CAPITOLO 1

Anelli

Il nome "anello" dato alle strutture che studieremo ora è dovuto a Dedekind, che fu uno dei primi ad indagare le proprietà degli interi da un punto di vista astratto e diede il nome di "Zahlring" all'insieme degli interi. Ci si accorse subito che il concetto comprendeva anche quello di campo di numeri, già allora usato: si tratta semplicemente dei sistemi dei numeri reali e complessi.

1.1. Generalità

Come abbiamo già detto, un esempio di anello è l'insieme degli interi, che ha *due* operazioni.

DEFINIZIONE. Un anello è un insieme A con due operazioni, denotate in modo generico come addizione e moltiplicazione, tali che:
(1) l'addizione è associativa;
(2) l'addizione ha elemento neutro 0;
(3) ogni elemento ha opposto rispetto all'addizione;
(4) la moltiplicazione è associativa;
(5) la moltiplicazione ha elemento neutro 1;
(6) la moltiplicazione è *distributiva* rispetto all'addizione, cioè, per ogni $a, b, c \in A$,

$$a(b+c) = ab + ac \qquad \text{e} \qquad (a+b)c = ac + bc.$$

Notiamo che, nelle formule delle proprietà distributive, la notazione è ambigua; non lo è se rispettiamo la convenzione che la moltiplicazione ha la precedenza sull'addizione. Perciò $ab + ac$ significa "la somma di ab con ac". Naturalmente la notazione generica può lasciare spazio ad una notazione specifica; ne vedremo esempi.

Vediamo subito alcune conseguenze delle proprietà degli anelli.

PROPOSIZIONE. *Se A è un anello allora l'addizione è commutativa.*

DIMOSTRAZIONE. Siano $a, b \in A$; allora l'espressione $(1+1)(a+b)$ si può sviluppare in due modi: per semplicità scriviamo $x = 1+1$ e $y = a+b$. Allora

$$(1+1)(a+b) = x(a+b) = xa + xb = (1+1)a + (1+1)b = 1a + 1a + 1b + 1b = a + a + b + b;$$

$$(1+1)(a+b) = (1+1)y = 1y + 1y = y + y = a + b + a + b.$$

In definitiva

$$a + a + b + b = a + b + a + b$$

e, sommando $-a$ a sinistra e $-b$ a destra, otteniamo $a + b = b + a$. □

Spesso allora un anello è definito come un insieme A con due operazioni, addizione e moltiplicazione, in modo che
(1) $A, +$ è un gruppo abeliano;
(2) $A, \cdot$ è un semigruppo con 1;
(3) la moltiplicazione è *distributiva* rispetto all'addizione.

Notiamo che non abbiamo richiesto che la moltiplicazione sia commutativa: di fatto in molti anelli interessanti questo non vale. Un anello in cui la moltiplicazione è commutativa, si dice *commutativo.*[*]

Esempi di anelli sono: gli interi $\mathbf{Z}$, i razionali $\mathbf{Q}$, i reali R e i complessi $\mathbf{C}$. Tutti questi sono commutativi. Se $n > 1$, le matrici $n \times n$ a coefficienti complessi, rispetto alla somma di matrici e al prodotto righe per colonne, sono un anello *non commutativo* $M_n(\mathbf{C})$.

PROPOSIZIONE. *Sia A un anello e siano $a, b \in A$.*
(1) $a0 = 0a = 0$;

[*]Per motivi storici è *proibitissimo* dire che un anello commutativo è abeliano!

(2) $a(-b) = -(ab) = (-a)b$.

DIMOSTRAZIONE. Scriviamo $x = a0$. Allora $x = a0 = a(0+0) = a0 + a0 = x + x$. Ne segue che $x = 0$.

Verifichiamo che $a(-b)$ è l'opposto di ab: infatti

$$ab + a(-b) = a(b + (-b)) = a0 = 0.$$

Le altre asserzioni si dimostrano in modo analogo. □

In generale, come già stabilito in altre occasioni, scriveremo $a - b$ come abbreviazione di $a + (-b)$ e $-ab$ invece di $-(ab)$. Per la proposizione appena dimostrata, l'ultimo simbolo non è ambiguo.

Come al solito, alcuni anelli hanno proprietà migliori di altri: per essi valgono allora risultati particolari e perciò si dà loro un nome diverso.

DEFINIZIONE. Un anello commutativo A si dice un *dominio* (*di integrità*) se $1 \neq 0$ e, per $a, b \in A$,

$$\text{da } ab = 0 \text{ segue } a = 0 \text{ oppure } b = 0.$$

Un anello commutativo A si dice un *campo* se $1 \neq 0$ ed ogni elemento diverso da 0 di A è invertibile (rispetto alla moltiplicazione).

Notiamo che nella definizione di dominio e di campo imponiamo che sia $1 \neq 0$. Il motivo è che si voglio evitare casi banali.

PROPOSIZIONE. *Se nell'anello A vale $1 = 0$, allora $A = \{0\}$.*

DIMOSTRAZIONE. Se $a \in A$, allora $a = a1 = a0 = 0$. □

La proposizione può essere sorprendente, perché contro il senso comune: quando mai è $1 = 0$? Il fatto è che 0 denota l'elemento neutro per l'addizione e 1 quello per la moltiplicazione e nessuno vieta che possano essere uguali. Se sono uguali, la proprietà distributiva fa sì che non ci possano essere altri elementi.

PROPOSIZIONE. *Ogni campo è un dominio.*

DIMOSTRAZIONE. Sia A un campo e siano $a, b \in A$ tali che $ab = 0$. Se $a = 0$, non c'è nulla da dimostrare. Se $a \neq 0$, allora a è invertibile e perciò

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

Quindi da $ab = 0$ segue che $a = 0$ oppure $b = 0$. □

Esempi di campi sono $\mathbf{Q}$, $\mathbf{R}$ e $\mathbf{C}$. Invece $\mathbf{Z}$ è un dominio che non è un campo, poiché gli elementi invertibili di $\mathbf{Z}$ sono solo 1 e -1. Daremo più avanti altri esempi molto importanti di campi.

1.2. Omomorfismi, ideali e sottoanelli

Siano A e B due anelli e sia $f\colon A \to B$ un'applicazione. Poiché A ha due operazioni, diremo che f è un omomorfismo di anelli, se $f\colon A, + \to B, +$ e $f\colon A, \cdot \to B, \cdot$ sono omomorfismi, rispettivamente di gruppi e di semigruppi con 1.

DEFINIZIONE. Siano A e B anelli. Un'applicazione $f\colon A \to B$ si dice un *omomorfismo di anelli* se

(1) per $a, b \in A$, $f(a + b) = f(a) + f(b)$;
(2) per $a, b \in A$, $f(ab) = f(a)f(b)$;
(3) $f(1) = 1$.

Poiché f è in particolare un omomorfismo di gruppi, il suo nucleo $\ker f$ è un sottogruppo di $A, +$. Decidiamo ancora di chiamarlo *nucleo di* f. Al solito, poi, l'omomorfismo f definisce una congruenza sull'anello A, cioè rispetto a entrambe le operazioni: infatti, come è ovvio,

$$\text{da } a \sim_f b \text{ e } c \sim_f d, \text{ segue che } a + c \sim_f b + d \text{ e } ac \sim_f bd.$$

Perciò $A/\sim_f$ diventa un anello con le operazioni

$$[a] + [b] = [a + b] \qquad \text{e} \qquad [a][b] = [ab].$$

L'unico requisito da verificare è che valgano le proprietà distributive, ma questo è facile e si lascia per esercizio.

Anche in questo caso, invece di scrivere $A/\sim_f$, scriveremo $A/\ker f$.

Sia ora $\sim$ una congruenza su A (cioè una congruenza su $A,+$ e su $A,\cdot$). Allora, per $a,b\in A$,

$$a\sim b \quad \text{se e solo se} \quad a-b\sim 0$$

e quindi la congruenza è determinata dalla classe di equivalenza di 0. Poniamo $I=[0]_\sim$. Allora I è un sottogruppo di $A,+$. Che proprietà ha rispetto alla moltiplicazione?

Se $x\in I$ e $a\in A$, allora $x\sim 0$ e $a\sim a$, e perciò

$$ax\sim x0, \qquad xa\sim 0x$$

cioè $ax\sim 0$ e $xa\sim 0$. Ne segue che

$$ax\in I \qquad \text{e} \qquad xa\in I.$$

Vedremo che queste proprietà sono sufficienti per determinare una congruenza.

Definizione. Sia A un anello e sia $I\subseteq A$. Allora I si dice un *ideale* di A se:

(1) $0\in I$;
(2) da $x,y\in I$ segue $x+y\in I$;
(3) da $x\in I$ segue $-x\in I$;
(4) da $a\in A$ e $x\in I$ segue $ax\in I$ e $xa\in I$.

Naturalmente le prime tre condizioni esprimono il fatto che I è un sottogruppo di $A,+$ e quindi si possono ridurre alla verifica che I non è vuoto e che, da $x,y\in I$ segue $x-y\in I$.

Proposizione. *Sia I un ideale dell'anello A e definiamo la relazione $\sim$ ponendo, per $a,b\in A$,*

$$a\sim b \qquad \textit{se e solo se} \qquad a-b\in I.$$

Allora la relazione $\sim$ è una congruenza su A e $[0]_\sim=I$.

Dimostrazione. Che da $a\sim b$ e $c\sim d$ segua $a+c\sim b+d$ discende dal fatto corrispondente già dimostrato per i gruppi. Verifichiamo che vale anche $ac\sim bd$. Infatti

$$ac-bd=ac-bc+bc-bd=(a-b)c+b(c-d).$$

Ma $a-b\in I$ e quindi $(a-b)c\in I$; inoltre $c-d\in I$ e quindi $b(c-d)\in I$. In definitiva, $ac-bd\in I$, cioè $ac\sim bd$. □

Se $\sim$ è una congruenza su A e $I=[0]_\sim$, scriveremo A/I per denotare l'anello quoziente $A/\sim$. In tal caso è chiaro che la proiezione $\pi\colon A\to A/I$ è un omomorfismo di anelli.

Abbiamo anche, come è ovvio il teorema di omomorfismo per gli anelli.

Teorema. *Sia $f\colon A\to B$ un omomorfismo di anelli e sia $\pi\colon A\to A/I$ la proiezione. Allora esiste un unico omomorfismo di anelli $\widetilde{f}\colon A/I\to B$ tale che $f=\widetilde{f}\circ\pi$. Inoltre $\widetilde{f}$ è iniettivo ed è suriettivo se e solo se f è suriettivo.*

Abbiamo anche il teorema di corrispondenza, ma lo enunceremo dopo aver definito il concetto di sottoanello.

