interpretato semplicemnete come un simbolo che separa i vari termini del polinomio, e non come un simbolo di addizione. Similmente per il simbolo di sommatoria con il punto.

Notazione: se $a_0, \dots, a_n \in A$ scrivendo $a_0X^0 \dot{+} a_1X^1 \dot{+} \cdots \dot{+} a_nX^n$ intendiamo il polinomio

$$a_0X^0 \dot{+} a_1X^1 \dot{+} a_2X^2 \dot{+} \cdots \dot{+} a_nX^n \dot{+} 0X^{n+1} \dot{+} 0X^{n+2} \dot{+} \cdots .$$

Il simbolo X^1 viene spesso sostituito dal più semplice simbolo X. Il simbolo X^0 può essere talvolta omesso così come tutti i termini del tipo $0X^i$ per cui, ad esempio,

$$a_0 \dot{+} a_1X \dot{+} a_3X^3 = a_0X^0 \dot{+} a_1X^1 \dot{+} 0X^2 \dot{+} a_3X^3$$

In particolare, per ogni $a \in A$ con il simbolo a intendiamo anche il polinomio dato da

$$aX^0 \dot{+} 0X \dot{+} 0X^2 \dot{+} \cdots,$$

identificando quindi A con un sottoinsieme di $A[X]$.

Sull'insieme dei polinomi $A[X]$ consideriamo le seguenti operazioni di somma e prodotto $+$ e $\cdot$:

$$(\dot{\sum_i} a_i X^i) + (\dot{\sum_i} b_i X^i) = \dot{\sum_i} (a_i + b_i) X^i$$

e

$$(\dot{\sum_i} a_i X^i) \cdot (\dot{\sum_i} b_i X^i) = \dot{\sum_i} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) X^i.$$

Lemma 11.1. *Si ha che $(A[X], +, \cdot)$ è un anello commutativo unitario.*

Dimostrazione. Tutte le verifiche sono elementari, ancorché piuttosto noiose. □

Osserviamo a questo punto che con le nostre notazioni abbiamo che il simbolo $\dot{+}$ può essere sostituito dal più semplice $+$ dato dalla somma in $A[X]$ come anello:

$$aX^i \dot{+} bX^j = aX^i + bX^j,$$

per cui non utilizzeremo più il simbolo $\dot{+}$ e similmente per il simbolo di sommatoria. Se a questo punto ti stai chiedendo "e allora perché l'ha introdotto?" ritorna indietro, rifletti, e cerca di darti una risposta.

Siamo abituati sin dalla scuola secondaria a lavorare con i polinomi, ma non dobbiamo tralasciare alcuni particolari: nel nostro contesto un polinomio è una scrittura simbolica e non va confuso con la "funzione" che gli potremo associare sostituendo la variabile con un determinato valore, e che è stata il principale utilizzo dei polinomi fino ad ora. Torneremo comunque più avanti su questo aspetto.

Se $f = \sum a_i X^i$ è un polinomio indichiamo con $[f]_i := a_i$ il *coefficiente* di X^i in f, detto anche coefficiente di grado i. Il *termine noto* di un polinomio è $[f]_0$, il suo coefficiente di grado 0.

Il *grado* di un polinomio $f \neq 0$ è dato da $\deg(f) = \max\{i \in \mathbb{N} : [f]_i \neq 0\}$. Se un polinomio non nullo ha grado n il *coefficiente direttore* di f è $[f]_n$. Un polinomio non nullo si dice *monico* se il suo coefficiente direttore è 1.

Il grado del polinomio nullo non viene definito, anche se talvolta si pone per convenzione $\deg(0) = -\infty$.

Un monomio è un polinomio f tale che esiste un unico $i \in \mathbb{N}$ per cui $[f]_i \neq 0$. I monomi di grado 0 vengono anche detti costanti e, come già detto, vengono identificati con gli elementi di A.

Lemma 11.2. *Siano f e g polinomi non nulli in $A[X]$. Allora*

- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$*;*
- $\deg(fg) \leq \deg(f) + \deg(g)$*.*

Inoltre, se A è un dominio si ha $\deg(fg) = \deg(f) + \deg(g)$*.*

Dimostrazione. Lasciata al lettore. □

Proposizione 11.3. *Se A è un dominio anche $A[X]$ lo è.*

Dimostrazione. Segue direttamente dal Lemma 11.2. □

Proposizione 11.4. *Se A è un dominio gli elementi invertibili sono le costanti invertibili*

Dimostrazione. Segue dalle proprietà dei gradi che un elemento invertibile deve avere necessariamente grado 0 e il risultato segue. □

Attenzione: se A non è un dominio la Proposizione 11.4 non è vera e si può dimostrare che questa proposizione è vera se e solo se A è ridotto, cioè non ha elementi nilpotenti. Ad esempio in $\mathbb{Z}_4[X]$, infatti, $(2X+1)^2 = 1$ e quindi $2X+1$ è invertibile. Più in generale se $a \in A$ è nilpotente, $a^n = 0$, abbiamo $(-aX+1)(1+aX+a^2X^2+\cdots a^{n-1}X^{n-1}) = 1$. Dimostrare il viceversa, cioè che se un anello è ridotto allora gli unici elementi invertibili sono le costanti è un po' più complicato.

Indichiamo con A^A l'insieme di tutte le funzioni di dominio A e codominio A.

Proposizione 11.5. *Sia A un anello e consideriamo su A^A le operazioni di somma e prodotto date da:*

- $(f+g)(a) = f(a) + g(a)$;
- $(fg)(a) = f(a)g(a)$,

per ogni $f, g \in A^A$ e per ogni $a \in A$. Allora A^A è un anello commutativo unitario.

Dimostrazione. Lo 0 è la funzione nulla e l'1 è la funzione costante 1. L'opposto di f è dato da $(-f)(a) = -f(a)$. Tutte le proprietà discendono dalle analoghe proprietà di A. □

Proposizione 11.6. *L'applicazione*

$$A[X] \to A^A$$

che a $f \in A[X]$ associa la funzione $\tilde{f} \in A^A$ data dalla valutazione di f, cioè se $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ allora $\tilde{f}(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n$ per ogni $a \in A$, è un omomorfismo di anelli.

Dimostrazione. Si ha $\tilde{1} = 1$. Si ha inoltre:

$$\widetilde{(f+g)}(a) = \sum (a_i + b_i)a^i = \sum a_ia^i + \sum b_ia^i = \tilde{f}(a) + \tilde{g}(a) = (\tilde{f} + \tilde{g})(a)$$

e

$$\widetilde{(fg)}(a) = \sum_i (\sum_{j=0}^{i} a_jb_{j-i})a^i = \sum_i (\sum_{j=0}^{i} a_ja^jb_{j-i}a^{j-i}) = (\sum a_ia^i)(\sum b_ja^j) = \tilde{f}(a)\tilde{g}(a) = (\tilde{f}\tilde{g})(a).$$

□

Una *funzione polinomiale* è una funzione del tipo $\tilde{f}$ per qualche $f \in A[X]$. Osserviamo che l'applicazione $f \mapsto \tilde{f}$ non è in generale iniettiva. Ad esempio, infatti, se A è finito si ha che $A[X]$ è infinito mentre A^A è finito. Anche se A è infinito può accadere che $f \mapsto \tilde{f}$ non sia iniettiva: ad esempio se prendiamo come A l'anello delle funzioni da $\mathbb{N}$ a $\mathbb{Z}_2$, si ha che se $f = X^2 - X$ allora $\tilde{f} = 0$. Vedremo però che questo non può accadere se A è un campo.

12. Polinomi a coefficienti in un campo

In questa sezione studiamo il caso in cui l'anello dei coefficienti A è un campo e lo indicheremo quindi con K, come d'abitudine. Osserviamo innanzitutto che in ogni classe di associatura (non nulla) di $K[X]$ esiste un unico polinomio monico. Faremo quindi spesso riferimento unicamente ai polinomi monici per quel che riguarda questioni di divisibilità. Mostriamo intanto il teorema più importante che riguarda la struttura algebrica di $K[X]$.

Teorema 12.1. *$K[X]$ è un dominio euclideo.*

Dimostrazione. Prendiamo come $\rho = \deg$ sui polinomi non nulli, e poniamo per convenzione $\rho(0) = -1$. La proprietà $\rho(f) \leq \rho(fg)$ per ogni $f, g \neq 0$ è immediatamente verificata per la proprietà del grado di un prodotto. Dobbiamo quindi mostrare che dati $f, g \in K[X]$, con $g \neq 0$, esistono $q, r \in K[X]$ tali che $f = qg + r$ con $\rho(r) < \rho(g)$. Osserviamo intanto che possiamo supporre che g sia monico. Questo segue dal fatto che i polinomi monici rappresentano le classi di associatura oppure si può verificare direttamente: infatti, se $g = b\bar{g}$, con $b \in K$ e $\bar{g}$ monico abbiamo che se $f = q\bar{g}+r$ allora $f = qb^{-1}b\bar{g}+r = (b^{-1}q)g+r$.

Supponiamo quindi g monico e procediamo per induzione su $\deg(f)$.

Passo base: $\deg f = 0$, cioè f è una costante. Se anche $g = k$ è una costante basta prendere $q = fk^{-1}$ e $r = 0$. Se invece g non è costante possiamo prendere $q = 0$ e $r = f$.

Passo induttivo: supponiamo $\deg f > 0$ e chiamiamo a il coefficiente direttore di f. Se $\deg f < \deg g$ basta scegliere $q = 0$ e $r = f$. Altrimenti, se $\deg f \geq \deg g$, possiamo trovare $n \geq 0$ tale che f e $aX^n g$ sono polinomi dello stesso grado e con lo stesso coefficiente direttore, e quindi $\deg(f - aX^n g) < \deg(f)$. Per ipotesi induttiva abbiamo che esistono q', r tali che

$$f - aX^n g = q'g + r$$

da cui $f = (q' + aX^n)g + r$. □

Gli elementi q ed r nella divisione in $K[X]$ sono univocamente determinati, a differenza di quanto capitava in $\mathbb{Z}[i]$ (e in $\mathbb{Z}$). Infatti, supponiamo che

$$q_1 g + r_1 = q_2 g + r_2.$$

con le condizioni sui gradi. Abbiamo $(q_1 - q_2)g = r_2 - r_1$. Se $r_1 \neq r_2$ (e quindi anche $q_1 \neq q_2$) avremmo

$$\deg(g) > \deg(r_2 - r_1) = \deg(q_1 - q_2) + \deg(g) \geq \deg(g).$$

Corollario 12.2. *Un polinomio in $K[X]$ è primo se e solo se è irriducibile; inoltre $K[X]$ è un dominio a ideali principali e quindi anche a fattorizzazione unica.*

I polinomi di primo grado sono sempre irriducibili: questo segue direttamente dal Lemma 11.2 sul grado del prodotto di polinomi.

Osserviamo che la divisione con resto si può sempre fare se g è monico, anche se A non è un campo: basta riadattare la dimostrazione del Teorema 11.1. Di conseguenza:

Teorema 12.3. *Sia A un anello, $a \in A$ e $f \in A[X]$, $f \neq 0$. Allora esiste $g \in A[X]$ tale che $f = (X-a)g$ se e solo se $\tilde{f}(a) = 0$.*

Dimostrazione. Basta effettuare la divisione

$$f = q(X-a) + r$$

dove r è una costante. Se $\tilde{f}(a) = 0$ allora $r = 0$ e quindi $(X-a)|f$. Il viceversa è ovvio. □

Se $f \in A[X]$ e $a \in A$ diciamo che a è una *radice* del polinomio f se $\tilde{f}(a) = 0$. Se a è radice di un polinomio $f \neq 0$ la molteplicità di a in f è

$$\mu(a, f) = \max\{n : (X-a)^n | f\}.$$

Per il Teorema 12.3 la molteplicità di una radice è sempre > 0.

Proposizione 12.4. *Un polinomio irriducibile in $K[X]$ ha una radice se e solo se ha grado 1.*

Dimostrazione. Segue direttamente dal Teorema 12.3. □

Teorema 12.5. *La somma delle molteplicità delle radici di un polinomio non nullo in $K[X]$ è $\leq$ del grado.*

Dimostrazione. Viene direttamente dal fatto che $K[X]$ è a fattorizzazione unica e che i polinomi $X-a$ e $X-b$ sono associati se e solo se $a = b$. □

Questo teorema non vale se K non è un campo. Ad esempio in $\mathbb{Z}_8[X]$ sappiamo che il polinomio $X^2 - 1$ ha 4 radici di molteplicità 1. Conseguenza: se K è un campo infinito allora l'applicazione $f \mapsto \tilde{f}$ è iniettiva: infatti se $\tilde{f} = 0$ avremmo che ogni elemento di K è una radice di f contraddicendo il Teorema 12.5. Deduciamo ora un'importante conseguenza sulla struttura del gruppo moltiplicativo in un campo che ci sarà utile più avanti. Se K è un campo indichiamo con $K^* = \mathcal{U}(K)$ il gruppo moltiplicativo degli elementi non nulli in K.

Corollario 12.6. *Sia K un campo e G un sottogruppo finito di K^*. Allora G è ciclico. In particolare se K è finito allora K^* è un gruppo ciclico.*

Dimostrazione. Per la Proposizione 1.9 è sufficiente mostrare che per ogni d esiste al più un sottogruppo di G con d elementi. Se esistessero due sottogruppi distinti di G aventi la stessa cardinalità d la loro unione conterrebbe almeno $d+1$ elementi. Questi $d+1$ elementi sarebbero tutti radici del polinomio $X^d - 1$ contraddicendo il Teorema 12.5.

In alternativa, senza richiamare il criterio visto sui gruppi ciclici, si potrebbe procedere nel seguente modo, utilizzando un po' di teoria dei gruppi. Osserviamo il seguente fatto: se G è un gruppo abeliano finito, $|G| = n$, consideriamo l'insieme parzialmente ordinato P dato dagli ordini degli elementi di G, ordinati per divisibilità. Mostriamo che P ha un unico elemento massimale; infatti, supponiamo che r, s siano elementi massimali in P: ne segue che esistono $g, h \in G$ di ordine rispettivamente r e s. Se $d = \mathrm{MCD}(r, s)$ consideriamo l'elemento $g^d h$: questo ha ordine rs/d (perché?), da cui, per massimalità di r ed s deduciamo che necessariamente $r = s = d$.

Ora applichiamo questo fatto al sottogruppo finito G di K^*: se l'elemento massimo di P è d abbiamo che tutti gli elementi di G sono radici del polinomio $X^d - 1$ e per il Teorema 12.5 abbiamo che $d = n$ cioè G ha un elemento di ordine n e quindi G è ciclico. □

Se ci poniamo delle questioni analoghe nel caso in cui l'anello dei coefficienti è un dominio A avremmo una risposta immediata se A fosse contenuto in un campo K. In questo caso infatti se un polinomio ha coefficienti in A ha anche coeffcienti in K e quindi non può avere più radici di quanto è il suo grado e un sottogruppo finito di $\mathcal{U}(A)$ è anche sottogruppo di K^* e quindi è automaticamente ciclico. È questo quindi un buon momento per introdurre il *campo dei quozienti* di un dominio. Tale campo sarà un'estensione del dominio di partenza e lo costruiamo esplicitamente prendendo come modello il caso dei numeri interi e dei numeri razionali.