Definizione. Un sottoinsieme S dell'anello A è un *sottoanello* se è un sottogruppo di $A,+$ ed un sottosemigruppo di $A,\cdot$. Perciò S è un sottoanello se e solo se:

(1) $0\in S$;
(2) da $a,b\in S$ segue $a+b\in S$;
(3) da $a\in S$ segue $-a\in S$;
(4) $1\in S$;
(5) da $a,b\in S$ segue $ab\in S$.

Proposizione. *Sia A un anello e sia $S\subseteq A$; allora S è un sottoanello di A se e solo se:*

(a) $1\in S$;
(b) *da $a,b\in S$ segue $a-b\in S$ e $ab\in S$.*

Dimostrazione. Le condizioni sono ovviamente necessarie.

Dimostriamo la sufficienza. Poiché $1\in S$, $S\neq\emptyset$. Inoltre è un sottogruppo di $A,+$ ed un sottosemigruppo di $A,\cdot$. □

Non è difficile verificare la seguente proposizione.

Proposizione. *Sia $f\colon A\to B$ un omomorfismo di anelli. Allora* $\operatorname{im} f$ *è un sottoanello di B.*

Il teorema di corrispondenza per gli anelli è un po' diverso da quello per i gruppi; questa diversità dovrebbe mettere in maggior luce la distinzione fra il concetto di sottogruppo e quello di sottogruppo normale. Infatti i concetti corrispondenti per gli anelli sono, rispettivamente, quello di sottoanello e di ideale.

PROPOSIZIONE. *Sia A un anello e sia $S \subseteq A$; allora, se S è un sottoanello e un ideale, necessariamente $S = A$.*

DIMOSTRAZIONE. Siccome S è un sottoanello, $1 \in S$; sia $a \in A$: allora, poiché S è un ideale, $a = a1 \in S$. □

Se I è un ideale di A, poniamo

$$\begin{aligned}\mathscr{L}_i(A; \supseteq I) &= \text{ideali di } A \text{ contenenti } I;\\ \mathscr{L}_s(A; \supseteq I) &= \text{sottoanelli di } A \text{ contenenti } I;\\ \mathscr{L}_i(A) &= \text{ideali di } A = \mathscr{L}_i(A; \supseteq \{0\});\\ \mathscr{L}_s(A) &= \text{sottoanelli di } A = \mathscr{L}_s(A; \supseteq \{0\}).\end{aligned}$$

È evidente che tutti questi sono reticoli, rispetto all'ordinamento per inclusione: dimostrare che, dati $J, J' \in \mathscr{L}_i(A; \supseteq I)$ (rispettivamente $S, S' \in \mathscr{L}_s(A; \supseteq I)$), allora

$$J \wedge J' = J \cap J' \quad \text{e} \quad J \vee J' = J + J'$$
$$S \wedge S' = S \cap S'$$

dove, dati $X, Y \subseteq A$, $X + Y$ denota l'insieme di tutti gli elementi di A che si possono scrivere come somma di un elemento di X con un elemento di Y. Non è altrettanto semplice descrivere $S \vee S'$.

TEOREMA. *Sia $f\colon A \to B$ un omomorfismo suriettivo di anelli. Allora esistono due isomorfismi di reticoli*

$$\begin{aligned}\Phi_{i;f}\colon \mathscr{L}_i(A; \supseteq \ker f) &\to \mathscr{L}_i(B) & \qquad \Phi_{s;f}\colon \mathscr{L}_s(A; \supseteq \ker f) &\to \mathscr{L}_s(B)\\ I &\mapsto f^{\rightarrow}(I) & S &\mapsto f^{\rightarrow}(S)\end{aligned}$$

DIMOSTRAZIONE. La dimostrazione procede esattamente come quella del teorema corrispondente per i gruppi. Gli isomorfismi inversi si definiscono usando immagini inverse. □

Nel caso dei semigruppi abbiamo dimostrato una "proprietà di unicità" per gli omomorfismi di $\mathbf{N}, +$ in un semigruppo; un risultato analogo vale per $\mathbf{Z}$ e gli omomorfismi in un gruppo. Vediamo che $\mathbf{Z}$ ha anche una proprietà di unicità per gli omomorfismi di anello.

PROPOSIZIONE. *Sia A un anello. Allora esiste un unico omomorfismo di anelli $\chi_A\colon \mathbf{Z} \to A$.*

DIMOSTRAZIONE. Supponiamo che $f\colon \mathbf{Z} \to A$ sia un omomorfismo di anelli. Allora $f(1) = 1$ e, con facile induzione, $f(n) = n1$, per $n \geq 0$ (attenzione: $n1$ al secondo membro indica il multiplo di 1 secondo n). Ma allora è anche $f(-n) = (-n)1$ e quindi $f(z) = z1$, per ogni $z \in \mathbf{Z}$.

Facciamo allora vedere che, ponendo $z \mapsto z1$ otteniamo un omomorfismo di anelli $\chi_A\colon \mathbf{Z} \to A$.

Per l'addizione non ci sono problemi, basta applicare le proprietà dei multipli. Inoltre $\chi_A(1) = 1$. Dobbiamo allora verificare che $\chi_A(z_1 z_2) = \chi_A(z_1)\chi_A(z_2)$. Siccome "meno per meno fa più", ci basta verificare la cosa sui naturali. Dimostriamo allora, per induzione su n che

$$(mn)1 = (m1)(n1).$$

L'unica difficoltà è quella di distinguere il numero naturale 1 dall'elemento 1 dell'anello. Per semplificare le cose indicheremo con $\mathbf{e}$ l'elemento 1 dell'anello. Allora dobbiamo mostrare che

$$(mn)\mathbf{e} = (m\mathbf{e})(n\mathbf{e}).$$

Per $n = 0$ la cosa è ovvia. Supponiamola vera per n. Allora

$$(m(n+1))\mathbf{e} = (mn + m)\mathbf{e} = (mn)\mathbf{e} + m\mathbf{e} = (m\mathbf{e})(n\mathbf{e}) + (m\mathbf{e})\mathbf{e} = (m\mathbf{e})(n\mathbf{e} + \mathbf{e}) = (m\mathbf{e})((n+1)\mathbf{e})$$

e la tesi è provata. □

COROLLARIO. *Sia A un anello e siano $a, b \in A$ e $m, n \in \mathbf{Z}$; allora*

$$(ma)(nb) = (mn)(ab).$$

DIMOSTRAZIONE. Indichiamo ancora con $\mathbf{e}$ l'elemento 1 dell'anello. Allora, per $m \geq 0$,

$$ma = m(\mathbf{e}a) = (m\mathbf{e})a = a(m\mathbf{e}),$$

con una facile induzione su m. L'affermazione per $m < 0$ è allora ovvia. Perciò

$$(ma)(nb) = a(m\mathbf{e})(n\mathbf{e})b = a\chi_A(m)\chi_A(n)b = a\chi_A(mn)b = a((mn)\mathbf{e})b = ((mn)\mathbf{e})(ab) = (mn)(ab)$$

e la tesi è dimostrata. □

In base a questi risultati, possiamo fare la seguente convenzione:

Se A è un anello e $n \in \mathbf{Z}$, chiamiamo ancora n l'immagine $\chi_A(n)$.

Non ci preoccuperemo più, quindi, di che cosa denotiamo con 1, parlando di un anello.

Attenzione: possono accadere cose strane, quando si adopera questa convenzione; tuttavia, con un po' di attenzione, non ci sono difficoltà.

PROPOSIZIONE. *Sia A un anello tale che, per ogni $a \in A$, $a^2 = a$. Allora A è commutativo e, per ogni $a \in A$, $2a = 0$.*

DIMOSTRAZIONE. Sia $a \in A$ e poniamo $c = 2a$. Allora, per l'ultimo corollario, $c^2 = (2a)(2a) = 4a^2$. Ma, per ipotesi, $c^2 = c$ e $a^2 = a$: perciò

$$c^2 = 4a^2 = 4a = c = 2a$$

e quindi $4a - 2a = 0$, da cui $2a = 0$. In particolare $a + a = 0$ e quindi $a = -a$, per ogni $a \in A$.

Siano ora $a, b \in A$ e poniamo $c = a + b$. Allora

$$a + b = c = c^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b$$

e quindi $ab + ba = 0$, cioè $ba = -ab$. Ma $-ab = ab$ e quindi $ba = ab$. □

Un anello con questa proprietà si chiama *anello di Boole*. Vedremo più avanti quali sono le connessioni con i reticoli di Boole.

In un anello di Boole, quindi, $2 = 0$ (perché $2 = 1 + 1 = 2 \cdot 1 = 0$).

1.3. Il campo razionale

L'anello degli interi è un dominio, ma non un campo. È possibile trovare un campo che contiene gli interi? Il problema è analogo a quello che abbiamo risolto in precedenza: trovare un gruppo che contiene il semigruppo $\mathbf{N}, +$.

Possiamo, in realtà risolvere il problema per ogni dominio.

Sia A un dominio e consideriamo $X = A \times (A \setminus \{0\})$, cioè l'insieme delle coppie ordinate di elementi di A, con seconda componente *non nulla*. Definiamo una relazione $\sim$ su X ponendo

$$(a, b) \sim (c, d) \qquad \text{se e solo se} \qquad ad = bc.$$

La relazione appena definita è una relazione di equivalenza. Che sia riflessiva e simmetrica è ovvio. Supponiamo allora $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Allora $ad = bc$ e $cf = de$; quindi

$$(ad)f = (bc)f = b(cf) = b(de)$$

cioè $d(af) = d(be)$ (notiamo che abbiamo usato la proprietà commutativa della moltiplicazione). Ne segue che $d(af - be) = 0$ e, essendo per ipotesi $d \neq 0$, ne segue che $af = be$, cioè che $(a, b) \sim (e, f)$.

Poniamo allora $Q(A) = X/\sim$ e indichiamo con il simbolo

$$\frac{a}{b}$$

la classe di equivalenza della coppia (a, b); useremo anche la notazione a/b, per risparmiare spazio.