Consideriamo l'insieme dei simboli $\frac{a}{b}$ con $a, b \in A$, $b \neq 0$. Su questo insieme di simboli introduciamo la seguente relazione, che si verifica banalmente essere di equivalenza:

$$\frac{a}{b} \sim \frac{c}{d} \text{ se e solo se } ad = bc.$$

Chiamiamo $Q(A)$ l'insieme delle classi di equivalenza.

Teorema 12.7. *Le operazioni su $Q(A)$ date da*

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

e

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

sono ben poste e danno a $Q(A)$ la struttura di campo. Inoltre l'insieme degli elementi della forma $\frac{a}{1}$ formano un sottoanello isomorfo ad A.

Dimostrazione. Lasciata al lettore. □

Il campo $Q(A)$ si dice *campo dei quozienti* del dominio A. Come è naturale aspettarsi, se un dominio A è contenuto in un campo L allora L contiene un sottocampo isomorfo a $Q(A)$ e contenente A.

Proposizione 12.8. *Sia A un dominio, L un campo $A \subset L$. Allora l'intersezione K di tutti i sottocampi di L contenenti A è isomorfa a $Q(A)$.*

Proof. Si ha che K è un campo in quanto intersezione non vuota di sottocampi. Mostriamo intanto che

$$K = \{ab^{-1} : a, b \in A.b \neq 0\}.$$

Sia quindi $\tilde{K} = \{ab^{-1} : a, b \in A, b \neq 0\}$. Se un sottocampo di L contiene A allora necessariamente deve contenere tutti gli inversi degli elementi non nulli di A e quindi tutti gli elementi di $\tilde{K}$. Abbiamo quindi che $\tilde{K}$ è contenuto in ogni sottocampo contenente A e quindi $\tilde{K} \subset K$. Per vedere che $K \subset \tilde{K}$ è sufficiente mostrare che $\tilde{K}$ è un sottocampo contenente A. Il fatto che $A \subset \tilde{K}$ è chiaro: basta considerare gli elementi con $b = 1$. Vediamo che $\tilde{K}$ è un sottocampo:

- $1 \in \tilde{K}$: chiaro;
- $a_1b_1^{-1}$, $a_2b_2^{-1} \in \tilde{K}$ allora $a_1b_1^{-1} - a_2b_2^{-1} = a_1b_1^{-1}b_2b_2^{-1} - a_2b_2^{-1}b_1b_1^{-1} = (a_1b_2 - a_2b_1)(b_1b_2)^{-1} \in \tilde{K}$.
- Analogamente si ha $a_1b_1^{-1} \cdot a_2b_2^{-1} \in \tilde{K}$;
- Infine ogni elemento di $\tilde{K}$ ha inverso in $\tilde{K}$: chiaro.

Rimane quindi da mostrare che $Q(A) \cong K$. Basta mostrare che

$$\varphi : Q(A) \to K$$

data da $\varphi(\frac{a}{b}) = ab^{-1}$ è ben posta e che è un isomorfismo di campi: tutte le verifiche sono elementari e lasciate al lettore. □

Ritorniamo ora allo studio delle radici e dell'irriducibilità di un polinomio. La seguente definizione non dovrebbe stupire.

Definizione. Se $P = \sum a_iX^i$ è un polinomio in $K[X]$ definiamo la sua *derivata* con la formula

$$P' = \sum_{i>0} ia_iX^{i-1}$$

Non ci sono né limiti, né rapporti incrementali, il nostro campo può anche essere finito! Osserviamo che in generale il grado della derivata è il grado del polinomio meno 1, ma ciò non è vero in caratteristica positiva, in cui il grado può diminuire anche di più. Ad esempio se $carK = p$ abbiamo che la derivata di X^p è 0.

Valgono tuttavia delle regole che ben conosciamo per le derivate di funzioni reali.

Lemma 12.9. *La derivata è K-lineare (ricordiamo che $K[X]$ è uno spazio vettoriale su K). Vale inoltre la regola di Leibniz per il prodotto:*

$$(FG)' = F'G + FG'$$

Dimostrazione. Se $F = \sum a_iX^i$ e $G = \sum b_iX^i$ e $a, b \in K$ abbiamo

$$\begin{aligned}(aF + bG)' &= (\sum (aa_i + bb_i)X^i)' = \sum i(aa_i + bb_i)X^{i-1} = a\sum ia_iX^{i-1} + b\sum ib_iX^{i-1} \\ &= aF' + bG'.\end{aligned}$$

Grazie alla linearità è sufficiente mostrare la regola di Leibniz solo nel caso in cui $F = X^j$ e $G = X^k$. Infatti se la regola vale per F_1, G e per F_2, G allora vale anche per $aF_1 + bF_2, G$:

$$\begin{aligned}((aF_1 + bF_2)G)' &= (aF_1G + bF_2G)' = a(F_1G)' + b(F_2G)' = \\ &= a(F_1'G + F_1G') + b(F_2'G + F_2G') \\ &= (aF_1 + bF_2)'G + (aF_1 + bF_2)G'\end{aligned}$$

Verfichiamo la formula per X^j e X^k:

$$(X^jX^k)' = (X^{j+k})' = (j + k)X^{j+k-1} = jX^{j-1}X^k + kX^jX^{k-1}.$$

□

Osserviamo in particolare che la derivata di $(X-a)^m$ è $m(X-a)^{m-1}$: questo deriva direttamente dalla regola di Leibniz e una piccola induzione: infatti

$$((X-a)^m)' = (X-a)'(X-a)^{m-1} + (X-a)(m-1)(X-a)^{m-2} = m(X-a)^{m-1}$$

Il risultato più importante che riguarda la derivata di un polinomio è il seguente

Teorema 12.10. *Sia $f \in K[X]$, $f \neq 0$, e $a \in K$ una radice di f. Allora a è radice multipla di f (cioè ha molteplicità > 1) se e solo se è radice anche di f'.*

Dimostrazione. Sia $m \geq 1$ la molteplicità di a come radice di f. Abbiamo per definizione $f = (X-a)^m g$, con $\tilde{g}(a) \neq 0$. Abbiamo

$$f' = m(X-a)^{m-1}g + (X-a)^m g'.$$

Se $m > 1$ abbiamo $\tilde{f'}(a) = 0$. Se $m = 1$ abbiamo $\tilde{f'}(a) = \tilde{g}(a) \neq 0$. □

Corollario 12.11. *Se $car(K)|n$ allora $X^n - X$ non ha radici multiple.*

Dimostrazione. Infatti in tal caso la derivata del polinomio è -1 e il risultato segue dal teorema precedente. □

Consideriamo ora due campi K ed L con $K \subset L$. Diciamo in questo caso semplicemente che $K \subset L$ è un'estensione di campi. Siano inoltre $f \in K[X]$ e $\alpha \in L$. Diciamo che α è una radice di f se α è una radice di f come polinomio in $L[X]$.

Osservazione importante: siano $f, g \in K[X]$ e $K \subseteq L$ campi. Allora un MCD(f,g) in $K[X]$ è anche un MCD(f,g) in $L[X]$: questo perché il MCD lo possiamo ottenere tramite l'algoritmo euclideo delle divisioni successive e l'algoritmo produce lo stesso risultato sia pensando i coefficienti in K, sia pensandoli in L. Da questo segue, ad esempio, che due polinomi a coefficienti razionali sono coprimi (cioè hanno MCD uguale a 1) in $\mathbb{Q}[X]$ se e solo se lo sono in $\mathbb{C}[X]$.

Proposizione 12.12. *Sia K un campo e $f \in K[X]$ tale che $MCD(f, f') = 1$. Allora f non ha radici multiple (in nessun campo L contenente K).*

Dimostrazione. Ricordiamo che la derivata e il MCD possono essere calcolati considerando indifferentemente i polinomi con coefficienti in K o in L e quindi è sufficiente mostrare il caso $K = L$.

Ma è chiaro che se a è una radice di f allora $X - a$ è un divisore di f che non può essere anche un divisore di f' perché f e f' sono coprimi. Quindi a non è una radice di f' e quindi, per il Teorema 12.10, a non è una radice multipla di f. □

Corollario 12.13. *Sia $f \in K[X]$ irriducibile, con $f' \neq 0$. Allora f non ha radici multiple in nessuna estensione L di K. In particolare, se K è un campo a caratteristica 0 ogni polinomio irriducibile non ha radici multiple (in nessuna estensione L di K).*

Proof. Se $f' \neq 0$ abbiamo che $MCD(f, f')$ ha grado al più $\deg(f') < \deg(f)$. Essendo f irriducibile gli unici divisori di f di grado strettamente minore di $\deg(f)$ sono le costanti e quindi $MCD(f, f') = 1$. Il risultato segue dalla Proposizione 12.12. □

Osserviamo infine che nel Corollario 12.13 la condizione $f' \neq 0$ in caratteristica p equivale a richiedere che f non è un polinomio in X^p.

Il prossimo risultato è una parziale inversione della Proposizione 12.12.

Proposizione 12.14. *Sia $f \in K[X]$ un polinomio e supponiamo che esista un'estensione $K \subset L$ tale che f si fattorizza nel prodotto di polinomi di primo grado in $L[X]$. Supponiamo che f non abbia radici multiple in L. Allora $MCD(f, f') = 1$.*

Proof. Ancora una volta, siccome la derivata e il MCD non dipendono dal campo, possiamo assumere $K = L$ e quindi che f si fattorizzi nel prodotto di polinomi di primo grado. Se f non ha radici multiple nessun fattore irriducibile di f divide f' per il Teorema 12.10 e quindi $MCD(f, f') = 1$. □

Vedremo più avanti che dato un polinomio $f \in K[X]$ non costante esiste sempre un campo L in cui f si può scrivere come prodotto di polinomi di primo grado per cui la prima ipotesi della Proposizione 12.14 è sempre automaticamente soddisfatta.

13. Polinomi a coefficienti reali e complessi

I campi più "semplici" da studiare da un punto di vista algebrico sono quelli i cui polinomi irriducibili hanno tutti grado 1 e sono quindi in corrispondenza biunivoca con gli elementi di K (a meno di associati).

Definizione. Un campo K si dice *algebricamente chiuso* se ogni polinomio di grado positivo in $K[X]$ ammette una radice in K.

Vogliamo ora mostrare che il campo $\mathbb{C} = \mathbb{R}[i]$ è algebricamente chiuso. Vediamo prima un caso particolare.

Lemma 13.1. *Dato $z \in \mathbb{C}$ e $k \in \mathbb{Z}$, $k \neq 0$, esiste $\omega \in \mathbb{C}$ tale che $\omega^k = z$.*

Dimostrazione. Questo segue immediatamente dal teorema di De Moivre. Infatti, se $z = re^{i\theta}$, con $r \in \mathbb{R}_{\geq 0}$ e $\theta \in \mathbb{R}$ basta scegliere $\omega = r^{1/k} e^{\frac{i\theta}{k}}$. □

Ricordiamo anche le disuguaglianze triangolari :$|z| - |w| \leq |z + w| \leq |z| + |w|$ per ogni $w, z \in \mathbb{C}$, dove $|z|$ indica il modulo del numero complesso z.

Teorema 13.2 (Fondamentale dell'algebra)**.** *Il campo $\mathbb{C}$ è algebricamente chiuso.*

Dimostrazione. Lo dimostriamo con un pizzico di analisi. Vogliamo mostrare che, se $f \in \mathbb{C}[X]$ allora la funzione $|\tilde{f}|$ ammette minimo e che tale minimo è 0. Intanto mostriamo che ammette minimo. Abbiamo $f = a_0 + a_1 X + \cdots + a_n X^n$ da cui

$$|\tilde{f}(z)| = |a_0 + a_1 z + \cdots + a_n z^n| \geq |a_n||z|^n - |a_1||z|^1 - \cdots - |a_{n-1}||z|^{n-1}$$

per ogni $z \in \mathbb{C}$, per le disuguaglianze triangolari. Abbiamo quindi che $|\tilde{f}(z)|$ tende a $+\infty$ per $|z|$ che tende a $+\infty$. Ne segue che esiste $R > 0$ tale che per $|z| > R$ si ha $|f(z)| > |f(0)|$. Deduciamo che $|\tilde{f}|$ ammette inf nella palla chiusa di raggio R e quindi ammette minimo per il teorema di Weierstrass.

A meno di una traslazione possiamo assumere che $|\tilde{f}|$ ammetta minimo in 0. Inoltre, assumendo per assurdo che tale minimo non sia 0, a meno di moltiplicare f per uno scalare non nullo, possiamo anche assumere che $\tilde{f}(0) = 1$.

Sia quindi $f = 1 + a_k X^k + X^{k+1} g(X)$ con $a_k \neq 0$ e $k \geq 1$. Per il Lemma 13.1 esiste ω tale che $\omega^k = -a_k^{-1}$. Fissiamo tale ω e abbiamo

$$f(r\omega) = 1 - r^k + (r\omega)^{k+1} g(r\omega),$$

dove abbiamo iniziato ad omettere il simbolo $\sim$ per indicare la funzione anziché il polinomio, per ogni $r > 0$. Siccome $g(r\omega)$ è limitato per $0 < r \leq 1$ abbiamo $|r^{k+1}\omega^{k+1} g(r\omega)| \leq cr^{k+1}$ per un'opportuna costante reale positiva c per ogni $r \leq 1$. Scegliendo ora $r < \min\{1, 1/c\}$ (per cui $cr - 1 < 0$) abbiamo

$$|f(r\omega)| \leq |1 - r^k| + |(r\omega)^{k+1} g(r\omega)| \leq 1 - r^k + cr^{k+1} = 1 + r^k(cr - 1) < 1$$

contraddicendo le ipotesi. □

Passiamo quindi a studiare la riducibilità di polinomi a coefficienti reali. La situazione è ancora abbastanza semplice. Abbiamo

Proposizione 13.3. *Un polinomio $f \in \mathbb{R}[X]$ è irriducibile se e solo se ha grado 1 oppure ha grado 2 e non ammette radici reali (cioè ha discriminante negativo).*

Dimostrazione. Infatti se un polinomio irriducibile $f \in \mathbb{R}[X]$ ha grado maggiore di 2, sia α una sua radice in $\mathbb{C}$. Osserviamo che anche $\bar{\alpha}$ è una radice di f; infatti se $f = a_0 + a_1 X + \cdots + a_n X^n$ e $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ allora, ricordando che il coniugio è un automorfismo di anello in ogni estensione quadratica e quindi in particolare in $\mathbb{R}[i] = \mathbb{C}$ abbiamo:

$$0 = \overline{a_0 + a_1\alpha + \cdots + a_n\alpha^n} = a_0 + a_1\bar{\alpha} + \cdots + a_n\bar{\alpha}^n$$

e quindi anche $\bar{\alpha}$ è radice di f. Ne segue che $(X-\alpha)(X-\bar{\alpha})$ divide f: ma $(X-\alpha)(X-\bar{\alpha}) = X^2 - 2Re(\alpha)X + \alpha\bar{\alpha}$ è un polinomio a coefficienti reali e quindi f non è irriducibile. □

Ad esempio il polinomio $X^4 + 1$ non ammette radici reali. Le radici complesse sono le radici quarte di -1 e sono quindi $\frac{\sqrt{2}}{2}(\pm 1 \pm i)$ e in effetti, ponendo $\alpha = \frac{\sqrt{2}}{2}(1 + i)$ e $\beta = \frac{\sqrt{2}}{2}(-1 + i)$ abbiamo che le radici di $X^4 + 1$ sono $\alpha, \bar{\alpha}, \beta, \bar{\beta}$. Abbiamo quindi che la fattorizzazione di $X^4 + 1$ in $\mathbb{R}[X]$ è

$$X^4 + 1 = ((X - \alpha)(X - \bar{\alpha}))((X - \beta)(X - \bar{\beta})) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

14. Polinomi interi e razionali

Trattiamo in questa sezione il problema dell'irriducibilità di polinomi a coefficienti in $\mathbb{Z}$ e in $\mathbb{Q}$. Tuttavia, tutte le definizioni, i risultati e le dimostrazioni possono essere generalizzate sostituendo a $\mathbb{Z}$ un qualunque dominio a fattorizzazione unica A e a $\mathbb{Q}$ il suo campo dei quozienti $Q(A)$. In particolare, ad esempio, possiamo leggere $\mathbb{Z}[i]$ al posto di $\mathbb{Z}$ e $\mathbb{Q}[i]$ al posto di $\mathbb{Q}$.

Vediamo prima un semplice criterio per determinare le radici di un polinomio in $\mathbb{Q}[X]$.

Lemma 14.1. *Sia $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ con $a_n \neq 0$ e sia $\frac{r}{s} \in \mathbb{Q}$, con $MCD(r,s) = 1$, una radice di f. Allora $r|a_0$ e $s|a_n$.*

Dimostrazione. Infatti, nelle ipotesi date, si ha, calcolando $\tilde{f}(r/s)$ e moltiplicando per s^n,

$$a_0s^n + a_1s^{n-1}r + \cdots + a_nr^n = 0$$

da cui il risultato segue. □

Ad esempio, se $f = 3+5X+5X^2+2X^3$ abbiamo che le radici razionali di f sono necessariamente della forma r/s con $r = \pm1, \pm3$ e $s = \pm1, \pm2$, cioè sono $\pm1, \pm3, \pm1/2, \pm3/2$. E in effetti si verifica facilmente che l'unica radice razionale è $-3/2$. Se andiamo a dividere il polinomio f per $X - 3/2$ otteniamo

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

Osserviamo che la fattorizzazione in $\mathbb{Q}[X]$ può in questo caso essere modificata in una fattorizzazione in $\mathbb{Z}[X]$ semplicemente moltiplicando i due fattori per una costante. Uno dei prossimi obiettivi è quello di mostrare che questo è sostanzialmente sempre possibile.

Un polinomio $P \in \mathbb{Z}[X]$ si dice un polinomio intero.

Un polinomio intero si dice *primitivo* se i suoi coefficienti non hanno fattori in comune. Ogni polinomio intero si scrive in modo unico come

$$f = c(f)f^{\#}$$

dove $c(f) \in \mathbb{N}$ e $f^{\#}$ è un polinomio intero primitivo; $c(f)$ si dice il *contenuto* di f. Il contenuto di f è un MCD di tutti i coefficienti di f.

Teorema 14.2. *Siano f e g polinomi interi. Allora $c(fg) = c(f)c(g)$. In particolare il prodotto di polinomi primitivi è ancora primitivo.*

Dimostrazione. Se $f = c(f)f^{\#}$ e $g = c(g)g^{\#}$ abbiamo

$$fg = c(f)c(g)f^{\#}g^{\#}$$

e basta quindi mostrare che il prodotto $f^{\#}g^{\#}$ è ancora primitivo, cioè che il prodotto di due polinomi primitivi è primitivo.

Assumiamo quindi che f e g siano primitivi e supponiamo per assurdo che p sia un primo che divide tutti i coefficienti di fg; sia i minimo tale che il coefficiente a_i di f non è divisibile per p e j minimo tale che il coefficiente b_j di g non sia divisibile per p. Allora, il coefficiente di grado $i + j$ in fg non può essere divisibile per p. □

Teorema 14.3. *$f \in \mathbb{Z}[X]$ primitivo, $g \in \mathbb{Q}[X]$, tali che $fg \in \mathbb{Z}[X]$. Allora $g \in \mathbb{Z}[X]$.*

Dimostrazione. Sia $d \in \mathbb{N}_{>0}$ tale che $dg \in \mathbb{Z}[X]$. Si ha $d|c(fdg)$ in quanto fg è intero. Ma $c(fdg) = c(f)c(dg) = c(dg)$ perché f è primitivo e quindi $d|c(dg)$. Questo vuol dire che tutti i coefficienti di dg sono divisibili per d e quindi che $g \in \mathbb{Z}[X]$. □

Supponiamo ora che $f \in \mathbb{Z}[X]$. Ci chiediamo che legame c'è tra l'irriducibilità di f in $\mathbb{Z}[X]$ e l'irriducibilità di f come polinomio in $\mathbb{Q}[X]$. È chiaro che se $f = f_1f_2$ con $f_1, f_2 \in \mathbb{Z}[X]$ allora tale fattorizzazione vale anche in $\mathbb{Q}[X]$, ma può accadere che f_1 sia

irriducibile in $\mathbb{Z}[X]$ ma invertibile in $\mathbb{Q}[X]$: questo capita se f_1 è una costante. Ad esempio il polinomio $2X$ è riducibile in $\mathbb{Z}[X]$ ma irriducibile in $\mathbb{Q}[X]$. Se invece i polinomi f_1 e f_2 hanno entrambi grado positivo questi non possono essere invertibili in $\mathbb{Q}[X]$ e quindi f è riducibile anche in $\mathbb{Q}[X]$.

Molto più interessante è il problema contrario. Supponiamo che il polinomio $f \in \mathbb{Z}[X]$ sia riducibile in $\mathbb{Q}[X]$. Possiamo dedurre che è riducibile anche in $\mathbb{Z}[X]$? La risposta è affermativa ed è il contenuto del seguente famoso risultato.

Corollario 14.4 (Lemma di Gauss)**.** *Un polinomio intero è riducibile in $\mathbb{Q}[X]$ se e solo se è prodotto di due polinomi interi di grado positivo. Un polinomio primitivo è irriducibile in $\mathbb{Q}[X]$ se e solo se lo è in $\mathbb{Z}[X]$.*

Dimostrazione. Sia $h \in \mathbb{Z}[X]$ e $f, g \in \mathbb{Q}[X]$ non invertibili tali che $h = fg$. A meno di moltiplicare f per una costante razionale (e di dividere g per la stessa costante) possiamo assumere che f sia intero primitivo. Il Teorema 14.3 allora ci assicura che g è anche intero. Il viceversa è ovvio.

Supponiamo ora che h sia primitivo: se è riducibile in $\mathbb{Q}[X]$ lo è anche in $\mathbb{Z}[X]$ per la prima parte. Se è irriducibile in $\mathbb{Q}[X]$, ma non in $\mathbb{Z}[X]$ vuol dire che si può scrivere come prodotto di due polinomi di cui almeno uno è costante (altrimenti la fattorizzazione sarebbe "valida" anche in $\mathbb{Q}[X]$) e quindi non può essere primitivo. □

Vogliamo ora dimostrare che $\mathbb{Z}[X]$ è un UFD. Prima però enunciamo il seguente teorema che caratterizza gli UFD e che abbiamo sostanzialmente già dimostrato qualche settimana fa.

Proposizione 14.5. *Sia A un dominio in cui ogni elemento non nullo e non invertibile si scrive come prodotto di elementi irriducibili. Allora A è un dominio a fattorizzazione unica se e solo se gli elementi irriducibili di A sono primi.*

Dimostrazione. Se gli elementi irriducibili sono primi l'unicità discende nello stesso modo in cui abbiamo dimostrato l'unicità nei PID (e infatti in quel caso abbiamo utilizzato solo che che gli irriducibili sono primi).

Viceversa, se abbiamo unicità di fattorizzazione sia $x \in A$ irriducibile: vogliamo mostrare che è anche primo. Se $x|ab$ allora esiste c tale che $xc = ab$ e fattorizzando c, a, b in irriducibili abbiamo $xc_1 \cdots c_r = a_1 \cdots a_s b_1 \cdots b_t$ dove tutti gli elementi a_i, b_i, c_i sono irriducibili. Per unicità concludiamo che x è associato ad uno tra gli a_i o tra i b_i e quindi $x|a$ oppure $x|b$. □

Teorema 14.6. *$\mathbb{Z}[X]$ è un dominio a fattorizzazione unica.*

Dimostrazione. Sia $h \in \mathbb{Z}[X]$ un polinomio non nullo e non invertibile (cioè $h \neq 0, \pm 1$). Consideriamo la fattorizzazione di h in irriducibili di $\mathbb{Q}[X]$ (che esiste ed è unica perché $\mathbb{Q}[X]$ è euclideo):

$$h = f_1 \cdots f_r$$

dove gli f_i sono irriducibili in $\mathbb{Q}[X]$. Sia $q_i \in \mathbb{Q}$ tale che $q_i f_i$ è un polinomio intero primitivo. Abbiamo

$$h = \frac{1}{q_1 \cdots q_r}(q_1 f_1) \cdots (q_r f_r).$$

Il polinomio $(q_1 f_1) \cdots (q_r f_r)$ è un polinomio primitivo, essendo prodotto di primitivi, per il Teorema 14.2. Abbiamo quindi che il polinomio intero h si scrive come prodotto tra il polinomio razionale $\frac{1}{q_1 \cdots q_r}$ e il polinomio primitivo $(q_1 f_1) \cdots (q_r f_r)$: ne segue per il Teorema 14.3 che $\frac{1}{q_1 \cdots q_r} \in \mathbb{Z}$. Abbiamo quindi ottenuto una fattorizzazione di h nella forma

$$h = n h_1 \cdots h_r$$

dove gli h_i sono polinomi primitivi irriducibili in $\mathbb{Q}[X]$ e quindi anche in $\mathbb{Z}[X]$ e $n \in \mathbb{Z}$. Fattorizzando n in primi irriducibili abbiamo ottenuto una fattorizzazione in irriducibili di h.

Per l'unicità basta quindi mostrare che gli irriducibili sono primi, grazie alla Proposizione 14.5. Sia quindi h un polinomio irriducibile in $\mathbb{Z}[X]$ e $h | fg$. Se h è una costante abbiamo che $h = p$ dove p è un numero primo. Abbiamo quindi che $p | c(fg) = c(f)c(g)$ e quindi che $p | c(f)$ oppure $p | c(g)$ e quindi $p | f$ oppure $p | g$. Se h ha grado positivo abbiamo che h è primitivo e irriducibile in $\mathbb{Q}[X]$. Ne segue che h divide f o g in $\mathbb{Q}[X]$ e quindi anche in $\mathbb{Z}[X]$, per il Teorema 14.3. □

Tutti i risultati fin qui esposti in questa sezione valgono mutatis mutandis considerando al posto di $\mathbb{Z}$ un qualsiasi dominio a fattorizzazione unica A e al posto di $\mathbb{Q}$ il campo $Q(A)$ dei quozienti di A. Abbiamo in particolare il seguente risultato.

Teorema 14.7. *Se A è un dominio a fattorizzazione unica, allora anche $A[X]$ lo è. In particolare l'anello dei polinomi $K[X, Y] := (K[X])[Y]$ è a fattorizzazione unica.*

Osserviamo che $K[X, Y]$, non è un dominio a ideali principali: infatti l'ideale (X, Y) non è principale. Anche $\mathbb{Z}[X]$ non è a ideali principali in quanto $(2, X)$ non lo è. Si ha in effetti che $A[X]$ è a ideali pincipali se e solo se A è un campo. Infatti, se A è un campo allora $A[X]$ è euclideo. Viceversa, se A non è un campo allora esiste $a \in A$ non nullo e non invertibile. Allora l'ideale (a, X) non può essere principale.

Vediamo ora un semplice e utile criterio di irriducibilità per un polinomio a coefficienti interi.

Proposizione 14.8 (Criterio di Eisenstein)**.** *Sia $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, $a_n \neq 0$, e p un primo che divide $a_0, \ldots, a_{n-1}$ e $p^2 \nmid a_0$. Allora f è irriducibile.*

Dimostrazione. Supponiamo $a_0 + a_1 X + \cdots + a_n X^n = (b_0 + b_1 X + \cdots + b_k X^k)(c_0 + c_1 X + \cdots + c_h X^h)$. Si ha $b_0 c_0 = a_0$ e quindi $p | b_0$ e $p \nmid c_0$. Si mostra per induzione che $p | b_i$ per ogni i: infatti $a_i = b_0 c_i + \cdots + b_{i-1} c_1 + b_i c_0$. E questo è chiaramente un assurdo perché avremmo anche a_n divisibile per p. □

Questo criterio ci permette di determinare una prima famiglia infinita di polinomi irriducibili.

Corollario 14.9. *$f = X^{p-1} + X^{p-2} + \cdots + 1$ è irriducibile in $\mathbb{Q}[X]$.*

Dimostrazione. Osserviamo che basta mostrare che il polinomio $f(X+1)$ è irriducibile. Abbiamo $f(X)(X-1) = X^p - 1$ da cui

$$f(X+1)X = (X+1)^p - 1 = \sum_{k=0}^{p} \binom{p}{k} X^k - 1$$

da cui, dividendo per X, abbiamo:

$$f(X+1) = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$$

che soddisfa le ipotesi del criterio di Eisenstein.

□

Il polinomio $X^{p-1} + X^{p-2} + \cdots + 1$ è un esempio di polinomio ciclotomico, cioè un esempio di polinomio irriducibile le cui radici sono tutte radici dell'unità.

Proposizione 14.10. *Esiste un'unica famiglia di polinomi interi monici* $\{C_n \in \mathbb{Z}[X] : n \in \mathbb{N}_{>0}\}$ *tali che le radici complesse di* C_n *sono le radici primitive* n*-esime dell'unità, tutte con molteplicità 1.*

Dimostrazione. Abbiamo per esempio $C_1 = X - 1$, $C_2 = X + 1$. L'unicità è chiara: viene semplicemente dal fatto che

$$C_n = \prod (X - a)$$

dove il prodotto è esteso a tutte le radici primitive n esime dell'unità cioè tutti i numeri complessi della forma $e^{\frac{2k\pi i}{n}}$, dove k è un intero compreso tra 1 ed n e coprimo con n. Segue anche che $\deg(C_n) = \phi(n)$, dove ϕ è la funzione di Eulero. Per dimostrare che C_n ha coefficienti interi procediamo per induzione. Abbiamo che

$$X^n - 1 = \prod_{d|n} C_d.$$

Abbiamo quindi $C_n = \frac{X^n-1}{\prod_{d|n,\, d<n} C_d}$: per induzione il denominatore è un polinomio monico a coefficienti interi; ma la divisione tra polinomi monici in $\mathbb{Z}[X]$ è ancora un polinomio monico in $\mathbb{Z}[X]$ e il risultato segue. □

Segue dalla dimostrazione che se p è un primo $C_p = \frac{X^p-1}{X-1} = X^{p-1} + \cdots + 1$ che è irriducibile per quanto visto prima. Abbiamo anche che $C_4 = \frac{X^4-1}{C_1C_2} = X^2 + 1$ che è irriducibile. Altri due esempi: $C_6 = \frac{X^6-1}{C_1C_2C_3} = \frac{(X+1)(X^2-X+1)(X-1)(X^2+X+1)}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1$ che è irriducibile perché non ha radici razionali e $C_8 = X^4 + 1$ che sappiamo essere irriducibile avendolo visto in un esercizio. È possibile dimostrare che tutti i polinomi ciclotomici sono irriducibili, ma non lo facciamo.

15. Estensioni di un omomorfismo agli anelli di polinomi

Le seguenti proprietà dell'anello dei polinomi sono di fondamentale importanza.