Definiamo su $Q(A)$ due operazioni:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{e} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

La prima cosa da verificare è che queste operazioni siano *ben definite*, cioè che, se $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$, allora

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} \qquad \text{e} \qquad \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

In tal modo la definizione delle operazioni non dipende dal rappresentante delle classi di equivalenza. Verifichiamo l'addizione. Sappiamo che $ab' = a'b$ e $cd' = c'd$; dobbiamo allora stabilire che

$$(ad + bc)b'd' = (a'd' + b'c')bd.$$

Abbiamo dunque

$$(ad+bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'cd' = (a'd' + b'c')bd.$$

La verifica per la moltiplicazione è lasciata per esercizio. Naturalmente è necessario anche verificare che $(ad+bc, bd) \in X$, ma questo segue dal fatto che A è un dominio e che $b \neq 0$, $d \neq 0$.

Ora che le operazioni sono definite, dimostriamo che $Q(A)$, con queste operazioni, è un anello.

Associatività dell'addizione

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}$$
$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf + bcf + bde}{bdf}$$

Esistenza dello zero

$$\frac{0}{1} + \frac{a}{b} = \frac{0b+1a}{1b} = \frac{a}{b}$$
$$\frac{a}{b} + \frac{0}{1} = \frac{a1+b0}{b1} = \frac{a}{b}$$

Esistenza dell'opposto

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab-ba}{ab} = \frac{0}{ab}$$
$$\frac{-a}{b} + \frac{a}{b} = \frac{-ab+ba}{ab} = \frac{0}{ab}$$

Possiamo concludere: infatti

$$\frac{a}{b} = \frac{0}{1} \qquad \text{se e solo se} \qquad a1 = b0 = 0.$$

Pertanto $a/b = 0/1$ se e solo se $a = 0$. Ne segue che $a/b + (-a)/b = (-a)/b + a/b = 0/1$.

Associatività della moltiplicazione

$$\left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f} = \frac{ac}{bd}\frac{e}{f} = \frac{ace}{bdf}$$
$$\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right) = \frac{a}{b}\frac{ce}{df} = \frac{ace}{bdf}$$

Esistenza di 1

$$\frac{1}{1}\frac{a}{b} = \frac{1a}{1b} = \frac{a}{b}$$
$$\frac{a}{b}\frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}$$

Proprietà distributiva Esercizio; basta dimostrarne una, in quanto la moltiplicazione è commutativa:

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\frac{a}{b}$$

Analogamente a prima, abbiamo che $\frac{a}{b} = \frac{1}{1}$ se e solo se $a = b$.

PROPOSIZIONE. *L'anello $Q(A)$ è un campo ed esiste un omomorfismo iniettivo $j_A \colon A \to Q(A)$ con la seguente proprietà: se $x \in Q(A)$, allora esistono $a, b \in A$, con $b \neq 0$, tali che $x = j_A(a)j_A(b)^{-1}$.*

DIMOSTRAZIONE. Sia $a/b \in Q(A)$, $a/b \neq 0/0$. Allora $a \neq 0$ e quindi $b/a \in Q(A)$. È evidente che

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1},$$

perciò $b/a = (a/b)^{-1}$.

Definiamo l'applicazione $j_A \colon A \to Q(A)$ ponendo, per $a \in A$,

$$j_A(a) = \frac{a}{1}.$$

È facile verificare che j_A è un omomorfismo iniettivo di anelli (esercizio). Inoltre, se $b \in A$, $b \neq 0$,

$$\frac{1}{b} = \left(\frac{b}{1}\right)^{-1} = j_A(b)^{-1}$$

e quindi

$$\frac{a}{b} = \frac{a}{1}\frac{1}{b} = j_A(a)j_A(b)^{-1}$$

come si voleva. □

Come allora abbiamo già fatto, *identifichiamo* gli elementi di A con le loro immagini $a/1$ e, in tal modo, abbiamo un campo che contiene A.

Nel caso particolare di $A = \mathbf{Z}$, poniamo $Q(\mathbf{Z}) = \mathbf{Q}$, e lo chiamiamo *campo dei numeri razionali*. In tal caso, dal momento che sappiamo decomporre i numeri interi come prodotto di numeri primi, ogni elemento $q \in \mathbf{Q}$ si può scrivere *in modo unico* come $q = a/b$, dove $b > 0$ e $\mathrm{mcd}(a, b) = 1$. Questa scrittura di q si chiama *riduzione ai minimi termini*.

Se l'anello A è un campo, è in particolare un dominio e quindi possiamo eseguire la costruzione appena vista di $Q(A)$. Esercizio: dimostrare che, in tal caso, j_A è un isomorfismo (quindi la costruzione, eseguita a partire da un campo, non dà niente di nuovo).

L'esercizio appena visto mostra che la "costruzione" del campo dei reali a partire dai razionali ha bisogno di qualche altro metodo. Sono possibili due costruzioni, una che usa il concetto di "successione di Cauchy", l'altra quello di "sezione di Dedekind".

L'ultima cosa che vogliamo vedere sui razionali è che è possibile definire in $\mathbf{Q}$ una relazione d'ordine totale che estende quella sugli interi (cioè, per essere precisi, tale che $j_{\mathbf{Z}} \colon \mathbf{Z} \to \mathbf{Q}$ sia un omomorfismo di insiemi parzialmente ordinati). Poniamo

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

Si può verificare (esercizio) che questa è una relazione d'ordine totale che soddisfa la proprietà richiesta. Di fatto è l'*unica* relazione d'ordine che soddisfa la proprietà richiesta e tale che, dati $x, x_1, x_2, y_1, y_2 \in \mathbf{Q}$, con $0 \leq x$,

$$\text{da } x_1 \leq x_2 \text{ e } y_1 \leq y_2 \text{ segua } x_1 + y_1 \leq x_2 + y_2;$$
$$\text{da } x_1 \leq x_2 \text{ e segua } xx_1 \leq xx_2.$$

1.4. Gli ideali di Z

Abbiamo già classificato i sottogruppi di $\mathbf{Z}, +$; un ideale I di $\mathbf{Z}$ è necessariamente un sottogruppo di $\mathbf{Z}, +$ e perciò $I = n\mathbf{Z}$, per un unico $n \geq 0$. È però facile vedere che $n\mathbf{Z}$ è un ideale di $\mathbf{Z}$: infatti, se $x \in n\mathbf{Z}$ e $a \in \mathbf{Z}$, allora $x = ny$ per qualche y e

$$xa = (ny)a = n(ya) \in n\mathbf{Z}.$$

Proposizione. *Se I è un ideale di $\mathbf{Z}$, allora esiste uno ed un solo $n \in \mathbf{N}$ tale che $I = n\mathbf{Z}$. Se $n \in \mathbf{N}$, allora $n\mathbf{Z}$ è un ideale di $\mathbf{Z}$.*

Sia A un anello; allora $\ker \chi_A$ è un ideale di $\mathbf{Z}$ e quindi è della forma $n\mathbf{Z}$ per un unico $n \geq 0$; tale n si chiama la *caratteristica* di A.

Proposizione. *Sia A un anello di caratteristica $k > 0$; allora, per ogni $a \in A$, $ka = 0$. Inoltre k è il minimo intero positivo con tale proprietà.*

Dimostrazione. Sappiamo che $k\mathbf{Z} = \ker \chi_A$; questo vuol dire che $\chi_A(k) = k1 = 0$. Ma allora $ka = (k1)a = 0a = 0$. Se poi $na = 0$, per ogni $a \in A$, con $n > 0$, allora, in particolare $n1 = 0$, cioè $n \in \ker \chi_A$. Dunque $k \mid n$ e $k \leq n$. □

Molti degli anelli noti hanno caratteristica 0: è facile infatti vedere che, se A è un sottoanello di B, allora A e B hanno la stessa caratteristica (esercizio). Poiché $\mathbf{Z}$ ha caratteristica 0, lo stesso vale per $\mathbf{Q}$, $\mathbf{R}$ e $\mathbf{C}$.

Esercizio. Dimostrare che $M_n(\mathbf{C})$ e $M_n(\mathbf{R})$ hanno caratteristica 0. Dimostrare che, se $n \geq 0$, allora $\mathbf{Z}/n\mathbf{Z}$ ha caratteristica n.

Proposizione. *Se A è un dominio, allora la caratteristica di A è 0 oppure un numero primo.*

Dimostrazione. Supponiamo che la caratteristica di A sia $n > 0$ e scriviamo $n = hk$, con $h, k \geq 0$. Allora $n1 = 0 = (h1)(k1)$ e quindi, siccome siamo in un dominio, $h1 = 0$ oppure $k1 = 0$. Se $h1 = 0$, allora $h \in \ker \chi_A = n\mathbf{Z}$, e quindi $n \mid h$. Perciò $n = h$. Analogamente si procede se $k1 = 0$. □

1.5. La formula del binomio

Vogliamo ricavare, in termini generali, la classica formula del binomio, dimostrata da Newton e precorsa da molti, fra i quali Tartaglia, Pascal e anonimi matematici cinesi.

Il problema è quello di ricavare una formula per esprimere $(a+b)^n$. Questo è possibile solo se $ab = ba$; infatti, per esempio,

$$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2$$

e, se $ab \neq ba$, nulla di più si può dire.

Ricordiamo la definizione del simbolo binomiale: se $n, k \in \mathbf{N}$ e $n \geq k > 0$,

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{k!\,(n-k)!};$$

inoltre si pone

$$\binom{n}{0} = 1.$$

LEMMA. *Per $1 \leq k \leq n-1$,*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

DIMOSTRAZIONE. Abbiamo

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!\,(n-1-k)!} + \frac{(n-1)!}{(k-1)!\,(n-k)!} \\ &= \frac{(n-1)!}{(k-1)!\,(n-k-1)!}\left(\frac{1}{k} + \frac{1}{n-k}\right) \\ &= \frac{(n-1)!}{(k-1)!\,(n-k-1)!}\left(\frac{n-k+k}{k(n-k)}\right)\end{aligned}$$

e quindi la tesi. □

Notiamo che, come corollario a questo lemma, i coefficienti binomiali sono tutti numeri interi.

Il lemma è anche alla base della costruzione nota come *triangolo aritmetico* o *triangolo di Tartaglia*:

$(n=0)$							1							
$(n=1)$						1		1						
$(n=2)$					1		2		1					
$(n=3)$				1		3		3		1				
$(n=4)$			1		4		6		4		1			
$(n=5)$		1		5		10		10		5		1		
$(n=6)$	1		6		15		20		15		6		1	
$(n=7)$	1		7		21		35		35		21		7		1

nella quale ogni riga è determinata dalla precedente, scrivendo la somma dei coefficienti sovrastanti (e 1 all'inizio e alla fine).[†] Il fatto che questo triangolo fornisca i coefficienti per lo sviluppo di $(a+b)^n$ è il contenuto della proposizione seguente.

PROPOSIZIONE. *Siano $a, b \in A$ tali che $ab = ba$. Allora, per $n \in \mathbf{N}$,*

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

[†]Per evitare nazionalismi, si preferisce il nome di *triangolo aritmetico*. In effetti lo stesso triangolo è chiamato triangolo di Pascal in Francia, ma è stato trovato in un testo cinese del 1303; perciò né Tartaglia né tantomeno Pascal hanno la priorità della scoperta.

DIMOSTRAZIONE. L'asserto è ovvio per $n = 0$ e $n = 1$. Facciamo allora l'ipotesi che la tesi sia vera per $n-1$, con $n > 1$. Pertanto, dal momento che $b^m a = ab^m$,

$$\begin{aligned}
(a+b)^n = (a+b)^{n-1}(a+b) &= \left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k}\right)(a+b) \\
&= \sum_{l=0}^{n-1} \binom{n-1}{l} a^{l+1} b^{n-1-l} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k} \\
&= \sum_{l=0}^{n-2} \binom{n-1}{l} a^{l+1} b^{n-l-1} + a^n b^0 + a^0 b^n + \sum_{k=1}^{n-1} \binom{n-1}{k} a^k b^{n-k} \\
&= a^0 b^n + \left(\sum_{k=1}^{n-1} \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k=1}^{n-1} \binom{n-1}{k} a^k b^{n-k}\right) + a^n b^0 \\
&= a^0 b^n + \left(\sum_{k=1}^{n-1} \left(\binom{n-1}{k-1} + \binom{n-1}{k}\right) a^k b^{n-k}\right) + a^n b^0 \\
&= a^0 b^n + \left(\sum_{k=1}^{n-1} \binom{n}{k} a^k b^{n-k}\right) + a^n b^0 \\
&= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}
\end{aligned}$$

cioè la tesi. □

COROLLARIO. *Se $n > 0$, allora*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

DIMOSTRAZIONE. Entrambi i membri sono uno sviluppo di $(1+1)^n$. □

Non è un caso che, nelle righe del triangolo aritmetico corrispondenti a numeri primi i coefficienti interni siano tutti divisibili per quel numero primo.

LEMMA. *Se p è primo e $0 < k < p$, allora p divide $\binom{p}{k}$.*

DIMOSTRAZIONE. Infatti

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!},$$

e il numeratore della frazione è divisibile per p, mentre il denominatore non lo è. □

PROPOSIZIONE. *Sia A un anello di caratteristica p, con p numero primo. Se $a, b \in A$ e $ab = ba$, allora*

$$(a+b)^p = a^p + b^p.$$

DIMOSTRAZIONE. Basta sviluppare il binomio e osservare che tutti i termini intermedi sono moltiplicati per un multiplo di $p = 0$. □

COROLLARIO. *Sia A un anello commutativo di caratteristica p, con p numero primo. Allora l'applicazione $\Phi_A \colon A \to A$ definita da $\Phi_A(a) = a^p$ è un omomorfismo di anelli.*

DIMOSTRAZIONE. La proposizione precedente dice che $\Phi_A(a+b) = \Phi_A(a) + \Phi_A(b)$; il fatto che $\Phi_A(ab) = \Phi_A(a)\Phi_A(b)$ è già noto; è ovvio poi che $\Phi_A(1) = 1$. □

L'omomorfismo Φ_A si chiama *omomorfismo di Frobenius*.

PROPOSIZIONE. *Se A è un campo finito, allora A ha caratteristica p, con p numero primo e Φ_A è un isomorfismo.*

DIMOSTRAZIONE. Se A ha caratteristica 0, allora $n1 \neq 0$, per ogni $n \in \mathbf{N}$, $n > 0$. Ne segue che gli elementi $n1$, per $n \in \mathbf{N}$, sono tutti distinti. Pertanto A è infinito.

Sia p la caratteristica di A: allora $p > 0$ è un numero primo, perché A è un campo e, in particolare, un dominio. Inoltre $\Phi_A(1) = 1 \neq 0$ e quindi $1 \notin \ker \Phi_A$. Ma allora, essendo $\ker \Phi_A$ un ideale di A, è necessariamente $\ker \Phi_A = \{0\}$ e quindi Φ_A è iniettivo. Ora, essendo A finito, Φ_A è anche suriettivo. □

1.6. Ideali principali, primi e massimali

In questa sezione studieremo solo anelli commutativi.

Sia A un anello commutativo e sia $a \in A$; allora

$$aA = \{\, ax \mid x \in A \,\}$$

è un ideale di A, che si chiama *ideale principale generato da* a. Infatti $0 = a0 \in aA$; inoltre, se $x, y \in A$, abbiamo $ax - ay = a(x - y) \in aA$. Per finire, se $x, y \in A$, allora $(ax)y = a(xy) \in aA$.

La classificazione degli ideali di $\mathbf{Z}$ dice allora che ogni ideale di $\mathbf{Z}$ è principale. In generale un anello può avere ideali non principali. Vedremo più avanti esempi di altri anelli commutativi in cui ogni ideale è principale.

DEFINIZIONE. Sia A un anello commutativo; un ideale I di A si dice *primo* se, per $a, b \in A$,

$$\text{da } ab \in I \text{ segue } a \in I \text{ oppure } b \in I.$$

PROPOSIZIONE. *Un ideale I dell'anello commutativo A è primo se e solo se A/I è un dominio.*

DIMOSTRAZIONE. ($\Rightarrow$) Sia $[a][b] = [0]$ in A/I: allora $ab \in I$ e quindi $a \in I$ oppure $b \in I$; ne segue che $[a] = [0]$ oppure $[b] = [0]$.

($\Leftarrow$) Supponiamo $ab \in I$; allora $[ab] = [0]$, quindi $[a][b] = [0]$. Perciò $[a] = [0]$ oppure $[b] = [0]$, che è la tesi. □

Dire che $\{0\}$ è un ideale primo di A equivale a dire che A è un dominio: infatti A è isomorfo a $A/\{0\}$.

Gli ideali primi si chiamano così perché gli ideali primi di $\mathbf{Z}$ corrispondono ai numeri primi.

PROPOSIZIONE. *Sia $n \in \mathbf{N}$; allora $n\mathbf{Z}$ è un ideale primo se e solo se $n = 0$ oppure n è primo.*

DIMOSTRAZIONE. Per $n = 0$, $0\mathbf{Z} = \{0\}$ è primo perché $\mathbf{Z}$ è un dominio.

Supponiamo $n > 0$ e che l'ideale $n\mathbf{Z}$ sia primo; se $n = ab$, con $a, b \in \mathbf{N}$, allora $ab \in n\mathbf{Z}$ e quindi $a \in n\mathbf{Z}$ oppure $b \in n\mathbf{Z}$. Nel primo caso abbiamo $n \mid a$ e perciò $a = n$; nel secondo caso abbiamo $b = n$. Quindi n è primo.

Supponiamo n primo e siano $a, b \in \mathbf{Z}$ tali che $ab \in n\mathbf{Z}$. Allora $n \mid ab$ e quindi $n \mid a$ oppure $n \mid b$. In altre parole $a \in n\mathbf{Z}$ oppure $b \in n\mathbf{Z}$. □

Abbiamo già osservato che l'insieme degli ideali di un anello è un reticolo rispetto all'inclusione, $\mathscr{L}_i(A)$. Il lemma seguente vale anche per anelli non commutativi. Ricordiamo che un ideale I dell'anello A è *proprio* se $I \neq A$.

LEMMA. *Sia A un anello e sia I un ideale di A. Allora I è proprio se e solo se $1 \notin I$.*

DIMOSTRAZIONE. Se $1 \notin I$, certamente I è proprio. Viceversa, se $1 \in I$, allora, per ogni $a \in A$, $a = a1 \in I$ e quindi $I = A$. □

DEFINIZIONE. Un ideale I dell'anello A si dice *massimale* se è un elemento massimale di $\mathscr{L}_i(A) \setminus \{A\}$, cioè se è massimale fra gli ideali propri dell'anello A.

Come si fa a verificare che un ideale I è massimale? Ci sono due modi equivalenti: (1) si prende un ideale J tale che $I \subset J$ e si dimostra che $J = A$; oppure (2) si prende un ideale proprio J tale che $I \subseteq J$ e si dimostra che $I = J$.

La proposizione che segue vale solo per anelli commutativi.

PROPOSIZIONE. *Sia A un anello commutativo e sia I un ideale di A. Allora I è massimale se e solo se A/I è un campo.*

DIMOSTRAZIONE. Si possono usare due metodi: il primo è diretto e il secondo fa uso del teorema di corrispondenza.

Primo metodo.

($\Rightarrow$) Supponiamo che I sia massimale e sia $[a] \in A/I$, $[a] \neq [0]$. Allora $a \notin I$ e quindi l'ideale $aA + I$ contiene propriamente I, perché $a = a1 + 0 \in aA + I$. Ne segue che $aA + I = A$ e quindi esistono $x \in A$ e $y \in I$ tali che $1 = ax + y$. Passando alle classi di equivalenza,

$$[1] = [ax + y] = [a][x] + [y] = [a][x]$$

e quindi $[x]$ è l'inverso di $[a]$.

($\Leftarrow$) Supponiamo che A/I sia un campo e supponiamo che J sia un ideale di A tale che $I \subset J$. Sia $a \in J \setminus I$; allora $[a] \neq [0]$ in A/I e quindi esiste $b \in A$ tale che $[a][b] = [1]$. Otteniamo $ab - 1 \in I$ e quindi $ab - 1 = x \in J$. Ma da $a \in J$ segue $ab \in J$ e perciò $1 = ab - x \in J$. Dunque $J = A$.

Secondo metodo Sappiamo che un anello commutativo $B \neq \{0\}$ è un campo se e solo se ha esattamente due ideali, cioè $\{0\}$ e B. Perciò A/I è un campo se e solo se esistono esattamente due ideali di A che contengono I, cioè se e solo se I è massimale. □

COROLLARIO. *Ogni ideale massimale di un anello commutativo è primo.*

DIMOSTRAZIONE. Sia I un ideale massimale di A. Allora A/I è un campo, quindi un dominio. Ne segue che I è primo. □

1.7. Domini euclidei

Sia A un dominio. Diremo che A è *euclideo* se esiste un'applicazione

$$\delta\colon A \setminus \{0\} \to \mathbf{N}$$

con le seguenti proprietà:

(1) se $a, b \in A \setminus \{0\}$, allora $\delta(ab) \geq \delta(a)$;
(2) se $a, b \in A \setminus \{0\}$, allora esistono $q, r \in A$ tali che $a = bq + r$ e

$$r = 0 \qquad \text{oppure} r \neq 0 \quad \text{e} \quad \delta(r) < \delta(b).$$

La prima condizione è tecnica e serve per dimostrare il risultato seguente; la seconda condizione dice che in A è possibile eseguire una specie di "divisione con resto". Poiché non possiamo pensare ad una relazione d'ordine su A, sostituiamo alla condizione usuale (sugli interi) $0 \leq r < |b|$, la condizione con δ. Notiamo poi che la richiesta $a \in A \setminus \{0\}$ può essere sostituita da $a \in A$, poiché $0 = b0 + 0$.