Teorema 15.1. *Siano A e B anelli e $\phi : A \to B$ un omomorfismo. Allora la funzione $A[X] \mapsto B[X]$ data da*

$$\varphi(\sum a_i X^i) = \sum \phi(a_i) X^i$$

è ancora un omomorfismo di anelli.

Dimostrazione. Abbiamo $\varphi(1) = 1$,

$$\varphi\big(\sum a_i X^i + \sum b_i X^i\big) = \varphi\big(\sum (a_i + b_i) X^i\big) = \sum (\phi(a_i) + \phi(b_i)) X^i = \varphi(\sum a_i X^i) + \varphi(\sum b_i X^i)$$

e

$$\varphi(\sum a_i X^i \cdot \sum b_i X^i) = \varphi(\sum_k \sum_{j=0}^{k} (a_j + b_{k-j}) X^k) = \sum_k (\sum_{j=0}^{k} \phi(a_j)\phi(b_{k-j})) X^k = \varphi(\sum a_i X^i) \cdot \varphi(\sum b_i X^i)$$

□

Se A è un anello e $a \in A$ poniamo $v_a : A[X] \to A$ data da $v_a(f) := \tilde{f}(a)$ e chiamiamo v_a la *valutazione* in a. Osserviamo che v_a è un omomorfismo di anelli. Infatti $v_a(1) = 1$ e,

$$v_a(f + g) = \widetilde{f + g}(a) = (\tilde{f} + \tilde{g})(a) = \tilde{f}(a) + \tilde{g}(a) = v_a(f) + v_a(g)$$

dove abbiamo utilizzato che $f \mapsto \tilde{f}$ è un omomorfimo e la definizione di somma in A^A. Lo stesso calcolo funziona sostituendo il $+$ con il $\cdot$.

Corollario 15.2. *Se A e B sono anelli e $\phi : A \to B$ omomorfismo. Per ogni $b \in B$ esiste un unico omomorfismo $\psi : A[X] \to B$ tale che $\psi(a) = \phi(a)$ per ogni $a \in A$ e $\psi(X) = b$*

Dimostrazione. L'unicità è data dal fatto che ψ deve essere un omomorfismo e quindi

$$\psi(a_0 + a_1 X + \cdots + a_n X^n) = \phi(a_0) + \phi(a_1) b + \cdots + \phi(a_n) b^n.$$

D'altra parte la funzione definita in questo modo non è altri che $\psi = v_b \circ \varphi$, dove φ è l'omomorfismo costruito nel Teorema 15.1, e quindi è un omomorfismo perché composizione di omomorfismi. □

16. Polinomi su campi finiti

Esempi di polinomi irriducibili di grado 2: in caratteristica 2 abbiamo $X^2 + X - c$ è irriducibile per qualche c. In caratteristica dispari abbiamo che $X^2 - c$ è irriducibile per qualche c. In caratteristica dispari basta scegliere c non quadrato. In caratteristica 2 basta mostrare che la funzione $a \mapsto a^2 + a$ è 2:1 (infatti a e $a + 1$ hanno la stessa immagine per ogni a) e quindi non è suriettiva.

Esempi di polinomi irriducibili in $\mathbb{Z}_2[X]$ di grado ≤ 3. Li possiamo ottenere ricorsivamente: abbiamo che $1, X, 1 + X$ sono irriducibili. In grado 2 otteniamo polinomi riducibili andando a moltiplicare quelli di grado 1 con se stessi. L'unico polinomio che non si ottiene in questo modo è $1 + X + X^2$ che è quindi irriducibile . Moltiplicando tra loro i polinomi

irriducibili di primo e secondo grado otteniamo sei polinomi riducibili di terzo grado per cui gli unici irriducibili sono i rimanenti due: $1 + X + X^3$ e $1 + X^2 + X^3$.

Riduzione modulo p di un polinomio intero. Ricordiamo che se $\phi : A \to B$ è un omomorfismo di anelli questo si estende ad un omomorfismo $\varphi : A[X] \to B[X]$ (Teorema 15.1).

Lemma 16.1. *Sia A un dominio e $\phi : A \to B$ un omomorfismo di anelli. Sia $f \in A[X]$ tale che $f = f_1 f_2$. Sia a il coefficiente direttore di f e supponiamo che $\phi(a) \neq 0$. Allora $\varphi(f)$ si fattorizza in $B[X]$ nel prodotto di due polinomi di grado* $\deg(f_1)$ *e* $\deg(f_2)$.

Dimostrazione. Per ipotesi abbiamo che $\varphi(f) = \varphi(f_1)\varphi(f_2)$. Detti b e c i coefficienti direttori di f_1 e di f_2 rispettivamente abbiamo che $a = bc$ e quindi che $\phi(a) = \phi(b)\phi(c)$. Di conseguenza abbiamo che $\phi(b)$ e $\phi(c)$ sono entrambi non nulli e quindi che $\deg(\varphi(f_1)) = \deg(f_1)$ e similmente per f_2. □

Se $\phi : \mathbb{Z} \to \mathbb{Z}_p$ è l'omomorfimso di proiezione e $f \in \mathbb{Z}[X]$ chiamiamo $\varphi(f)$ la riduzione di f modulo p. Ad esempio, se $f = 9X^3 + 5X^2 - 3X + 2$ e $\phi : \mathbb{Z} \to \mathbb{Z}_5$ abbiamo $\varphi(f) = 4x^3 + 2X + 2 \in \mathbb{Z}_5[X]$. Siccome $\varphi(f)$ non ammette radici in $\mathbb{Z}_5$ esso è irriducibile in $\mathbb{Z}_5$ e quindi f, essendo primitivo, è irriducibile in $\mathbb{Z}[X]$.

Corollario 16.2. *Sia $f \in \mathbb{Z}[X]$ un polinomio primitivo e $p \in \mathbb{N}$ tale che p non divide il coefficiente direttore di f. Se f è prodotto di due polinomi di grado r, s anche la sua riduzione modulo p è prodotto di due polinomi di grado r ed s. In particolare se la riduzione modulo p è irriducibile anche f lo è.*

Questo corollario può anche essere utilizzato per (ri)dimostrare il criterio di Eisenstein o che il prodotto di polinomi primitivi è primitivo. Infatti, se $f \in \mathbb{Z}[X]$ soddisfa le condizioni del criterio di Eisenstein allora la sua riduzione modulo p è aX^n. Se f si fattorizza nel prodotto di due polinomi di grado positivo in $\mathbb{Z}[X]$ questi devono essere una potenza di X se ridotti modulo p. Questo vuol dire che il loro termine noto è divisibile per p e quindi il termine noto di f sarebbe divisibile per p^2, contraddicendo le ipotesi.

Un'altra applicazione consiste nel (ri)dimostrare che il prodotto di primitivi è ancora primitivo. Infatti, se fg non è primitivo abbiamo che esiste $p > 0$ che divide tutti i coefficienti di fg e quindi $\varphi(fg) = 0$ in $\mathbb{Z}_p[X]$. Ma $\mathbb{Z}_p[X]$ è un dominio e quindi $\varphi(f) = 0$ oppure $\varphi(g) = 0$, e quindi almeno uno tra f e g sarebbe non primitivo.

Esempio 16.3. Consideriamo il polinomio $f = X^4 - 3X^3 - X^2 + 1 \in \mathbb{Z}[X]$. Si fattorizza in $\mathbb{Z}_2[X]$ come $(X + 1)(X^3 + X + 1)$. Se fosse riducibile in $\mathbb{Z}[X]$ sarebbe come prodotto di un polinomio di grado 1 e uno di grado 3. Ma ciò non può essere (non ha soluzioni razionali) e quindi è irriducibile.

Esempio 16.4. $X^4 + 1$ è irriducibile in $\mathbb{Z}[X]$ ma riducibile mod p per ogni primo p Che $X^4 + 1$ sia irriducibile in $\mathbb{Z}[X]$ lo abbiamo già visto. Per dimostrare la seconda parte abbiamo bisogno del seguente risultato

Lemma 16.5. *Sia K un campo finito e $a, b \in K^*$. Allora ab è un quadrato se e solo se sia a che b lo sono oppure nessuno dei due lo è.*

Dimostrazione. Se $car(K) = 2$ ogni elemento è un quadrato e il risultato è banale. In caratteristica dispari ricordiamo che K^* è un gruppo ciclico di cardinalità pari, e denotiamo con x un generatore. I quadrati di K^* sono chiaramente le potenze con esponente pari di x e i non quadrati le potenze con esponente dispari. Il risultato segue. □

Torniamo ora all'esempio di $X^4 + 1$. Dal lemma abbiamo che almeno uno tra -1, 2 e -2 è un quadrato in $\mathbb{Z}_p$ e questo ci permette sempre di determinare una fattorizzazione di $X^4 + 1$: infatti se $a^2 = -1$ abbiamo $X^4 + 1 = (X^2 + a)(X^2 - a)$. Se $a^2 = \pm 2$ abbiamo $X^4 + 1 = X^2 + aX \pm 1)(X^2 - aX \pm 1)$.

Più in generale possiamo chiederci quando un polinomio biquadratico è irriducibile.

Esempio 16.6. Consideriamo il polinomio $f = X^4 + 2\alpha X^2 + \beta \in K[X]$. Allora f è prodotto di due polinomi di secondo grado se e solo se una delle seguenti condizioni è soddisfatta:

- $\alpha^2 - \beta$ è un quadrato in K;
- esistono $a, b \in K$ tali che $b^2 = \beta$ e $a^2 = 2b - 2\alpha$.

Vediamo che le condizioni sono sufficienti: se $\alpha^2 - \beta = \delta^2$ abbiamo

$$X^4 + 2\alpha X^2 + \beta = (X^2 + \alpha + \delta)(X^2 + \alpha - \delta);$$

in questo caso abbiamo semplicemente risolto l'equazioni biquadratica, cioè quadratica in X^2. Se a, b sono tali che $b^2 = \beta$ e $a^2 = 2b - 2\alpha$ abbiamo

$$X^4 + 2\alpha X^2 + \beta = (X^2 + aX + b)(X^2 - aX + b).$$

Viceversa, supponiamo che $X^4 + 2\alpha X^2 + \beta$ si fattorizzi nel prodotto di due polinomi di secondo grado:

$$X^4 + 2\alpha X^2 + \beta = (X^2 + aX + b)(X^2 + cX + d)$$

con $a, b, c, d \in K$. Abbiamo allora che, uguagliando i rispettivi coefficienti, il seguente sistema è soddisfatto:

$$\begin{cases} a + c = 0 \\ d + ac + b = 2\alpha \\ ad + bc = 0 \\ bd = \beta \end{cases}$$

Dalla prima equazione otteniamo che $c = -a$ e sostituendo nella terza otteniamo $a(b-d) = 0$ per cui $a = 0$ oppure $b = d$.

Se $a = 0$ otteniamo $b + d = 2\alpha$ e $bd = \beta$ da cui segue che $\alpha^2 - \beta$ è un quadrato (facendo attenzione in caratteristica 2).

Se $b = d$ abbiamo dalla quarta equazione $b^2 = \beta$ e dalla seconda $a^2 = 2b - 2\alpha$.

Come applicazione della riduzione modulo p di un polinomio mostriamo che i polinomi ciclotomici sono irriducibili. Facciamo prima un lemma preliminare.

Lemma 16.7. *Sia $n \geq 1$, A l'insieme delle radici primitive n-esime, $B \subseteq A$, $B \neq \emptyset$ tale che per ogni $\zeta \in B$ e per ogni primo p tale che $MCD(p, n) = 1$ si ha $\zeta^p \in B$. Allora $A = B$.*

Proof. Ricordiamo che le radici di $\Phi_n(X)$ sono proprio i generatori del gruppo ciclico di ordine n dato dalle radici n-esime dell'unitá. Data una qualunque radice primitiva ζ possiamo ottenere tutte le altre elevando ζ ad un esponente coprimo con n. Sia quindi $\zeta \in B$ e $\zeta' \in A$. Per quanto detto esistono primi $p_1, \dots, p_r$ (non necessariamente distinti) tali che $\zeta' = \zeta^{p_1 \cdots p_r}$. Abbiamo $\zeta^{p_1} \in B$ per ipotesi e quindi anche $(\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2} \in B \dots$ e quindi anche $\zeta' \in B$. □

Teorema 16.8. *Il polinomio ciclotomico $\Phi_n(X)$ é irriducibile per ogni $n \geq 1$.*

Proof. Poniamo $P(X) = X^n - 1$. Sia f un fattore irriducibile di $\Phi_n(X)$ e supponiamo per assurdo che non tutte le radici primitive n-esime siano radici di f. Per il Lemma abbiamo che esiste una radice ζ di f e un primo p che non divide n tale che ζ^p non é radice di f. Sia ora g il polinomio irriducibile che abbia ζ^p come radice. Osserviamo che f e g sono distinti irriducibili e che fg divide Φ_n e quindi P. Osserviamo inoltre che ζ é radice del polinomio $g(X^p)$ per cui esiste un polinomio h tale che

$$g(X^p) = h(X)f(X)$$

Riducendo questa identitá modulo p otteniamo

$$\overline{g(X^p)} = \bar{g}^p = \bar{h}\bar{f}.$$

Di conseguenza, se π é un un fattore irriducibile di $\bar{f}$ esso é anche un fattore irriducibile di $\bar{g}$, $\bar{P}$ sarebbe divisibile per π^2 e quindi $\bar{P}'$ sarebbe divisibile per π. Ma $\bar{P}' = nX^{n-1}$ é coprimo con $\bar{P}$ e quindi abbiamo ottenuto un assurdo. □

17. Quozienti di $K[X]$

Se K è un campo sappiamo che ogni ideale in $K[X]$ è principale e quindi sarà della forma (f). Vogliamo ora studiare il quoziente $K[X]/(f)$.

Proposizione 17.1. *Sia $f \in K[X]$, $n = \deg(f) > 0$. Allora $K[X]/(f)$ è un K-spazio vettoriale di dimensione n che contiene (un sottocampo isomorfo a) K.*

Dimostrazione. Consideriamo le classi degli elementi $1, X, \dots, X^{n-1}$: questi sono un insieme di generatori per $K[X]/(f)$. Infatti, ogni polinomio g è congruente $\mod f$ al resto nella divisione per f e sarà quindi congruente ad un polinomio di grado minore di n, cioè ad una combinazione lineare di $1, X, \dots, X^{n-1}$. Inoltre ogni combinazione lineare non nulla di $1, X, \dots, X^{n-1}$ non può essere congruente a 0 per l'unicità del quoziente q e del resto r nella divisione per f.

Il fatto che $K[X]/(f)$ contenga una copia di K è immediato: le classi rappresentate dai polinomi di grado 0 sono chiaramente tutte distinte (la differenza di due costanti distinte non può essere un multiplo di f) e quindi formano un campo isomorfo a K. □

Osserviamo che se ϕ è un omomorfismo tra due anelli A e B che contengono K, e ϕ fissa gli elementi di K, allora ϕ è anche un'applicazione lineare tra K-spazi vettoriali.

Che struttura può avere il quoziente $K[X]/(f)$? Quando è un campo?

Formalizziamo una proprietà che abbiamo visto in un esercizio in passato. Se A è un anello diciamo che un suo ideale I è *massimale* se $I \neq A$ e gli unici ideali di A che contengono I sono proprio I ed A.