L'applicazione δ si chiama *applicazione grado su* A. Un elemento $a \in A \setminus \{0\}$ si dice di *grado minimo* se $\delta(a) = \min \operatorname{im} \delta$. Osserviamo che un elemento di grado minimo esiste.

PROPOSIZIONE. *Sia A un dominio euclideo con applicazione grado δ. Allora gli elementi invertibili di A sono tutti e soli quelli di grado minimo.*

DIMOSTRAZIONE. Sia $a \in A$ di grado minimo. Allora esistono $q, r \in A$ tali che $1 = aq + r$ e

$$r = 0 \qquad \text{oppure} \qquad r \neq 0 quade \quad \delta(r) < \delta(a).$$

Poiché a ha grado minimo, non può essere $\delta(r) < \delta(a)$ e quindi deve essere $r = 0$. Perciò $1 = aq$ e a è invertibile.

Supponiamo che a sia invertibile. Se $b \in A \setminus \{0\}$, abbiamo

$$\delta(b) = \delta(1b) \geq \delta(1) = \delta(aa^{-1}) \geq \delta(a)$$

e quindi $\delta(a)$ è minimo in $\operatorname{im} \delta$. □

Diamo qualche esempio di dominio euclideo. Il primo è, ovviamente, $\mathbf{Z}$, prendendo come applicazione grado il valore assoluto.

Consideriamo ora l'*anello degli interi di Gauss*:

$$\mathbf{Z}[i] = \{\, a + bi \mid a, b \in \mathbf{Z} \,\},$$

cioè l'insieme dei numeri complessi con parte reale e parte immaginaria intere. È facile verificare che $\mathbf{Z}[i]$ è un sottoanello di $\mathbf{C}$ e che quindi è un dominio.

Definiamo $\delta\colon \mathbf{Z}[i] \to \mathbf{N}$ mediante $\delta(a + bi) = a^2 + b^2$; in altre parole $\delta(z) = z\bar{z} = |z|^2$. (L'applicazione è definita anche in 0; questo non è rilevante, basta che siano verificate le proprietà sugli elementi diversi da 0.)

La prima proprietà è banale: $\delta(xy) = |xy|^2 = |x|^2|y|^2 \geq |x|^2 = \delta(x)$.

La seconda richiede un po' di lavoro. Siano $a = a_1 + a_2 i$ e $b = b_1 + b_2 i$ interi di Gauss e supponiamo $b \neq 0$. Allora la parte reale c_1 e la parte immaginaria c_2 di ab^{-1} sono numeri razionali. Siano q_1 e q_2 due numeri interi tali che

$$|c_1 - q_1| \leq \frac{1}{2} \qquad \text{e} \qquad |c_2 - q_2| \leq \frac{1}{2}$$

e scriviamo $p_1 = c_1 - q_1$, $p_2 = c_2 - q_2$. Poniamo $q = q_1 + q_2 i$ e $r = a - bq$; allora $a = bq + r$ e ci basta verificare che $\delta(r) < \delta(b)$. Possiamo eseguire i calcoli seguenti in $\mathbf{C}$:

$$a = b(ab^{-1}) = b(c_1 + c_2 i) = b((q_1 + p_1) + (q_2 + p_2)i) = b((q_1 + q_2 i) + (p_1 + p_2 i)) = bq + b(p_1 + p_2 i).$$

Dunque $r = a - bq = b(p_1 + p_2 i)$. Usiamo ora il fatto che possiamo definire δ su *tutto* l'insieme $\mathbf{C}$ dei complessi e che vale ancora che $\delta(xy) = \delta(x)\delta(y)$. Perciò:

$$\delta(r) = \delta(b)\delta(p_1 + p_2 i) = \delta(b) \cdot (p_1^2 + p_2^2) \leq \delta(b) \left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}\delta(b) < \delta(b),$$

dal momento che $\delta(b) > 0$.

I domini euclidei sono importanti perché in essi valgono proprietà simili a quelle dei numeri interi, per quanto riguarda la fattorizzazione.

TEOREMA. *Sia A un dominio euclideo. Allora ogni ideale di A è principale.*

DIMOSTRAZIONE. Sia I un ideale di A. Se $I = \{0\}$, allora $I = 0A$ è principale. Supponiamo allora $I \neq \{0\}$ e denomo con δ un'applicazione grado su A. L'insieme

$$\delta^{\rightarrow}(I \setminus \{0\}) \subseteq \mathbf{N}$$

non è vuoto (perché $I \setminus \{0\} \neq \emptyset$). Di conseguenza ha minimo m ed esiste $b \in I \setminus \{0\}$ tale che $\delta(b) = m$.

Poiché $b \in I$, è necessariamente $bA \subseteq I$ (esercizio). Viceversa, sia $a \in I$. Allora esistono $q, r \in A$ tali che $a = bq + r$, con $r = 0$ oppure $r \neq 0$ e $\delta(r) < \delta(b)$. Ora, da $a, b \in I$, segue che $r = a - bq \in I$. Perciò la possibilità $r \neq 0$ non può verificarsi. Si otterrebbe infatti $r \in I \setminus \{0\}$ e $\delta(r) < \delta(b) = m$, contro il fatto che m è il minimo di $\delta^{\rightarrow}(I \setminus \{0\})$.

In definitiva $r = 0$ e $a = bq \in bA$, cioè $I \subseteq bA$. □

DEFINIZIONE. Sia A un anello commutativo e siano $a, b \in A$. Diciamo che a *divide* b se esiste $c \in A$ tale che $b = ac$.

Diciamo che a e b sono *associati* se esiste $u \in A$ invertibile tale che $a = ub$.

Diremo che $d \in A$ è *un massimo comun divisore* di a e b se

(1) d divide a e d divide b;
(2) se $c \in A$, c divide a e c divide b, allora c divide d.

È facile verificare che la relazione $a \sim b$ definita da a e b sono associati è una relazione di equivalenza.

ESERCIZIO. Se A è un dominio e $a, b \in A$, allora:

(a) a e b sono associati se e solo se $aA = bA$;
(b) a divide b se e solo se $aA \supseteq bA$.

PROPOSIZIONE. *Sia A un dominio e siano $a, b \in A$. Se d e d' sono massimi comuni divisori di a e b, allora d e d' sono associati.*

DIMOSTRAZIONE. Come nel caso degli interi, abbiamo che d divide d' e che d' divide d; perciò $d = d'\alpha$ e $d' = d\beta$, da cui $d = d\alpha\beta$ e $d(1 - \alpha\beta) = 0$. Perciò, dal momento che siamo in un dominio, $d = 0$ oppure $\alpha\beta = 1$. Nel primo caso $d' = 0\beta = 0$, ma è anche $0 = 01$. Nel secondo caso α è invertibile. □

Non è detto che in un dominio esista un massimo comun divisore di due elementi.

PROPOSIZIONE. *Sia A un dominio euclideo e siano $a, b \in A$. Allora esistono α e β in A tali che $d = a\alpha + b\beta$ sia un massimo comun divisore di a e b.*

DIMOSTRAZIONE. Sia $I = aA + bA$; allora I è un ideale di A e perciò è principale, cioè $I = dA$, per un opportuno $d \in A$. Poiché $a = a1 + b0 \in I = dA$, esiste $a' \in A$ tale che $a = da'$. Quindi d divide a e, analogamente d divide b. Inoltre esistono $\alpha, \beta \in A$ tali che $d = a\alpha + b\beta$.

Sia $c \in A$ tale che c divide a e b. Allora $a = ca''$ e $b = cb''$ e quindi

$$d = a\alpha + b\beta = ca''\alpha + cb''\beta = c(a''\alpha + b''\beta)$$

cioè c divide d. □

Stiamo in effetti ripetendo, in ordine leggermente diverso, i vari passi che hanno permesso la dimostrazione della unicità ed esistenza della fattorizzazione di un numero naturale come prodotto di primi.

ESERCIZIO. Si verifichi che, se A è un dominio e d è un massimo comun divisore di a e b, allora $d' \in A$ è anch'esso un massimo comun divisore di a e b se e solo se d e d' sono associati.

Per tutto il resto della sezione lavoreremo in un dominio A.

DEFINIZIONE. Un elemento $a \in A$ si dice *irriducibile* se non è 0 e non è invertibile e, dal fatto che $a = bc$, con $b, c \in A$, segue che uno fra b e c è invertibile.

Un elemento $a \in A$ si dice *primo* se non è 0 e non è invertibile e, dal fatto che a divide bc, con $b, c \in A$, segue che a divide uno fra b e c.

ESERCIZIO. Sia A un anello commutativo e siano $a, b \in A$ associati. Allora:

(a) a è irriducibile se e solo se b è irriducibile;
(b) a è primo se e solo se b è primo.

PROPOSIZIONE. *Ogni elemento primo in un dominio è irriducibile.*

DIMOSTRAZIONE. Sia a un elemento primo e supponiamo che $a = bc$. Allora a divide bc e quindi divide b oppure c. Da $b = aa'$ segue $a = bc = aa'c$ e quindi, essendo $a \neq 0$, $1 = a'c$ e c è invertibile. □

PROPOSIZIONE. *Sia A un dominio euclideo. Allora ogni elemento irriducibile di A è primo.*

DIMOSTRAZIONE. Supponiamo che a sia irriducibile e che divida bc. Se a non divide b, allora un massimo comun divisore di a e b è necessariamente invertibile: infatti un massimo comun divisore esiste, sia d. Ma allora d divide a e, per l'irriducibilità di a, d è invertibile o è associato ad a. Non può essere associato ad a, in quanto altrimenti a dividerebbe b (esercizio). Perciò d è invertibile.

Per il teorema, esistono α e β tali che $d = a\alpha + b\beta$; allora

$$c = c1 = cd^{-1}d = cd^{-1}(a\alpha + b\beta) = a(cd^{-1}\alpha) + (bc)(d^{-1}\beta)$$

e quindi a divide c. □

Una volta dimostrato questo teorema possiamo usare la stessa tecnica impiegata negli interi per dimostrare il teorema di fattorizzazione.

TEOREMA. *Sia A un dominio euclideo e sia $a \in A$, $a \neq 0$ e a non invertibile. Allora esistono elementi primi $p_1, p_2, \ldots, p_n \in A$ tali che*

$$a = p_1 p_2 \ldots p_n.$$

Inoltre, se $a = q_1 q_2 \ldots q_m$ è un'altra decomposizione di a come prodotto di elementi primi, è $m = n$ ed esiste una permutazione $\sigma \in S_n$ tale che, per ogni $i = 1, 2, \ldots, n$, p_i è associato a $q_{\sigma(i)}$.

DIMOSTRAZIONE. La dimostrazione della "unicità" si fa come per i naturali, con le opportune modifiche (esercizio).

Veniamo all'esistenza di questa decomposizione. Sia $a \neq 0$, a non invertibile e supponiamo, per assurdo, che a non sia prodotto di elementi primi.

In particolare a non è primo e quindi $a = a_1 b_1$, con a_1 e b_1 non invertibili. Se a_1 e b_1 fossero prodotto di primi, anche a lo sarebbe. Perciò uno di essi, diciamo a_1, non è prodotto di primi. Perciò $a_1 = a_2 b_2$, con a_2 e b_2 non invertibili. Possiamo allora costruire, per induzione, una successione a_n tale che (1) $a = a_0$, (2) a_{n+1} divida a_n e (3) a_{n+1} non sia associato a a_n. Ciò significa che $a_n A \subset a_{n+1} A$.

Consideriamo ora $I = \bigcup_n a_n A$; allora I è un ideale di A e quindi è principale. Sia dunque $I = bA$; allora $b \in I$ ed esiste n tale che $b \in a_n A$. Ma allora

$$bA \subseteq a_n A \subset a_{n+1} A \subset \cdots \subseteq I = bA$$

e ne segue che $a_n A = a_{n+1} A$: assurdo. □

Vedremo più avanti un'applicazione di questo teorema agli anelli di polinomi.

PROPOSIZIONE. *Sia I un ideale primo di un dominio euclideo A, $I \neq \{0\}$. Allora I è massimale.*

DIMOSTRAZIONE. Sappiamo che $I = aA$, per un opportuno $a \in A$, $a \neq 0$; non è difficile dimostrare che allora a è primo (esercizio) e quindi irriducibile. Sia J un ideale proprio di A tale che $I \subseteq J$; allora $J = bA$ e b non è invertibile, altrimenti $J = A$. Essendo $a \in I \subseteq J$, esiste $c \in A$ tale che $a = bc$. Ne segue che c è invertibile e quindi $b = ac^{-1} \in I$. Ma allora $J = bA \subseteq I$ e dunque $I = J$. □

Si potrebbe pensare che tutti i domini siano euclidei. Questo non è vero, come mostra il seguente esempio.

Esempio di un dominio non euclideo. Consideriamo $A = \mathbf{Z}[i\sqrt{5}] = \{\, a + bi\sqrt{5} \mid a, b \in \mathbf{Z} \,\}$. Come per gli interi di Gauss, è facile vedere che A è un sottoanello di $\mathbf{C}$, quindi un dominio. Se A fosse, rispetto a qualche applicazione grado, un dominio euclideo, varrebbe il teorema di fattorizzazione.

Consideriamo $9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$. Faremo vedere che 3, $(2 + i\sqrt{5})$ e $(2 - i\sqrt{5})$ sono elementi irriducibili e che 3 non è associato a $(2 + i\sqrt{5})$. In tal modo avremo provato che il teorema di fattorizzazione non vale e che quindi A non è un dominio euclideo.

Definiamo $\nu(a + bi\sqrt{5}) = a^2 + 5b^2$; in altre parole, abbiamo $\nu(x) = |x|^2$ e $\nu(xy) = \nu(x)\nu(y)$.

Supponiamo $3 = xy$, con $x, y \in A$. Allora $\nu(3) = 9 = \nu(x)\nu(y)$ e quindi i casi possibili sono (1) $\nu(x) = 9$ e $\nu(y) = 1$; (2) $\nu(x) = \nu(y) = 3$; (3) $\nu(x) = 1$ e $\nu(y) = 9$.

Sia $x = a + bi\sqrt{5}$. Se $\nu(x) = 1$, allora $1 = a^2 + 5b^2$ e, necessariamente, $a = \pm 1$ e $b = 0$. Ma allora un tale x è invertibile. Perciò, i casi (1) e (3) danno che uno fra x e y è invertibile. Facciamo allora vedere che il caso (2) non può accadere. Infatti $a^2 + 5b^2 = 3$ (con a e b *interi*) è una relazione impossibile, perché essa implica $b \neq 0$, e quindi $a^2 + 5b^2 \geq 5 > 3$.

Abbiamo dunque che 3 è irriducibile.

Supponiamo $2 + i\sqrt{5} = xy$, con $x, y \in A$. Allora $\nu(2 + i\sqrt{5}) = 9 = \nu(x)\nu(y)$ e quindi i casi possibili sono nuovamente (1) $\nu(x) = 9$ e $\nu(y) = 1$; (2) $\nu(x) = \nu(y) = 3$; (3) $\nu(x) = 1$ e $\nu(y) = 9$. Come prima, abbiamo che $2 + i\sqrt{5}$ è irriducibile. Analogamente, $2 - i\sqrt{5}$ è irriducibile.

Per verificare che 3 e $2 + i\sqrt{5}$ non sono associati, dobbiamo calcolare gli elementi invertibili di A. Sia $x \in A$ invertibile. Allora $1 = \nu(1) = \nu(xx^{-1}) = \nu(x)\nu(x^{-1})$ e quindi $\nu(x) = 1$, cioè $x = 1$ oppure $x = -1$. I due elementi dati, 3 e $2 + i\sqrt{5}$ non sono allora associati.

Elementi primi negli interi di Gauss. L'anello $\mathbf{Z}[i]$ degli interi di Gauss è un dominio euclideo. Vogliamo stabilire quali sono gli elementi primi. L'applicazione grado su $\mathbf{Z}[i]$ è $\delta\colon z \mapsto |z|^2$; gli elementi invertibili sono quelli di grado minimo e quindi sono quelli per i quali $\delta(z) = 1$ (poiché $\delta(1) = 1$). Di conseguenza gli elementi invertibili sono 1, -1, i e $-i$.

Chiameremo *numeri primi* i soliti numeri primi in $\mathbf{N}$.

PROPOSIZIONE. *Sia $z \in \mathbf{Z}[i]$; se $\delta(z)$ è un numero primo, allora z è irriducibile.*

DIMOSTRAZIONE. Supponiamo $z = xy$; allora $\delta(z) = \delta(x)\delta(y)$ e quindi $\delta(x) = 1$ oppure $\delta(y) = 1$. □

Quali sono gli interi di Gauss z tali che $\delta(z)$ sia un numero primo? Ad esempio $1 + i$ e $1 - i$. Più in generale, se p è un numero primo che è somma di due quadrati di interi, $p = a^2 + b^2$, allora $a + bi$ è un elemento primo in $\mathbf{Z}[i]$.

Quindi, siccome $5 = 1^2 + 2^2$, gli elementi

$$1 + 2i, 1 - 2i, -1 + 2i, -1 - 2i, 2 + i, 2 - i, -2 + i, -2 - i$$

sono tutti primi in $\mathbf{Z}[i]$ (trovare quali fra questi sono associati). In effetti, considerando gli elementi a meno di associati, abbiamo trovato due elementi primi.

Viceversa, 7 non si può scrivere come somma di due quadrati; perciò $7 = 7 + 0i$ è primo in $\mathbf{Z}[i]$.

Quali sono i numeri primi che sono somma di due quadrati? Di sicuro $2 = 1 + 1$ lo è. Sia p un numero primo dispari che è somma di due quadrati: $p = a^2 + b^2$; non è restrittivo supporre che $a = 2c$ sia pari e che $b = 2d + 1$ sia dispari. Allora

$$p = a^2 + b^2 = 4c^2 + 4d^2 + 4d + 1 \equiv 1 \pmod 4.$$

Eulero dimostrò anche il viceversa: *un numero primo dispari p è somma di due quadrati se e solo se* $p \equiv 1 \pmod 4$. Ne segue che un numero primo dispari p tale che $p \equiv 3 \pmod 4$ è irriducibile anche come elemento di $\mathbf{Z}[i]$.

Usando questi risultati, Lagrange riuscì a dimostrare che *ogni numero naturale è somma di quattro quadrati di interi.*

1.8. Anelli di matrici

Sia A un anello (anche non commutativo); possiamo considerare l'insieme $M_n(A)$ delle *matrici quadrate di ordine n a coefficienti in A*, esattamente come si fa per le matrici a coefficienti complessi. Se si riguardano le dimostrazioni fatte per provare che le matrici a coefficienti comnplessi sono un anello, ci si accorge che le proprietà che si usano sono solo quelle che dicono che $\mathbf{C}$ è un anello. Perciò, se definiamo la somma di matrici e il prodotto righe per colonne in modo formalmente identico a quello usato allora, otteniamo che $M_n(A)$ è un anello.

Se X è un sottoinsieme di A, indichiamo con $M_n(X)$ l'insieme delle matrici di ordine n i cui coefficienti stanno in X.

PROPOSIZIONE. *Se A è un anello e I è un ideale di A, allora $M_n(I)$ è un ideale di $M_n(A)$. Viceversa, se J è un ideale di $M_n(A)$, allora esiste uno ed un solo ideale I di A tale che $J = M_n(I)$.*

DIMOSTRAZIONE. La prima affermazione è una facile conseguenza della definizione delle operazioni su $M_n(A)$ e del fatto che I è un ideale (esercizio).

Sia J un ideale di $M_n(A)$. Consideriamo I, l'insieme dei coefficienti di tutte le matrici appartenenti a J: in altre parole $a \in I$ se e solo se esiste $x \in J$ tale che a sia uno dei coefficienti di x. È chiaro allora che $J \subseteq M_n(I)$.

Dimostriamo che I è un ideale. Se $a \in I$, sia x una matrice in J in cui a sia un coefficiente, diciamo di posto (i, j). Allora, indicando con e_{ij} la matrice che si ottiene dall'identità scambiando la i-esima riga con la j-esima, la matrice $e_{1i}x$ ha il coefficiente a al posto $(1, j)$ e quindi la matrice $e_{1i}xe_{1j}$ ha il coefficiente a al posto $(1, 1)$. Poiché J è un ideale di $M_n(A)$ e $x \in J$, anche $e_{1i}xe_{1j} \in J$.