Lemma 17.2. *Sia A un anello e I un suo ideale. Allora A/I è un campo se e solo se I è massimale.*

Dimostrazione. Osserviamo che un campo K contiene esattamente due ideali, $\{0\}$ e K. Infatti, se un ideale I di K contiene un elemento non nullo, essendo quest'ultimo invertibile, si ha necessariamente $I = K$ per il Lemma 4.6. Il risultato segue quindi dalla Proposizione 4.19. □

Lemma 17.3. *Sia A un PID (ad esempio $A = K[X]$) e sia $f \in A$, $f \neq 0$. Allora le seguenti condizioni sono equivalenti:*

(1) *$A/(f)$ è un campo;*
(2) *l'ideale (f) è massimale;*
(3) *f è irriducibile.*

Dimostrazione. L'equivalenza tra le prime affermazioni l'abbiamo già vista nela Lemma 17.2. Mostriamo quindi l'equivalenza tra (2) e (3).

Vediamo che (2) implica (3). Se f è invertibile allora $(f) = A$ e quindi (f) non è massimale. Se f è riducibile allora $f = f_1 f_2$ con f_1 e f_2 non invertibili e quindi $(f) \subset (f_1) \subset A$ e quindi f non è massimale.

Vediamo che (3) implica (2). Se (f) non è massimale allora esiste g non invertibile e non associato ad f tale che $(f) \subset (g)$. Ma allora g divide f e quindi f non è irriducibile. □

Osserviamo che questo risultato è falso in un UFD in generale. Ad esempio sappiamo che l'ideale (X) non è massimale (è contenuto nell'ideale $(2, X)$) anche se X è irriducibile. E in effetti il quoziente $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ non è un campo.

Corollario 17.4. *Il quoziente $K[X]/(f)$ è un campo se e solo se f è irriducibile.*

Prima di procedere nello studio dei quozienti vogliamo fare un parallelismo con le estensioni quadratiche viste un po' di tempo fa. Sia $d \in K$. Ricordiamo che $K[\sqrt{d}]$ è un campo se e solo se d non è un quadrato in K. Questa condizione è equivalente a richiedere che il polinomio $X^2 - d$ è irriducibile. Abbiamo quindi che

$$K[X]/(X^2 - d) \text{ è un campo } \iff K[\sqrt{d}] \text{ è un campo}$$

Ciò non è un caso e in effetti abbiamo

Teorema 17.5. *Per ogni $d \in K$ si ha*

$$K[X]/(X^2 - d) \cong K[\sqrt{d}].$$

Dimostrazione. Sappiamo che esiste un unico omomorfismo $\psi : K[X] \to K[\sqrt{d}]$ tale che $\psi(a) = a$ per ogni $a \in K$ e $\psi(X) = \varepsilon$ per il Corollario 15.2; inoltre ψ è anche un'applicazione lineare tra K-spazi vettoriali per quanto osservato precedentemente. Si ha chiaramente che ψ è suriettiva e osserviamo che $\ker(\psi)$ contiene $(X^2 - d)$; ma $\ker(\psi)$ non può essere

strettamente più grande di $X^2 - d$ altrimenti sarebbe generato da un polinomio di grado ≤ 1 e quindi $K[X]/\ker(\psi)$ avrebbe dimensione minore di 2 per la Proposizione 17.1 e non potrebbe essere quindi isomorfo a $K[\sqrt{d}]$. Ne segue che $\ker(\psi) = (X^2 - d)$ e il teorema segue dal teorema fondamentale di omomorfismo. □

Questo teorema è illuminante per quel che riguarda il legame tra quozienti di $K[X]$ ed estensioni di K. Consideriamo quindi più in generale un simbolo ε e "imponiamo" che sia radice di un polinomio $f \in K[X]$: nel caso delle estensioni quadratiche tale polinomio era proprio $X^2 - d$, ma nessuno ci impedisce do considerare polinomi arbitrari.

Esempio 17.6. Consideriamo in $\mathbb{Q}[X]$ il polinomio $f = X^3 + X^2 + X + 1$. Sappiamo bene che tale polinomio non è irriducibile, ma per ora non ce ne preoccupiamo. Vogliamo quindi estendere l'anello $\mathbb{Q}$ con un elemento ε che sia radice del polinomio $X^3 + X^2 + X + 1$. Chiaramente non ci basta più considerare solo elementi del tipo $a + b\varepsilon$, perché l'elemento ε^2 non potrei esprimerlo in questa forma; siamo portati a considerare elementi del tipo

$$a + b\varepsilon + c\varepsilon^2.$$

Questi elementi formano un anello che possiamo denotare con $\mathbb{Q}[\varepsilon]$ imponendo la condizione $\varepsilon^3 = -\varepsilon^2 - \varepsilon - 1$. Questo anello non è un dominio di integrità perché ad esempio $(1 + \varepsilon)(1 + \varepsilon^2) = 0$ e questo fatto rispecchia la riducibilità del polinomio scelto f.

Prima di procedere introduciamo la seguente notazione: se $K \subset L$ è un'estensione di campi e $\alpha \in L$ denotiamo con $K[\alpha]$ l'immagine dell'omomorfismo $v_\alpha : K[X] \to L$: $K[\alpha]$ è quindi l'insieme di tutti gli elementi di L della forma $k_0 + k_1\alpha + \cdots + k_n\alpha^n$ al variare di $n \in \mathbb{N}$ e dei $k_i \in K$. Osserviamo che $K[\alpha]$ è il più piccolo sottoanello di L che contiene K e α.

È importante osservare che nell'Esempio 17.6 non stiamo aggiungendo a $\mathbb{Q}$ una particolare radice del polinomio f in $\mathbb{C}$: il polinomio ha le radici distinte $-1, \pm i$ e sicuramente non possiamo vedere l'anello $\mathbb{Q}[\varepsilon]$ all'interno di $\mathbb{C}$ aggiungendo una di queste radici (anche perché non è un dominio!). Osserviamo infine che l'anello $\mathbb{Q}[\varepsilon]$ lo possiamo costruire anche come quoziente $\mathbb{Q}[X]/(f)$ e la dimostrazione è la stessa del caso $f = X^2 - d$ vista nel Teorema 17.5.

Nel caso in cui il polinomio f è irriducibile la situazione cambia in modo significativo. Supponiamo che f sia un polinomio irriducibile in $K[X]$ e che f abbia una radice α in un campo L contenente K (si può pensare ad esempio a $K = \mathbb{Q}$ e ad $L = \mathbb{C}$): a differenza di prima in cui ε era un simbolo astratto, adesso α è un elemento concreto che "esiste" già di per sè.

Se $f = X^n - g(X)$ dove g è un polinomio di grado minore di n abbiamo che $\alpha^n = g(\alpha)$ e quindi gli elementi di $K[\alpha]$ avranno tutti la forma $k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}$ al variare dei $k_i \in K$, questo perché se avessi un termine α^m, con $m \geq n$, posso sempre ridurlo utilizzando l'uguaglianza $\alpha^n = g(\alpha)$. Si ha

Teorema 17.7. *Siano $K \subset L$ campi e $f \in K[X]$ irriducibile. Sia $\alpha \in L$ una radice di f. Allora esiste un unico isomorfismo di anelli*

$$\psi : \frac{K[X]}{(f)} \to K[\alpha]$$

tale che $\psi(k) = k$ per ogni $k \in K$ e $\psi(X) = \alpha$. In particolare $K[\alpha]$ è un campo.

Dimostrazione. L'unicità è ovvia perché le immagini delle costanti e di X determinano le immagini di ogni elemento di $K[X]/(f)$. Per l'esistenza sappiamo dal Corollario 15.2 che esiste un unico omomorfismo di anelli $\psi : K[X] \to K[\alpha]$ tale che $\psi(k) = k$ per ogni $k \in K$ e $\psi(X) = \alpha$ (osserviamo che in questo caso $\psi = v_\alpha$, la valutazione in α). Questo omomorfismo è ancora suriettivo. $\ker(\psi)$ contiene l'ideale (f) e siccome f è irriducibile abbiamo che (f) è massimale e quindi necessariamente $\ker(\psi) = (f)$. Il risultato segue dal teorema di omomorfismo. □

Corollario 17.8. *Sia f un polinomio irriducibile in $K[X]$, $K \subset L$ e $\alpha \in L$ una radice di f. Allora $K[\alpha]$ è un K-spazio vettoriale di dimensione* $\deg(f)$.

Dimostrazione. Segue direttamente dalla Proposizione 17.1 e dal Teorema 17.7. □

Corollario 17.9 (Teorema fondamentale di isomorfismo delle estensioni semplici)**.** *Sia f un polinomio irriducibile in $K[X]$, $K \subset L, L'$, $\alpha \in L$ e $\alpha' \in L'$ radici di f. Allora esiste un unico isomorfismo $\theta : K[\alpha] \to K[\alpha']$ tale che $\theta(\alpha) = \alpha'$ e θ ristretto a K è l'identità.*

Dimostrazione. L'esistenza deriva dal Teorema 17.7. L'unicità è chiara perché abbiamo fissato le immagini delle costanti e di α. □

Questo enunciato lo possiamo anche enunciare in una forma (apparentemente) più generale.

Corollario 17.10. *Sia $\phi : K \to K'$ un isomorfismo di campi e $\varphi : K[X] \to K'[X]$ l'isomorfismo tra anelli definito come nel Teorema 15.1. Siano $K \subset L$, $K' \subset L'$ estensioni di campi, f un polinomio irriducibile in $K[X]$, $\alpha \in L$ una radice di f e $\alpha' \in L'$ una radice di $\varphi(f)$. Allora esiste un unico isomorfismo da $K[\alpha]$ a $K'[\alpha']$ che estende ϕ e che manda α in α'.*

Dimostrazione. Il precedente corollario è il caso particolare in cui $\phi =$ identità su K. Osserviamo comunque che i due enunciati sono equivalenti se identifichiamo K e K' tramite ϕ.

Volendo procedere un po' più formalmente, sia $\varphi : K[X] \to K'[X]$ l'isomorfismo associato a ϕ. Tramite questo isomorfismo abbiamo che l'immagine dell'ideale generato da f è l'ideale generato da $\varphi(f)$ e in particolare ϕ induce un isomorfismo

$$K[X]/(f) \to K'[X]/(\varphi(f)).$$

Il risultato segue componendo i 3 isomorfismi tra $K[\alpha]$ e $K[X]/(f)$, tra $K[X]/(f)$ e $K'[X]/\varphi(f)$, e tra $K'[X]/\varphi(f)$ e $K'[\alpha']$. □

Definizione. Consideriamo un'estensione di campi $K \subset L$. Un elemento $\alpha \in L$ si dice *algebrico* su K se è radice di un polinomio non nullo in $K[X]$. Un numero complesso si dice algebrico se è algebrico su $\mathbb{Q}$.

Ad esempio abbiamo che $\sqrt{2}$ è algebrico e anche $\sqrt{2}+\sqrt[3]{3}$. Infatti, come si può ottenere un polinomio in $\mathbb{Z}[X]$ che ammette $\sqrt{2}+\sqrt[3]{3}$ come soluzione? Ponendo $\alpha = \sqrt{2}+\sqrt[3]{3}$ abbiamo $\alpha - \sqrt{2} = \sqrt[3]{3}$ ed elevando al cubo otteniamo $\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} = 3$ da cui $\alpha^3 + 6\alpha - 3 = \sqrt{2}(3\alpha^2+2)$; eleviamo al quadrato quest'ultima identità ottenendo $\alpha^6 + 36\alpha^2 + 9 + 12\alpha^4 - 6\alpha^3 - 36\alpha = 2(9\alpha^4 + 4 + 12\alpha^2)$ e poi portando tutti i termini dalla stessa parte abbiamo finalmente $\alpha^6 - 6\alpha^4 - 6\alpha^3 + 12\alpha^2 + 36\alpha + 1 = 0$ per cui α è radice del polinomio $X^6 - 6X^4 - 6X^3 + 12X^2 + 36X + 1$.

Se α è algebrico su K allora l'insieme dei polinomi che hanno α come radice è un ideale in $K[X]$: infatti, se $f(\alpha) = g(\alpha) = 0$ allora $(f+g)(\alpha) = 0$ e $fh(\alpha) = f(\alpha)h(\alpha) = 0$ per ogni $h \in K[X]$; detto I l'ideale dei polinomi in $K[X]$ che si annullno in α abbiamo quindi che esiste un polinomio f tale che $I = (f)$. Tale polinomio può essere scelto monico in modo unico e in tal caso lo chiamiamo il polinomio minimo di α su K e lo denotiamo $\mathrm{pm}_{\alpha,K}$.

Ad esempio se $\alpha = \sqrt{2}$ il polinomio minimo di α su $\mathbb{Q}$ è $X^2 - 2$. Il polinomio minimo di $\sqrt{2}+\sqrt[3]{3}$ è quello che abbiamo calcolato qui sopra.

Lemma 17.11. *Sia $K \subset L$ e $\alpha \in L$ algebrico su K. Allora $pm_{\alpha,K}$ è irriducibile in $K[X]$. Viceversa, se α è radice di un polinomio $f \in K[X]$ monico e irriducibile allora $f = pm_{\alpha,K}$.*

Dimostrazione. Per la prima parte, se f non fosse irriducibile si potrebbe scrivere come prodotto hg di due polinomi di grado positivo. Avremmo quindi $f(\alpha) = g(\alpha)h(\alpha)$ e quindi $g(\alpha) = 0$ o $h(\alpha) = 0$ e quindi almeno uno tra g ed h annullerebbero α, contraddicendo l'ipotesi che tutti i polinomi che si annullano in α sono multipli di f. La seconda parte è immediata. □

Abbiamo visto prima un esempio in cui la somma di due elementi algebrici è ancora algebrico calcolando esplicitamente un polinomio razionale che ammette $\sqrt{2}+\sqrt[3]{3}$ come radice. C'è tuttavia anche una ragione un po' più profonda e immediata che ci permette di dire che somma, prodotto e rapporto di due elementi algebrici è ancora un elemento algebrico. Dato $\alpha \in L$ consideriamo il campo $K(\alpha)$ "generato" da α su K, $K \subset K(\alpha) \subset L$ dato da

$$K(\alpha) = \{f(\alpha)/g(\alpha) \in L : \, f, g \in K[X], \, g(\alpha) \neq 0\}.$$

il campo $K(\alpha)$ può anche essere definito come il più piccolo sottocampo di L che contiene K ed α, cioè come l'intersezione di tutti i sottocampi che contengono sia K che α. Osserviamo anche che $K(\alpha)$ è (isomorfo a) il campo dei quozienti di $K[\alpha]$.

Se $K \subset L$ diciamo che L è un'estensione finita di K se L è un K-spazio vettoriale di dimensione finita. Abbiamo il seguente fondamentale risultato.

Teorema 17.12. *Siano $K \subset L$ campi e $\alpha \in L$. Sono equivalenti*

(1) *α è algebrico su K;*
(2) *$K[\alpha]$ è un K-spazio vettoriale di dimensione finita.*
(3) *$K(\alpha)$ è un'estensione finita di K;*

(4) $K(\alpha) = K[\alpha]$.

Dimostrazione. (1) $\Rightarrow$ (2) lo abbiamo già visto nel Corollario 17.8.

(2) $\Rightarrow$ (3) Abbiamo che esiste $n > 0$ tale che $1, \alpha, \alpha^2, \ldots, \alpha^n$ sono linearmente dipendenti e quindi α è algebrico. Ne segue che $K[\alpha]$ è un campo per il Teorema 17.7 e quindi $K(\alpha) = K[\alpha]$ ed in particolare $K(\alpha)$ è un'estensione finita di K.

(3) $\Rightarrow$ (4) Segue ragionando come nel punto precedente, osservando che si ha sempre $K[\alpha] \subseteq K(\alpha)$.

(4) $\Rightarrow$ (1) Abbiamo che esiste $f \in K[X]$ tale che $\alpha^{-1} = \tilde{f}(\alpha)$. Di conseguenza $\alpha\tilde{f}(\alpha) - 1 = 0$ e quindi α è radice del polinomio $Xf - 1$ ed in particolare è algebrico su K.

□

Corollario 17.13. *Se $K \subset L$ è un'estensione finita di campi ogni elemento di L è algebrico su K.*

Dimostrazione. Basta osservare che, essendo L un campo che contiene α e K allora $K(\alpha) \subset L$ e quindi $K(\alpha)$ è un'estensione finita di K. □

Vogliamo ora dimostrare che un'estensione finita di un'estensione finita è ancora un'estensione finita e per questo utilizziamo la seguente notazione: se $K \subset L$ è un'estensione finita di campi con $\dim_K(L) = d$ diciamo che L è un'estensione finita di grado d di K e scriviamo $[L : K] = d$.

Proposizione 17.14 (Lemma della torre)**.** *Siano $K \subset L$ e $L \subset M$ estensioni di campi finite. Allora $K \subset M$ è un'estensione di campi finita e $[M : L][L : K] = [M : K]$.*

Dimostrazione. Sia $\{a_1, \ldots, a_n\}$ una base di L su K e $\{b_1, \ldots, b_m\}$ una base di M su L. È sufficiente mostrare che gli elementi della forma $a_i b_j$ formano una base di M su K. Infatti, sia $x \in M$. Esisteranno allora $l_1, \ldots, l_m \in L$ tali che

$$x = l_1 b_1 + \cdots + l_m b_m.$$

A loro volta, ciascuno degli l_i può essere espresso come combinazione lineare di $a_1, \ldots, a_n$. Otteniamo quindi un'espressione del tipo

$$x = \sum_i \sum_j k_{i,j} a_i b_j.$$

e abbiamo quindi che gli elementi $a_i b_j$ generano M su K. Mostriamo anche che sono linearmente indipendenti. Se $k_{i,j} \in K$ sono tali che

$$\sum_{i,j} k_{i,j} a_i b_j = 0$$

abbiamo che

$$\sum_j \Big(\sum_i k_{i,j} a_i \Big) b_j = 0$$

e quindi, per l'indipendenza lineare dei b_i su L abbiamo che

$$\sum_i k_{i,j} a_i = 0$$

per ogni j. Infine, sfruttando l'indipendenza lineare degli a_i su K concludiamo che $k_{i,j} = 0$ per ogni i, j e quindi gli $a_i b_j$ sono linearmente indipendenti. □

Da questi risultati segue direttamente che se $\alpha_1, \ldots, \alpha_r \in L$ sono algebrici su K allora ogni elemento $\beta \in L$ che può essere espresso come rapporto di polinomi in $\alpha_1, \ldots, \alpha_r$ è a sua volta algebrico.

Infatti abbiamo che $K[\alpha_1]$ è un campo che è un'estensione finita di K. L'elemento α_2, essendo algebrico su K lo è a maggior ragione su $K[\alpha_1]$ e quindi $(K[\alpha_1])[\alpha_2]$ è a sua volta un'estensione finita di $K[\alpha_1]$ e quindi anche di K per la proposizione. Osserviamo inoltre che $(K[\alpha_1])[\alpha_2]$ è il più piccolo sottocampo di L che contiene sia K che α_1 che α_2: infatti i suoi elementi possono essere espressi come polinomi a coefficienti in K nelle "variabili" α_1 e α_2. Possiamo quindi denotare il campo $(K[\alpha_1])[\alpha_2]$ semplicemente con $K[\alpha_1, \alpha_2]$. Reiterando abbiamo che $K[\alpha_1, \ldots, \alpha_r]$ è un'estensione finita di K. L'elemento β per costruzione appartiene al campo $K[\alpha_1, \ldots, \alpha_r]$ e quindi, in particolare $K(\beta) \subset K[\alpha_1, \ldots, \alpha_r]$. Siccome $K(\beta)$ è un K-sottospazio di $K[\alpha_1, \ldots, \alpha_r]$ abbiamo che $K(\beta)$ ha dimensione finita e quindi concludiamo che β è algebrico e che $K(\beta) = K[\beta]$. Detto in altri termini, possiamo anche dire:

Corollario 17.15. *Sia $K \subset L$ un'estensione di campi. Allora gli elementi algebrici di L su K formano un campo.*

Se $K \subset L$ sono campi diciamo che L è algebrico su K se ogni elemento di L è algebrico su K. Nello stesso spirito di questi risultati possiamo anche mostrare il seguente.

Teorema 17.16. *Siano $K \subset L \subset M$ campi con L algebrico su K e M algebrico su L. Allora M è algebrico su K.*

Dimostrazione. Basta mostrare che ogni elemento di $\alpha \in M$ è contenuto in un'estensione finita di K. Infatti consideriamo il polinomio minimo $l_0 + l_1 X + \cdots + l_n X^n$ di α su L. Gli elementi l_i, essendo in L sono algebrici su K e quindi possiamo considerare l'estensione finita di K data da $K' = K[l_0, \ldots, l_n]$. Siccome α è algebrico su K' abbiamo che $K'[\alpha]$ è un'estensione finita di K' e quindi anche di K. □

Facciamo un'osservazione conclusiva nel caso in cui α non è algebrico.

Proposizione 17.17. *Sia $K \subset L$ un'estensione di campi e $\alpha \in L$ trascendente su K. Allora*

$$K[\alpha] \cong K[X]$$

e

$$K(\alpha) \cong K(X),$$

dove $K(X)$ indica il campo dei quozienti di $K[X]$.

Dimostrazione. Consideriamo l'omomorfismo

$$v_\alpha : K[X] \to K[\alpha].$$

Tale omomorfismo è suruettivo per definizione ed iniettivo perché α è trascendetne e quindi non annulla alcun polinomio non nullo. La seconda parte segue dalla prima in quanto

stiamo considerando i campi dei quozienti. In alternativa possiamo ancora considerare l'applicazione $v_\alpha : K(X) \mapsto K(\alpha)$ data dalla valutazione in α, cioè

$$v_\alpha(f/g) = f(\alpha)/g(\alpha).$$

Il fatto che $g(\alpha) \neq 0$ viene dal fatto che α è trascendente e quindi non è radice di alcun polinomio non nullo. Inoltre, che v_α sia ben definita e un omomorfismo viene dal fatto che lo è quando è ristretta a $K[X]$. Infine, osserviamo che v_α è suriettiva per definizione di $K(\alpha)$ e iniettiva perché α è trascendente.

□

18. Costruzioni con riga e compasso

In questa sezionea affrontiamo il classico problema della costruzione di figure geometriche con riga e compasso. Supporremo che la nostra riga non sia graduata ma di lunghezza arbitrariamente grande e che il nostro compasso sia anche in grado di fare cerchi arbitrariamente grandi.

Il nostro punto di partenza é dato da due punti che denoteremo P_0 e P_1 a distanza unitaria.

Cosa possiamo fare con la nostra riga e il nostro compasso? Con la riga possiamo tracciare una retta passante per due punti che siamo riusciti a costruire e con il compasso possiamo tracciare un circonferenza che abbia il centro in un punto costruito e passante per un altro punto costruito. Formalizziamo questo fatto nelle seguenti definizioni

Definizione. Dato un insieme S di punti del piano diciamo che una retta é una S-retta se passa per due punti di S. Analogamente diciamo che una circonferenza é una S-circonferenza se il suo centro é un punto di S e passa per un punto di S.

Definizione. Una costruzione (con riga e compasso) é una sequenza di punti $(P_0, P_1, \ldots, P_r)$ del piano tale che, detto $S_i = \{P_0, \ldots, P_i\}$ si ha per ogni $i = 3, \ldots, r$ una delle seguenti condizioni

- P_i é nell'intersezione tra due S_{i-1}-rette;
- P_i é nell'intersezione tra una S_{i-1}-retta e una S_{i-1}-circonferenza;
- P_i é nell'intersezione tra due S_{i-1}-circonferenze;

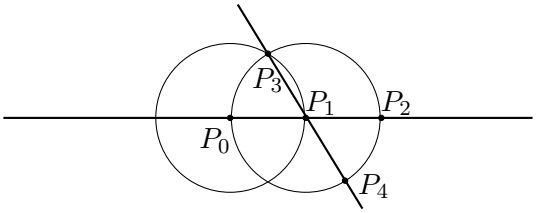

Figure 1. Un esempio di costruzione

Facciamo qualche osservazione su alcune operazioni elementari che possiamo fare con riga e compasso.

Proposizione 18.1. *Le seguenti operazioni si possono fare con riga e compasso*

(1) *Data una retta r e un punto P possiamo tracciare la perpendicolare ad r passante per P;*
(2) *Data una retta r e un punto P possiamo tracciare la parallela ad r passante per P;*
(3) *Dato un segmento AB e un punto P possiamo costruire un segmento parallelo e congruente ad AB e che abbia un vertice in P*

Proof. (1) Facciamo una costruzione valida sia nel caso in cui P appartenga ad r sia se P non appartiene ad r. Tracciamo la circonferenza di centro P passante per un punto A (che non stia sulla perpendicolare cercata) costruito sulla retta r e sia B l'altro punto di intersezione tra questa circonferenza ed r. Intersecando la circonferenza di centro A passante per B e quella di centro B passante per A otteniamo due punti per i quali passa la retta cercata.
(2) segue dal punto precedente;
(3) segue dal punto precedente.

□

Diciamo che un numero reale α é costruibile se riusciamo a costruire un segmento di lunghezza $|\alpha|$.

Teorema 18.2. *I numeri costruibili formano un campo F. Inoltre se $\alpha \in F$, $\alpha > 0$, allora $\sqrt{\alpha} \in F$.*

Proof. Siano α e β costruibili. Assumiamo senza perdere generalitá $0 < \beta \leq \alpha$. Abbiamo quindi due segmenti dil lunghezza α e β (vedi Figura 2). Per la Proposizione precedente possiamo traslare uno dei due in modo che i due segmenti abbiano un estremo in comune. Tracciamo la circonferenza con centro in questo estremo e passante per l'altro estremo del segmento di lunghezza β. Questa circonferenza individua sulla retta passante per il segmento di lunghezza α un segmento dil lunghezza $\alpha - \beta$ e uno di lunghezza $\alpha + \beta$. Le costruzioni con riga e compasso di α^{-1} e di $\alpha\beta$ sono mostrate in Figura 4 e in Figura 3 rispettivamente. La costruzione di $\sqrt{\alpha}$ é mostrata in Figura 5.

□

Introduciamo ora nel nostro piano un sistema di riferimento cartesiano ortogonale in modo che i nostri punti di riferimento P_0 e P_1 abbiano coordinate rispettivamente $(0, 0)$ e $(1, 0)$ e mostriamo il seguente risultato di compatibilitá.

Proposizione 18.3. *Un numero reale α é costruibile se e solo se esiste un punto costruibile che abbia una delle due coordinate uguale ad α. Un punto é costruibile se e solo se entrambe le sue coordinate sono costruibili.*

Proof. Se sappiamo costruire un segmento lungo $|\alpha|$ possiamo traslare questo segmento nell'origine e quindi tracciare la circonferenza che individua i punti $(0, \pm\alpha)$ e $(\pm\alpha, 0)$. Se abbiamo un punto di coordinate (α, β) possiamo tracciare le perpendicolari agli assi

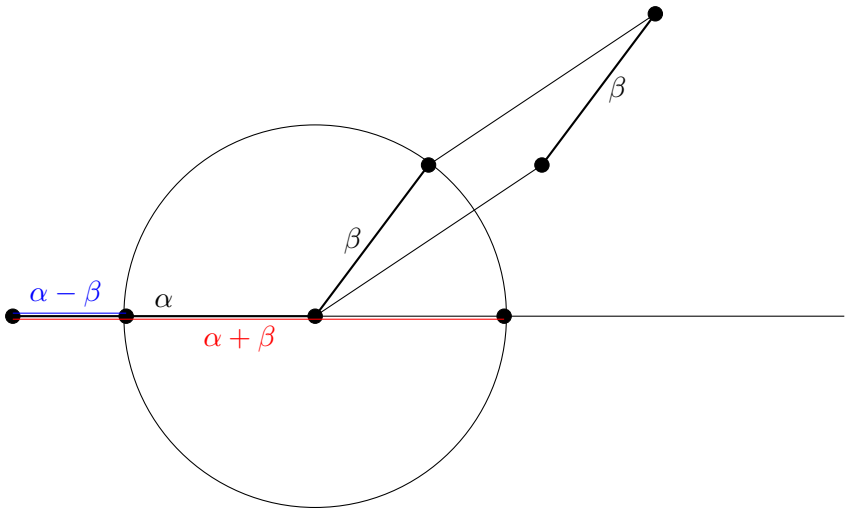

FIGURE 2. Costruzione di $\alpha \pm \beta$.

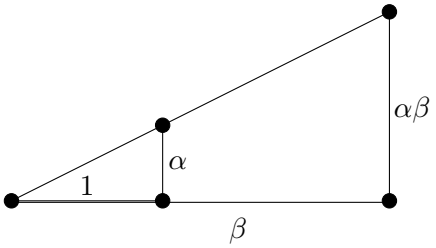

FIGURE 3. Costruzione di $\alpha\beta$.

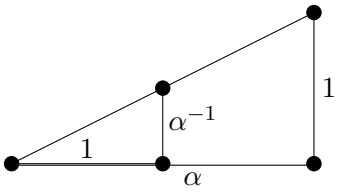

FIGURE 4. Costruzione di α^{-1}.

passanti per questo punto e trovare i punto $(\alpha, 0)$ e $(0, \beta)$ quindi determinando un segmento di lunghezza $|\alpha|$ e uno di lunghezza $|\beta|$. □

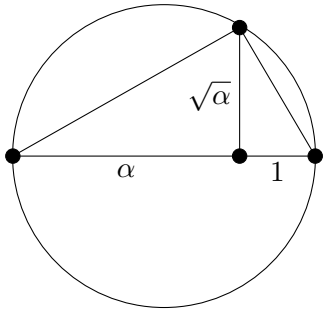

FIGURE 5. Costruzione di $\sqrt{\alpha}$.

Siamo ora pronti a dimostrare il principale risultato che riguarda le costruzioni con riga e compasso da un punto di vista algebrico

Teorema 18.4. *Sia $\alpha \in \mathbb{R}$. Allora α é costruibile se e solo se esiste una catena di campi contenuta in $\mathbb{R}$*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r \subseteq \mathbb{R}$$

tale che $[K_i : K_{i-1}] = 2$ per ogni $i = 1, \ldots, r$ e tale che $\alpha \in K_r$.

Proof. Supponiamo che esista tale catena e mostriamo per induzione su i che gli elementi di K_i sono costruibili. Chiaramente $K_0 = \mathbb{Q}$ é costruibile. Le condizioni $[K_i : K_{i-1}] = 2$ e $K_i \in \mathbb{R}$ implicano che esiste $\beta \in K_{i-1}$ tale che $K_i = K_{i-1}[\sqrt{\beta}]$. Allora K_i é costruibile per la Proposizione.