Quindi I è anche l'insieme dei coefficienti di posto $(1, 1)$ delle matrici in J. Il fatto che I sia un ideale è ora un facile calcolo: se $a, b \in I$, $x \in J$ ha a al posto $(1, 1)$ e $y \in J$ ha b al posto $(1, 1)$, allora $x - y$ ha $a - b$ al posto $(1, 1)$, quindi $a - b \in I$. Se poi $c \in A$, allora $x\tilde{c} \in J$ e $\tilde{c}x \in J$ hanno ac e ca, rispettivamente, al posto $(1, 1)$, dove $\tilde{c}$ è la matrice che ha c al posto $(1, 1)$ e 0 altrove. Il fatto che I non sia vuoto è ovvio.

La matrice $\tilde{1}$ ha un altro uso: sia $x \in M_n(A)$; allora $\hat{x} = \tilde{1}x\tilde{1}$ ha tutti i coefficienti uguali a zero, tranne al più quello di posto $(1, 1)$, in cui c'è lo stesso coefficiente di posto $(1, 1)$ di x. Notiamo che, se $x \in J$, anche $\hat{x} \in J$.

Dimostriamo, per finire, che $J = M_n(I)$. Sia $z = (a_{ij}) \in M_n(I)$ e, per ogni i e j, fissiamo una matrice $x_{ij} \in J$ tale che a_{ij} sia il coefficiente di posto $(1, 1)$ di x_{ij}. Per quanto visto sopra, possiamo anche supporre che tutti gli altri coefficienti di x_{ij} siano 0 (eventualmente sostituendo x_{ij} con $\widehat{x_{ij}}$. Allora la matrice

$$y_{ij} = e_{1i}x_{ij}e_{1j}$$

ha a_{ij} al posto (i, j) e zero altrove e $y_{ij} \in J$. Se sommiamo fra loro tutte queste matrici otteniamo proprio z, quindi $z \in J$. □

Si può anche dimostrare che, se A è un anello commutativo, vale anche la teoria dei determinanti, con una piccola differenza.

PROPOSIZIONE. *Sia A un anello commutativo. Allora $x \in M_n(A)$ è invertibile se e solo se* $\det x$ *è invertibile in A.*

Ad esempio, per $A = \mathbf{Z}/6\mathbf{Z}$, la matrice

$$x = \begin{bmatrix} 1 & 5 \\ 1 & 4 \end{bmatrix} \in M_2(\mathbf{Z}/6\mathbf{Z})$$

è invertibile, poiché $\det x = 1 \cdot 4 - 1 \cdot 5 = 5 = 5^{-1}$ (infatti $5 \cdot 5 = 25 = 1$).

COROLLARIO. *Se A è un campo, allora gli unici ideali di $M_n(A)$ sono $\{0\}$ e $M_n(A)$.*

Notiamo che, per $n > 1$, $M_n(A)$ non è commutativo e che esistono elementi $x, y \in M_n(A)$ non nulli tali che $xy = 0$.

Se A è commutativo, l'insieme degli elementi invertibili di $M_n(A)$ (rispetto alla moltiplicazione!) si denota con $GL(n, A)$; esso è un gruppo e l'applicazione

$$\det\colon GL(n, A) \to GL(1, A)$$

che manda x in $\det x$ è un omomorfismo di gruppi; $GL(1, A)$ è l'insieme degli elementi invertibili di A.

1.9. Anelli finiti

Sia p un numero primo; allora $p\mathbf{Z}$ è un ideale primo di $\mathbf{Z}$ e quindi $\mathbf{Z}/p\mathbf{Z}$ è un campo, poiché $\mathbf{Z}$ è un dominio euclideo. Esiste anche una dimostrazione diretta di questo fatto, basata solo sul fatto che $\mathbf{Z}/p\mathbf{Z}$ è un dominio.

PROPOSIZIONE. *Sia A un dominio finito. Allora A è un campo.*

DIMOSTRAZIONE. Sia $a \in A$, $a \neq 0$; allora l'applicazione $f\colon A \to A$ definita da $f(x) = ax$ è iniettiva, quindi suriettiva. Perciò esiste $b \in A$ tale che $f(b) = 1$, cioè $ab = 1$. □

Prendiamo un anello finito A; allora $U(A)$, insieme degli elementi invertibili di A è un gruppo finito. Ne segue che, se $a \in U(A)$, allora $a^{|U(A)|} = 1$.

Un caso particolare è quello di $A = \mathbf{Z}/n\mathbf{Z}$, con $n > 0$. Chi sono gli elementi invertibili? Per evitare complicazioni, usiamo la notazione delle classi di equivalenza.

PROPOSIZIONE. *Sia $0 < m < n$; allora $[m]$ è invertibile in $\mathbf{Z}/n\mathbf{Z}$ se e solo se* $\mathrm{mcd}(m, n) = 1$.

DIMOSTRAZIONE. Supponiamo $[m]$ invertibile. Allora $[m][\alpha] = [1]$, per un opportuno $\alpha \in \mathbf{Z}$, cioè esiste $\beta \in \mathbf{Z}$ tale che $m\alpha + n\beta = 1$. Ne segue che $1 \in m\mathbf{Z} + n\mathbf{Z}$ e quindi $\mathrm{mcd}(m, n) = 1$.

Viceversa, se $\mathrm{mcd}(m, n) = 1$, esistono $\alpha, \beta \in \mathbf{Z}$ tali che $m\alpha + n\beta = 1$; questo è come dire che $[m][\alpha] = [1]$. □

In particolare $|U(\mathbf{Z}/n\mathbf{Z})| = \varphi(n)$ (funzione di Eulero). Il seguente risultato è dovuto proprio a Eulero.

TEOREMA. *Sia $a \in \mathbf{Z}$ e sia* $\mathrm{mcd}(a, n) = 1$. *Allora*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

DIMOSTRAZIONE. Poiché $[a] \in U(\mathbf{Z}/n\mathbf{Z})$, si ha $[a]^{|U(\mathbf{Z}/n\mathbf{Z})|} = [1]$, cioè $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Il teorema da cui Eulero prese le mosse è chiamato *piccolo teorema di Fermat*[‡] ed è ora un corollario.

COROLLARIO. *Siano $a, p \in \mathbf{Z}$, con $p > 0$ primo. Allora*

$$a^p \equiv a \pmod{p}.$$

DIMOSTRAZIONE. Per il teorema di Eulero, $a^{\varphi(p)} \equiv 1$, cioè $a^{p-1} \equiv 1$, quando a non è divisibile per p. Poiché $a \equiv a$, ne segue che $a^p \equiv a$. Se a è divisibile per p, anche a^p lo è e perciò $a^p \equiv 0 \equiv a$. □

Un altro risultato importante è chiamato *teorema cinese dei resti*, perché sembra fosse noto ai cinesi fin dal XIV secolo. Lo dimostreremo solo in un caso particolare.

Se A e B sono anelli, possiamo considerare l'insieme $A \times B$ delle coppie di elementi presi negli insiemi A e B rispettivamente. L'insieme $A \times B$ diventa un anello con le operazioni

$$(a, b) + (a', b') = (a + a', b + b'), \qquad (a, b)(a', b') = (aa', bb').$$

Le applicazioni $\pi_A \colon A \times B \to A$ e $\pi_B \colon A \times B \to B$ definite da

$$\pi_A \colon (a, b) \mapsto a, \qquad \pi_B \colon (a, b) \mapsto b,$$

sono omomorfismi di anelli.

Siano m ed n interi positivi; allora possiamo considerare l'anello $A = \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ e l'omomorfismo $\chi_A \colon \mathbf{Z} \to A$. È facile vedere che $\chi_A(x) = ([x], [x])$. Ci domandiamo qual è il nucleo di χ_A. Un intero x sta in $\ker \chi_A$ se e solo se $\chi_A(x) = ([x], [x]) = ([0], [0])$, cioè se e solo se

$$\begin{cases} x \equiv 0 \pmod{m} \\ x \equiv 0 \pmod{n} \end{cases}$$

cioè x è soluzione di un sistema di congruenze.

Più in generale, ci domandiamo quando, assegnati m ed n interi positivi distinti e $a, b \in \mathbf{Z}$, il sistema $S(a, b)$ di congruenze

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

abbia soluzione.

TEOREMA. *Siano m ed n interi positivi distinti. Il sistema di congruenze $S(a, b)$ ha soluzione per ogni scelta di $a, b \in \mathbf{Z}$ se e solo se* $\mathrm{mcd}(m, n) = 1$.

[‡]Pierre de Fermat fu uno dei massimi matematici della storia; insieme a Pascal pose le basi del calcolo delle probabilità e fu un precursore di Newton e Leibniz in Analisi. Di professione era giudice e si occupava di matematica nel tempo libero. Va famoso per la sua congettura, nota come *grande teorema di Fermat*: se $n > 2$, non esistono interi positivi a, b, c tali che $a^n + b^n = c^n$. La congettura è stata finalmente dimostrata dopo più di tre secoli di tentativi, ad opera di A. Wiles.

DIMOSTRAZIONE. Manteniamo le notazioni introdotte in precedenza. Dato $x \in \mathbf{Z}$, abbiamo che $x \in \ker \chi_A$ se e solo se $x \equiv 0 \pmod{m}$ e $x \equiv 0 \pmod{n}$, cioè se e solo se $x \in m\mathbf{Z} \cap n\mathbf{Z} = l\mathbf{Z}$, dove $l = \operatorname{mcm}(m, n)$.

Dire che ogni sistema di congruenze ha soluzione equivale a dire che χ_A è suriettivo. In tal caso $\widetilde{\chi_A} \colon \mathbf{Z}/l\mathbf{Z} \to A$ è un isomorfismo e, in particolare $|\mathbf{Z}/l\mathbf{Z}| = |A| = mn$. Ne segue che $l\mathbf{Z} = mn\mathbf{Z}$, cioè che $\operatorname{mcm}(m, n) = mn$ e quindi $\operatorname{mcd}(m, n) = 1$.