Viceversa, supponiamo che α sia costruibile e supponiamo quindi che α sia una coordinata di un punto costruibile P e sia quindi $(P_0, P_1, \ldots, P_r = P)$ una costruzione. Chiamiamo (α_i, β_i) le coordinate del punto P_i e definiamo ricorsivamente dei campi F_i ponendo $F_0 = \mathbb{Q}$ e $F_i = F_{i-1}(\alpha_i, \beta_i)$. Vediamo ora le tre possibilitá che possono accadere. Osserviamo che una S_{i-1}-retta ha equazione con coefficienti in F_{i-1}: se infatti tale retta passa per i punti P_j e P_h, con $j, h < i$ allora l'equazione di questa retta é

$$(\alpha_j - \alpha_h)(y - \beta_h) = (\beta_j - \beta_h)(x - \alpha_h);$$

similmente una S_{i-1}-circonferenza avrá equazione con coefficienti in F_{i-1}: se ha centro in P_j e passa per P_h la sua equazione sará

$$(x - \alpha_j)^2 + (y - \beta_j)^2 = (\alpha_h - \alpha_j)^2 + (\beta_h - \beta_j)^2$$

Vediamo ora i tre casi possibili nella costruzione di P_i:

(1) P_i é intersezione di due S_{i-1}-rette: in questo caso (α_i, β_i) é soluzione di un sistema lineare di due equazioni in due incognite a coefficienti in F_{i-1} per cui appartengono anch'essi a F_{i-1} e quindi $F_i = F_{i-1}$;

(2) P_i é nell' intersezione di una S_{i-1}-retta e una S_{i-1} circonferenza: in questo caso (α_i, β_i) é soluzione di un sistema della seguente forma

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

con $a, b, c, a', b', c' \in F_{i-1}$. Se $a \neq 0$ (il caso $b \neq 0$ é analogo) ci permette di scrivere x in funzione di y dalla prima equazione. Sostituendo nella seconda otteniamo un'equazione di secondo grado soddisfatta da y per cui $F_{i-1}[\beta_i]$ é un'estensione di grado al piú due di F_{i-1}. La prima equazione ci fornisce anche $\alpha_i \in F_{i-1}[\beta_i]$ per cui $F_i = F_{i-1}[\beta_i]$.

(3) P_i é nell' intersezione di due S_{i-1}-circonferenze. In questo caso (α_i, β_i) é quindi soluzione di un sistema

$$\begin{cases} x^2 + y^2 + a'x + b'y + c' = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

con $a, b, c, a', b', c' \in F_{i-1}$. Sostituendo una delle due equazioni con la loro differenza ci riconduciamo al caso precedente.

□

19. Campi di spezzamento

Dato un polinomio f in $K[X]$ vogliamo determinare un'estensione di K "più piccola possibile" in cui il polinomio f si fattorizzi nel prodotto di polinomi di primo grado. Facciamo qualche esempio.

Consideriamo il polinomio $f = X^2 - 2 \in \mathbb{Q}[X]$: in questo caso il campo dato dall'estensione quadratica $\mathbb{Q}[\sqrt{2}]$ è un campo in cui f si fattorizza, o spezza, nel prodotto di polinomi di primo grado.

Facciamo un esempio un po' più complesso. Consideriamo il polinomio $f = X^3 + 3X + 3 \in \mathbb{Q}[X]$. Il polinomio f è irriducibile per il criterio di Eisenstein. Chiamiamo α una sua qualunque radice in $\mathbb{C}$, cioè un numero complesso tale che $\alpha^3 + 3\alpha + 3 = 0$. Per quanto visto sappiamo che $\mathbb{Q}[\alpha]$ è un'estensione di grado 3 di $\mathbb{Q}$. Ci chiediamo se f si fattorizza nel prodotto di polinomi di primo grado in $\mathbb{Q}[\alpha]$. Dividiamo f per $X - \alpha$ (ad esempio con Ruffini) e otteniamo

$$X^3 + 3X + 3 = (X - \alpha)(X^2 + \alpha X + 3 + \alpha^2).$$

Il polinomio $X^2 + \alpha X + 3 + \alpha^2$ è irriducibile in $\mathbb{Q}[\alpha]$: questo è evidente se abbiamo scelto per α una radice reale di f: in tal caso abbiamo che $\mathbb{Q}[\alpha] \subset \mathbb{R}$ e osserviamo che le altre radici complesse di f (cioè quelle di $X^2 + \alpha X + 3 + \alpha^2$) non sono reali in quanto il discriminante è dato da $-3\alpha^2 - 12 < 0$ e quindi non possono essere contenute in $\mathbb{Q}[\alpha]$. Alla stessa conclusione si poteva arrivare anche senza considerare una radice reale α, ma una qualunque altra radice: in questo caso bisogna però mostrare che il discriminante del polinomio $X^2 + \alpha X + 3 + \alpha^2$, cioè $\Delta = -3\alpha^2 - 12$ non è un quadrato in $\mathbb{Q}[\alpha]$. Abbiamo quindi bisogno di effettuare un'ulteriore estensione di $\mathbb{Q}[\alpha]$ aggiungendo un elemento β che sia radice del

polinomio $X^2+\alpha X+3+\alpha^2$, cioè tale che $\beta^2+\alpha\beta+3+\alpha^2=0$. In tal caso abbiamo quindi che $\mathbb{Q}[\alpha,\beta]$ è un'estensione di grado 6 di $\mathbb{Q}$ in cui il polinomio f si fattorizza nel prodotto di polinomi di primo grado:

$$f=(X-\alpha)(X-\beta)(X+\alpha+\beta).$$

Sappiamo inoltre che una base di $\mathbb{Q}[\alpha,\beta]$ su $\mathbb{Q}$ è data da $1,\alpha,\beta,\alpha\beta,\alpha^2,\alpha^2\beta$.

Definizione. Sia $K\subset L$ un'estensione di campi e $f\in K[X]$. Diciamo che L è *un campo di spezzamento* per f se esistono $\alpha_1,\dots,\alpha_n\in L$ e $k\in K$ tali che

- $f=k(X-\alpha_1)\cdots(X-\alpha_n)\in L[X]$;
- $L=K[\alpha_1,\dots,\alpha_n]$.

L'esistenza di un campo di spezzamento la possiamo ottenere generalizzando le idee sviluppate nell'esempio qui sopra.

Teorema 19.1. *Sia K un campo e $f\in K[X]$ un polinomio di grado $n>0$. Allora esiste un'estensione $K\subset L$ di grado al più $n!$ che è un campo di spezzamento per f.*

Dimostrazione. Procediamo per induzione su $n=\deg(f)$ e, senza perdita di generalità, assumiamo f monico. Se $n=1$ il risultato è ovvio: basta scegliere $L=K$. Per $n>1$ sia a un fattore irriducibile di f (eventualmente si prende $a=f$ se f stesso è irriducibile). Se consideriamo il quoziente

$$K_1=K[X]/(a)$$

abbiamo che K_1 è un'estensione di K di grado $\deg(a)\leq n$ in cui f ha una radice α_1 data dalla classe del polinomio X. Abbiamo quindi $K_1=K[\alpha_1]$ e che in $K_1[X]$ il polinomio f si fattorizza nella forma

$$f=(X-\alpha_1)g$$

dove $g\in K_1[X]$ ha grado $n-1$. Per induzione esiste un campo L che sia di spezzamento per g su K_1 cioè tale che

- $L=K_1[\alpha_2,\dots,\alpha_n]$;
- $g=(X-\alpha_2)\cdots(X-\alpha_n)$

e tale che il grado di L su K_1 è $\leq(n-1)!$. Essendo $K_1=K[\alpha_1]$ abbiamo $L=K[\alpha_1,\dots,\alpha_n]$, $f=(X-\alpha_1)\cdots(X-\alpha_n)$ e che il grado di $[L:K]=[L:K_1][K_1:K]\leq(n-1)!\deg(a)\leq n!$. □

Questo teorema ci permette di costruire un campo di spezzamento per il polinomio f. Molto più sottile è invece l'unicità, a meno di isomorfismi, di un tale campo.

Teorema 19.2. *Sia K un campo e f un polinomio in $K[X]$. Siano L,L' campi di spezzamento per f. Allora esiste un isomorfismo $\psi:L\to L'$ che ristretto a K è l'identità.*

Dimostrazione. Procediamo per induzione su $\min([L:K],[L':K])$. Se tale minimo è 1, diciamo $[L:K]=1$, allora $L=K$ e quindi le radici di f in L stanno già in K e quindi anche in L'. In particolare, anche $L'=K$.

Supponiamo quindi che $[L:K]>1$ e quindi che f non si fattorizza in polinomi lineari in $K[X]$. Sia quindi a un fattore irriducibile di f in $K[X]$. Siccome f si spezza sia in

L che in L' lo stesso accade per a e siano quindi $\alpha \in L$ e $\alpha' \in L'$ radici di a. Per il teorema fondamentale di isomorfismo delle estensioni semplici abbiamo che esiste un (unico) isomorfismo $K[\alpha] \to K[\alpha']$ che manda $\alpha \in \alpha'$ e fissa tutti gli elementi di K. In altre parole, a meno di sostituire α con α' possiamo identificare $K[\alpha]$ con $K[\alpha']$ e chiamiamo tale campo K_1. Abbiamo quindi che K_1 è un sottocampo di L e di L'.

Possiamo ora fattorizzare il polinomio f su $K_1[X]$: $f = (X - \alpha)g$, con $g \in K_1[X]$. Abbiamo quindi che L e L' sono campi di spezzamento per g su K_1. Per ipotesi induttiva, siccome $[L : K_1] < [L : K]$ e similmente con L' abbiamo che esiste un isomorfismo da L a L' che fissa gli elementi di K_1 (cioè che fissa K e manda α in α'). In particolare tale isomorfismo fissa gli elementi di K. □

Vediamo ora un'importante conseguenza sui campi finiti, iniziando da esempi che ben conosciamo. Sia K un campo con q elementi, q dispari, e siano $d, d' \in K$ due elementi non quadrati in K. Sappiamo dalla teoria delle estensioni quadratiche che $K[\sqrt{d}]$ e $K[\sqrt{d'}]$ sono campi, entrambi di cardinalità q^2. Vogliamo ora osservare che sono necessariamente isomorfi.

Teorema 19.3. *Sia K un campo finito $|K| = q$. Siano $d, d' \in K$ non quadrati. Allora esiste $c \in K$ tale che $c^2 = d/d'$ e la funzione $\psi : K[\sqrt{d}] \to K[\sqrt{d'}]$ data da*

$$a + b\sqrt{d} \mapsto a + bc\sqrt{d'}$$

è un isomorfismo di campi.

Dimostrazione. Ricordando che K^* è ciclico abbiamo che K^* è generato da un elemento x. Siccome d e d' non sono quadrati abbiamo che $d = x^{2n+1}$ e $d' = x^{2m+1}$. Abbiamo quindi che $d/d' = x^{2m-2n} = (x^{m-n})^2$ è un quadrato. Sia quindi $c \in K$ tale che $d/d' = c^2$. L'applicazione è chiaramente un isomorfismo di K-spazi vettoriali. Dobbiamo solo mostrare che ψ è moltiplicativa:

$$\begin{aligned}\psi(a + b\sqrt{d})\psi(a' + b'\sqrt{d}) = (a + bc\sqrt{d'})(a' + b'c\sqrt{d'} = aa' + bb'c^2d' + (ab'c + a'bc)\sqrt{d'} \\ = aa' + bb'd + (ab'c + a'bc)\sqrt{d'}\end{aligned}$$

e

$$\psi((a + b\sqrt{d}) \cdot (a' + b'\sqrt{d})) = \psi(aa' + bb'd + (ab' + a'b)\sqrt{d}) = aa' + bb'd + (ab'c + a'bc)\sqrt{d'}$$

e la dimostrazione è completata. □

In questa dimostrazione abbiamo usato la notazione $\sqrt{d}$ e $\sqrt{d'}$ anziché ε per non creare confusione tra i due anelli. Questo teorema è un caso particolare del seguente

Teorema 19.4 (Fondamentale dei campi finiti)**.** *Sia p un numero primo e $n > 0$. Allora esiste un unico, a meno di isomorfismi, campo con p^n elementi.*

Dimostrazione. Tale campo è unico perché se $|K| = p^n$ allora gli elementi di K sono tutte radici del polinomio $X^{p^n} - X$: ne segue che K è un campo di spezzamento per $X^{p^n} - X$ su $\mathbb{Z}_p$.

Per dimostrare l'esistenza procediamo in modo analogo: sia L un campo di spezzamento di $X^{p^n} - X$ su $\mathbb{Z}_p$. Non possiamo dedurre che L abbia esattamente p^n elementi. Tuttavia osserviamo che le radici di $X^{p^n} - X$ sono tutte distinte per il Teorema 12.10 in quanto la sua derivata è -1. Sia quindi K il sottoinsieme di L costituito dalle p^n radici di $X^{p^n} - X$ e verifichiamo che K è un campo. Infatti abbiamo 0 e 1 in K. Se α e β sono radici allora

- $(-\alpha)^{p^n} - (-\alpha) = -(\alpha^{p^n} - \alpha) = 0$ e quindi $-\alpha \in K$;
- $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ e quindi $\alpha + \beta \in K$;
- $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ e quindi $\alpha\beta \in K$;
- $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$ e quindi $\alpha^{-1} \in K$.

Abbiamo quindi che K è un campo con p^n elementi. Osserviamo anche che necessariamente $K = L$. □

Se q è potenza di un numero primo l'unico campo con q elementi viene denotato con $\mathbb{F}_q$.

Corollario 19.5. *Se K è un campo finito e f e g sono polinomi irriducibili in $K[X]$ dello stesso grado, allora $K[X]/(f) \cong K[X]/(g)$.*

Sia ora L un campo finito: vogliamo capire quali sottocampi contiene. Si ha chiaramente che se K è un sottocampo allora deve avere la stessa caratteristica. In particolare, se $|L| = p^n$ dovrà esistere d tale che $|K| = p^d$.

Proposizione 19.6. *Sia L un campo, $|L| = p^n$. Allora L contiene un (unico) campo con p^d elementi se e solo se $d|n$.*

Dimostrazione. Osserviamo che se un campo L contiene p^n elementi allora

$$\prod_{a \in L} (X - a) = X^{p^n} - X.$$

Se L contiene un campo con p^d elementi allora necessariamente $X^{p^d} - X$ divide $X^{p^n} - X$ e questo accade se e solo se $d|n$ (visto in un esercizio). Viceversa, se $d|n$ allora $X^{p^d} - X$ divide $X^{p^n} - X$ e quindi in L ci sono p^d elementi che soddisfano $X^{p^d} - X = 0$. Abbiamo quindi che L contiene un campo di spezzamento di $X^{p^d} - X$ su $\mathbb{Z}_p$ e sappiamo che questo campo ha p^d elementi. □

Teorema 19.7. *(non fatto) Sia K un campo finito, $|K| = q$. Allora il polinomio $X^{q^n} - X$ è il prodotto di tutti i polinomi monici irriducibili in $K[X]$ di grado divisore di n, tutti con molteplicità 1.*

Dimostrazione. Che la molteplicità sia 1 deriva dal fatto che $X^{q^n} - X$ ha derivata -1 e quindi non può avere radici multiple (se avesse fattori multipli avrebbe radici multiple nel suo campo di spezzamento). Sia quindi L il campo con q^n elementi (che sappiamo essere il campo di spezzamento di $X^{q^n} - X$). Se f è un divisore irriducibile di $X^{q^n} - X$ di grado d allora in L esiste una radice α di f. Allora L contiene il sottocampo $K[\alpha]$ che ha grado d su K: ne segue che $d|n$ per la moltiplicatività dei gradi delle estensioni: $n = [L : K] = [L : K[\alpha]][K[\alpha], K] = [L : K[\alpha]]d$.

Viceversa, se f è un polinomio (monico) irriducibile di grado $d|n$ allora $K[X]/(f)$ è il campo con q^d elementi. Sia α una radice di f in $K[X]/(f)$. Siccome $K[X]/(f)$ ha q^d elementi abbiamo che α soddisfa il polinomio $X^{q^d} - X$ e quindi anche $X^{q^n} - X$. Ne segue che $X^{q^n} - X$ è un multiplo del polinomio minimo di α che è proprio f. □

20. Numero di polinomi irriducibili su un campo finito digrado n

Mostriamo una conseguenza del Teorema 19.7. Consideriamo l'anello di convoluzione A costituito dalle funzioni $f : \mathbb{N}_{>0} \to \mathbb{C}$ con somma usuale e prodotto $*$ di convoluzione dato da

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

Sappiamo che A è un anello unitario con elemento neutro $e = \delta_{1,n}$: cioè $e(1) = 1$ e $e(n) = 0$ se $n \neq 1$. Sia $\mathbf{1} \in A$ la funzione costante uguale a 1 e μ la funzione di Möbius definita nel seguente modo:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ (-1)^r & \text{se } n = p_1 \cdots p_r \text{ con i } p_i \text{ primi distinti .} \\ 0 & \text{altrimenti.} \end{cases}$$

Lemma 20.1. *Le funzioni μ e $\mathbf{1}$ sono una l'inversa dell'altra rispetto alla convoluzione cioè*

$$\mu * \mathbf{1} = e.$$

Proof. Si ha chiaramente $\mu * \mathbf{1}(1) = \mu(1) = e(1) = 1$. Basta quindi mostrare che per ogni $n > 1$ si ha

$$(\mu * \mathbf{1})(n) = \sum_{d|n} \mu(d) = e(n) = 0.$$

Se $n = p_1^{a_1} \cdots p_r^{a_r}$ con i primi p_i a due a due distinti e $a_i > 0$ per ogni i poniamo $m = p_1 \cdots p_r$. Si ha chiaramente

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d)$$

perché i divisori senza fattori quadrati di n e di m coincidono. Abbiamo quindi

$$\sum_{d|m} \mu(d) = \sum_{S \subseteq \{1,\ldots,r\}} (-1)^S = 0$$

perché i sottoinsiemi di cardinalità pari di un insieme finito sono tanti quanti i sottoinsiemi di cardinalità dispari (perché?). □

Teorema 20.2. *Sia $f(n) =$ "numero di polinomi monici irriducibili di grado n in $\mathbb{F}_q[X]$", $h(n) = q^n$. Allora*

$$\mu * h = Id \cdot f$$

e quindi

$$f(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$$

Proof. Per il Teorema 19.7 abbiamo che $X^{q^n} - X$ è il prodotto di tutti i polinomi monici irriducibili di grado divisore di d. Guardando ai gradi abbiamo

$$q^n = \sum_{d|n} df(d).$$

In termini di convoluzione possiamo esprimere questa identità tramite

$$h = (Id \cdot f) * \mathbf{1}$$

da cui, facendo la convoluzione con μ da entrambi i membri otteniamo

$$h * \mu = Id \cdot f.$$

Calcolando entrambi i membri in n otteniamo l'espressione voluta per $f(n)$.

□

21. La corrispondenza di Galois

In questa sezione vogliamo mostrare un teorema fondamentale in algebra che é la perfetta conclusione dei due anni di Algebra 1 e Algebra 2 perché fornisce una corrispondenza tra campi e gruppi.

Per semplificare la trattazione considereremo solo sottocampi di $\mathbb{C}$, ma la teoria puó essere sviluppata con opportune ipotesi aggiuntive con campi arbitrari. Cominciamo con qualche definizione. Scriviamo in questa sezione L/K per indicare che $K \subseteq L \subseteq \mathbb{C}$. Il primo risultato che mostriamo riguarda le estensioni finite: esse sono sempre generate da un solo elemento.

Teorema 21.1. *Sia L/K un'estensione finita. Allora esiste $\gamma \in L$ tale che $L = K[\gamma]$*

Proof. Siccome l'estensione é finita esisteranno $\alpha_1, \ldots, \alpha_r \in L$ tali che $L = K[\alpha_1, \ldots, \alpha_r]$. Applicando un'induzione standard ci rendiamo conto che é sufficiente mostrare il risultato per $r = 2$ e quindi che $L = K[\alpha, \beta]$. Chiamiamo $\alpha = \alpha_1, \ldots, \alpha_m$ le radici del polinomio minimo f di α e $\beta = \beta_1, \ldots, \beta_n$ le radici del polinomio minimo g di β. Scegliamo una costante $c \in K$ tale che $\gamma = \alpha + c\beta$ sia diversa da $\alpha_i + c\beta_j$ per ogni $(i, j) \neq (1, 1)$ (tale c esiste perché ogni condizione esclude un solo valore di c, per cui staimo richiedendo che c sia diverso da al piú mn valori, e K é un campo infinito). Il polinomio $h(X) = f(\gamma - cX) \in (K[\gamma])[X]$ ammette β come radice. Inoltre β é l'unica radice che tale polinomio ha in comune con g per come é stato scelto c. Di conseguenza

$$MCD(h, g) = X - \beta$$

in $\mathbb{C}[X]$ e siccome sia h che g appartengono a $K[\gamma][X]$ abbiamo che $\beta \in K[\gamma]$ e di conseguenza anche $\alpha \in K[\gamma]$. □

Una definizione fondamentale:

Definizione. Sia L/K un'estensione. Un K-isomorfismo di L é un omomorfismo non nullo $\sigma : L \to \mathbb{C}$ tale che $\sigma(k) = k$ per ogni $k \in K$. L'estensione L/K si dice *normale* o *di Galois* se per ogni K-isomorismo di L si ha $\sigma(L) = L$.

Osserviamo che siccome L é un campo un K-isomorfismo é sempre iniettivo ed é quindi un isomorfismo di K con la relativa immagine, da cui il nome. Osserviamo inoltre che se l'estensione L/K é normale allora i K-isomorfismi sono automorfismi di L e formano un gruppo, detto gruppo di Galois dell'estensione L/K. Tale gruppo si indica con $Gal(L/K)$.

Osservazione. Se σ é un K-isomorfismo di L, $f \in K[X]$ e $\alpha \in L$ allora $\sigma(f(\alpha)) = f(\sigma(\alpha))$. In particolare, se α é una radice di f anche $\sigma(\alpha)$ lo é. Infatti, se $f = \sum a_i X^i$ abbiamo

$$\sigma(f(\alpha)) = \sigma(\sum a_i \alpha^i) = \sum \sigma(a_i)\sigma(\alpha)^i = \sum a_i \sigma(\alpha)^i = f(\sigma(\alpha))$$

Proposizione 21.2. *Sia $L = K[\gamma]$ e $[L : K] = n$. Siano $\gamma = \gamma_1, \ldots, \gamma_n$ le n radici del polinomio minimo di f. Allora esistono esattamente n K-isomorfismi di L $\sigma_1, \ldots, \sigma_n$ univocamente dati dalla condizione $\sigma_i(\gamma) = \gamma_i$. In particolare se L/K é un'estensione normale allora $|Gal(L/K)| = n$.*

Proof. Per l'osservazione precedente, se σ é un K-isomorfismo allora $\sigma(\gamma)$ deve essere una radice di f e quindi esiste i tale che $\sigma(\gamma) = \gamma_i$. E sappiamo giá per il teorema fondamentale delle estensioni semplici che esiste un unico K-isomorfismo $\sigma_i : K[\gamma] \to K[\gamma_i]$ che manda γ in γ_i. □

Esempio 21.3. Un'estensione di grado 2 é sempre normale. Infatti, se $[L : K] = 2$ allora esiste $\gamma \in L$, $\gamma \notin K$ tale che $L = K[\gamma]$ e $\gamma^2 \in K$.

Il seguente risultato mostra che le estensioni normali le possiamo vedere anche in un altro modo equivalente che giá conosciamo

Teorema 21.4. *Un'estensione L/K é normale se e solo se esiste un polinomio $f \in K[X]$ tale che L sia un campo di spezzamento per f.*

Proof. Sia L/K normale, $L = K[\gamma]$. Per la caratterizzazione dei K-isomorfismi abbiamo che tutte le radici del polinomio minimo f di γ stanno in L e quindi L é un campo di spezzamento di f.

Viceversa, se L é un campo di spezzamento di un polinomio f le cui radici sono $\alpha_1, \ldots, \alpha_n$ allora un K-isomorfismo σ deve permutare le radici α_i e quindi, siccome $L = K[\alpha_1, \ldots, \alpha_n]$ si ha $\sigma(L) = L$.

□

Abbiamo a questo punto una descrizione concreta di un'estensione normale. Siamo quasi arrivati al teorema fondamentale della teoria di Galois. Data un'estensione normale L/K in dichiamo con $\mathcal{F}(L/K)$ l'insieme dei campi intermedi, cioé i campi contenuti in L e conteneneti K e indichiamo con $\mathcal{G}(L/K)$ l'insieme dei sottogruppi di $Gal(L/K)$.

Osserviamo che se $F \in \mathcal{F}(L/K)$ allora l'estensione L/F é anche di Galois e che $Gal(L/F)$ é un sottogruppo di $Gal(L/K)$: infatti un F-isomorfismo é anche un K -isomorfismo.

Osserviamo anche che se $H \in \mathcal{G}(L/K)$ allora $L^H = \{\alpha \in L : h(\alpha) = \alpha \ \forall h \in H\}$ é un campo intermedio tra K e L. Abbiamo quindi costruito una funzione

$$\begin{aligned} \mathcal{F}(L/K) &\to \mathcal{G}(L/K) \\ F &\mapsto Gal(L/F) \end{aligned}$$

e una funzione

$$\begin{aligned} \mathcal{G}(L/K) &\to \mathcal{F}(L/K) \\ H &\mapsto L^H \end{aligned}$$

Teorema 21.5 (Corrispondenza di Galois)**.** *Le due funzioni qui sopra sono una l'inversa dell'altra, si ha cioé*

(1) $L^{Gal(L/F)} = F$ *per ogni campo intermedio* $F \in \mathcal{F}(L/K)$*;*
(2) $Gal(L/L^H) = H$ *per ogni sottogruppo* $H \in \mathcal{G}(L/K)$*.*

Si ha inoltre

$$|H| = [L : L^H] \ \ \forall H \in \mathcal{G}(L/K).$$

Dimostrazione (prima parte). Mostriamo la (1) e sia quindi F un campo intermedio e indichiamo $r = [L : F]$ per cui $|Gal(L/F)| = r$. Chiaramente F é fissato dagli elementi di $Gal(L/F)$ per definizione, per cui $F \subseteq L^{Gal(L/F)}$ e quindi $[L : L^{Gal(L/F)}] \leq r$. D'altra parte abbiamo almeno r isomorfismi di L che fissano $L^{Gal(L/F)}$ per cui $[L : L^{Gal(L/F)}] \geq r$. Il risultato segue. □

La seconda parte della corrispondenza di Galois é piú delicata e la vedremo come conseguenze del seguente fondamentale

Lemma 21.6 (di Artin)**.** *Sia* H *un sottogruppo di* $Gal(L/K)$*. Allora*

$$[L : L^H] \leq |H|.$$

Proof. Sia $|H| = n$ e mostriamo che $n+1$ elementi di L sono linearmente dipendenti su L^H. Siano quindi $\alpha_1, \ldots, \alpha_{n+1} \in L$ e siano $h_1 = id, h_2, \ldots, h_n$ gli elementi di H. Consideriamo il seguente sistema lineare a coefficienti in L

$$\begin{cases} h_1(\alpha_1)x_1 + \cdots + h_1(\alpha_{n+1})x_{n+1} = \alpha_1 x_1 + \cdots + \alpha_{n+1}x_{n+1} = 0 \\ h_2(\alpha_1)x_1 + \cdots + h_2(\alpha_{n+1})x_{n+1} = 0 \\ \cdots \\ h_n(\alpha_1)x_1 + \cdots + h_n(\alpha_{n+1})x_{n+1} = 0 \end{cases}$$

Tale sistema é omogeneo con n equazioni e $n+1$ incognite per cui esiste una soluzione non nulla. Fra tutte le soluzioni non nulle ne scegliamo una che indichiamo $(\beta_1, \ldots, \beta_{n+1})$ e che abbia il massimo numero di zeri tra i suoi coefficienti. Possiamo anche supporre che tale soluzione abbiamo un coefficiente uguale a 1, e senze perdere di generalitá per semplicitá di notazione supponiamo sia $\beta_1 = 1$. Vogliamo mostrare che tutti i coefficienti $\beta_1, \ldots, \beta_{n+1} \in L^H$, cosicché la prima equazione del sistema ci assicura che $\alpha_1, \ldots, \alpha_{n+1}$ sono linearmente dipendenti su L^H. Supponiamo quindi per assurdo che esiste un coefficiente, diciamo

$\beta_2 \notin L^H$ e sia quindi $h \in H$ tale che $h(\beta_2) \neq \beta_2$. Osserviamo ora che $(h(\beta_1), \dots, h(\beta_{n+1})$ é una soluzione del nostro sistema: infatti, per ogni $i = 1, \dots, n$

$$h_i(\alpha_1)h(\beta_1) + \cdots + h_i(\alpha_{n+1})h(\beta_{n+1}) = h\big(h^{-1}h_i(\alpha_1)\beta_1 + h^{-1}h_i(\alpha_{n+1}\beta_{n+1}\big) = h(0) = 0$$

dove abbiamo semplicemente sfruttato che $h^{-1}h_i = h_j$ per un opportuno indice j. Abbiamo a questo punto due soluzioni diverse del sistema: la loro differenza $(1-1, \beta_2 - h(\beta_2), \beta_3 - h(\beta_3), \dots, \beta_{n+1} - h(\beta_{n+1})$ é una soluzione non nulla (perché la seconda coordinata é non nulla) e che ha almeno una coordinata nulla in piú rispetto alla soluzione da cui siamo partiti. □

Siamo ora pronti a completare la dimostrazione della corrispondenza di Galois. Dato $H \in \mathcal{G}(L/H)$ abbiamo che $H \subseteq Gal(L/L^H)$, da cui $|H| \leq [L : L^H]$. Il lemma di Artin ci fornisce la disuguaglianza opposta per cui vale l'uguaglianza e $H = Gal(L/L^H)$.

Esempio 21.7. Consideriamo l'estensione $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ di $\mathbb{Q}$. Questa estensione é normale perché é il campo di spezzamento di $(X^2 - 2)(X^2 - 3)$ ed ha grado 4. Il gruppo di Galois ha quindi ordine 4. Siccome un automorfismo deve mandare $\sqrt{2}$ in $\pm\sqrt{2}$ e $\sqrt{3}$ in $\pm\sqrt{3}$ gli elementi del gruppo di Galois hanno tutti ordine 2 e quindi il gruppo di Galois di questa estensione é il gruppo di Klein. Il gruppo di Klein ha 3 sottogruppi di ordine 2 e quindi abbiamo esattamente tre estensioni intermedie di ordine 4/2=2 che sono $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{6}]$.