Viceversa, se $\operatorname{mcd}(m, n) = 1$, allora $l = \operatorname{mcm}(m, n) = mn$ e quindi $\ker \chi_A = mn\mathbf{Z}$. Ora l'omomorfismo $\widetilde{\chi_A} \colon \mathbf{Z}/mn\mathbf{Z} \to A$ è iniettivo e $|\mathbf{Z}/mn\mathbf{Z}| = mn = |A|$. Quindi $\widetilde{\chi_A}$ è suriettivo e perciò χ_A è suriettivo. □

1.10. Il gruppo moltiplicativo di un campo

Se F un campo, l'insieme degli elementi non nulli un gruppo rispetto alla moltiplicazione. Lo indicheremo con $F^\times$.

Un primo esempio di come si possa studiare questo gruppo il caso del campo dei numeri complessi. Si ricorder certamente che ogni numero complesso non nullo si pu scrivere in modo unico come prodotto di un numero reale positivo e di un numero complesso di modulo 1: la scrittura in *forma trigonometrica*. Si prenda infatti $z = a + bi \neq 0$; allora, ponendo $a_1 = a/|z|$ e $b_1 = b/|z|$, sappiamo che

$$a_1^2 + b_1^2 = 1$$

e quindi che esiste un unico numero reale φ tale che

$$a_1 = \cos\varphi, \quad b_1 = \operatorname{sen}\varphi, \qquad 0 \leq \varphi < 2\pi.$$

L'insieme $\mathbf{U}$ dei numeri complessi di modulo 1 un sottogruppo di $\mathbf{C}^\times$. Anche l'insieme $\mathbf{R}_{>0}$ dei numeri reali positivi un sottogruppo di $\mathbf{R}^\times$. Le regole di moltiplicazione dei numeri complessi in forma trigonometrica dicono allora che l'applicazione

$$\mathbf{R}_{>0} \times \mathbf{U} \to \mathbf{C}^\times, \qquad (r, \zeta) \mapsto r\zeta$$

un isomorfismo di gruppi.

Nel caso in cui il campo sia $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$, la struttura del gruppo moltiplicativo molto pi semplice. Proviamo nel caso $p = 11$ e consideriamo l'elemento $[2]$: si ha

$$[2]^2 = [4], [2]^3 = [8], [2]^4 = [5], [2]^5 = [10], [2]^6 = [9], [2]^7 = [7], [2]^8 = [3], [2]^9 = [6], [2]^{10} = [1].$$

Ci significa che l'elemento $[2] \in \mathbf{F}_{11}^\times$ ha ordine 10, quindi che il gruppo $\mathbf{F}_{11}^\times$ ciclico.

Dimostreremo ora che non un caso: il gruppo moltiplicativo di ogni campo finito ciclico. Non per vero che ogni gruppo ciclico sia il gruppo moltiplicativo di un campo. Si provi a verificare che nessun campo finito pu avere come gruppo moltiplicativo un gruppo ciclico di ordine 5. (Suggerimento: non esiste alcun campo con sei elementi.) A dire il vero potremo dimostrare di pi.

Enunciamo prima una propriet della funzione φ di Eulero: se $n > 0$, allora

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

Basta dimostrare la prima uguaglianza; la seconda ovvia essendo solo un riordinamento degli addendi.

Sull'insieme $X = \{0, 1, \ldots, n-1\}$ definiamo la relazione di equivalenza $\sim$ ponendo $a \sim b$ quando $\operatorname{mcd}(a, n) = \operatorname{mcd}(b, n)$. Se $d \mid n$, il numero di elementi in $[d]_\sim$ $\varphi(n/d)$. Infatti $\operatorname{mcd}(k, n) = d$ se e solo se $\operatorname{mcd}(k/d, n/d) = 1$. Basta allora sommare il numero di elementi delle classi di equivalenza che deve dare il numero di elementi di X, cio n.

TEOREMA. *Sia A un campo e sia H un sottogruppo finito del gruppo moltiplicativo di A. Allora H ciclico.*

DIMOSTRAZIONE. Ricordiamo che se G un gruppo ciclico con n elementi, allora il numero di elementi di G che sono generatori di G (cio gli elementi $g \in G$ tali che $\langle g \rangle = G$) $\varphi(n)$, dove φ indica la funzione φ di Eulero.

Se $|H| = n$, sappiamo che, per ogni $h \in H$, $h^n = 1$.

Diremo che un elemento $h \in H$ una radice primitiva d-esima di 1 in H se

(1) $H_d = \{\, h \in H \mid h^d = 1 \,\}$ un sottogruppo ciclico di H;
(2) $\langle h \rangle = H_d$.

(Si verifichi che H_d un sottogruppo di H). In particolare, se h una radice primitiva d-esima di 1 in H, allora l'ordine di h d e quindi $d \mid n$.

Per $d \mid n$, definiamo $\psi(d)$ come il numero di radici primitive d-esime di 1 in H. Avremo allora che $\psi(d) = 0$, se H_d non ciclico; altrimenti H_d ciclico e quindi $\psi(d) = \varphi(d)$.

Ora, ogni elemento $h \in H$ ha ordine finito e quindi genera un gruppo ciclico; quindi ogni elemento radice primitiva d-esima di 1 in H per un $d \mid n$. Di conseguenza

$$n = \sum_{d|n} \psi(d)$$

e perci

$$0 = \sum_{d|n} \varphi(d) - \sum_{d|n} \psi(d) = \sum_{d|n} (\varphi(d) - \psi(d)).$$

Ogni addendo nell'ultima somma non negativo; ma allora ogni addendo zero e, in particolare, $\psi(n) = \varphi(n) > 0$. Quindi, per definizione, H_n ciclico. Ma $H_n = H$. □

CAPITOLO 2

Polinomi

I polinomi compaiono già nella scuola media; tuttavia il modo in cui sono presentati è spesso lacunoso. Cercheremo in questo capitolo di fondare la teoria dei polinomi su basi più solide.

2.1. Generalità

In tutto questo capitolo useremo solo anelli commutativi.

Sia A un anello (commutativo); indichiamo con $A^{\mathbf{N}}$ l'insieme di tutte le *successioni* a valori in A, cioè le applicazioni $\mathbf{N} \to A$. Se $f\colon \mathbf{N} \to A$ è una successione, essa verrà indicata come

$$(f(0), f(1), \dots, f(n), \dots).$$

In generale, parleremo della successione

$$(a_0, a_1, \dots, a_n, \dots),$$

dove $a_i \in A$, $i \in \mathbf{N}$.

Definizione. Un *polinomio a coefficienti in A* è una successione

$$(a_0, a_1, \dots, a_n, \dots) \in A^{\mathbf{N}}$$

per la quale esiste $\bar{n} \in \mathbf{N}$ in modo che $a_n = 0$, per ogni $n > \bar{n}$. Indicheremo con $A[X]$ l'insieme dei polinomi a coefficienti in A.

Questa definizione può sembrare strana, a prima vista. In realtà stiamo identificando un polinomio (si pensi ai soliti polinomi) con la successione dei coefficienti delle potenze di X, cominciando dall'esponente 0.

Poiché un polinomio è un'applicazione $\mathbf{N} \to A$, due polinomi sono uguali se e solo se lo sono in quanto applicazioni:

$$(a_0, a_1, \dots, a_n, \dots) = (b_0, b_1, \dots, b_n, \dots) \quad \text{se e solo se} \quad a_i = b_i, i \in \mathbf{N}.$$

Vogliamo ora definire due operazioni in $A[X]$, in modo che diventi un anello. Definiamo la somma:

$$(a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = (c_0, c_1, \dots, c_n, \dots)$$

dove

$$c_i = a_i + b_i, \quad i \in \mathbf{N}.$$

Più in breve, scriveremo

$$(a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots).$$

È immediato verificare che questa operazione di addizione è ben definita, cioè che la successione $(c_0, c_1, \dots, c_n, \dots) \in A[X]$. Inoltre è facile verificare che $A[X], +$ è un gruppo. L'elemento neutro per questa operazione è $(0, 0, \dots, 0, \dots)$ e l'opposto di $(a_0, a_1, \dots, a_n, \dots)$ è la successione

$$-(a_0, a_1, \dots, a_n, \dots) = (-a_0, -a_1, \dots, -a_n, \dots).$$

La moltiplicazione richiede una definizione e verifiche più complicate. Definiamo

$$(a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = (c_0, c_1, \dots, c_n, \dots)$$

dove, per $i \in \mathbf{N}$,

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Dimostriamo che la successione così definita è ancora in $A[X]$. Sappiamo che $a_n = 0$, per $n > \bar{n}$ e che $b_m = 0$ per $m > \bar{m}$. Calcoliamo c_i, per $i > \bar{n} + \bar{m}$:

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=0}^{\bar{n}} a_j b_{i-j} + \sum_{j=\bar{n}+1}^{i} a_j b_{i-j}.$$

Ora, se $i > \bar{n} + \bar{m}$ e $0 \leq j \leq \bar{n}$, abbiamo che $i - j > \bar{m}$; perciò tutti i termini nella prima somma hanno $b_{i-j} = 0$. Quindi la prima somma è zero. Nella seconda somma, dove $j > \bar{n}$, vale $a_j = 0$ e quindi anche la seconda somma è zero.

In definitiva, $c_i = 0$, per $i > \bar{n} + \bar{m}$, e la successione sta in $A[X]$. Si tratta ora di dimostrare che:

(1) la moltiplicazione è associativa;
(2) esiste un elemento neutro;
(3) la moltiplicazione è distributiva rispetto all'addizione;
(4) la moltiplicazione è commutativa.

Adottiamo una notazione più breve per le successioni: $(a_n)_{n\in\mathbf{N}}$ o anche (a_n) stanno per la successione $(a_0, a_1, \dots, a_n, \dots)$.

Dimostriamo che la moltiplicazione è associativa; siano (a_n), (b_n) e (c_n) polinomi. Poniamo $(a_n)(b_n) = (d_n)$, $(d_n)(c_n) = (e_n)$, $(b_n)(c_n) = (f_n)$ e $(a_n)(f_n) = (g_n)$. Dobbiamo allora verificare che $(e_n) = (g_n)$:

$$e_n = \sum_{j=0}^{n} d_j c_{n-j} = \sum_{j=0}^{n} \Big(\sum_{k=0}^{j} a_k b_{j-k} \Big) c_{n-j};$$

il termine a_0 compare n volte, il termine a_1 compare $n-1$ volte, e così via, fino ad a_n, che compare una volta. Se raccogliamo a_0, a_1, …, a_n, otteniamo:

$$\begin{aligned} e_n &= a_0 \Big(\sum_{j=0}^{n} b_j c_{n-j} \Big) + a_1 \Big(\sum_{j=0}^{n-1} b_j c_{n-1-j} \Big) + \cdots + a_{n-1} \Big(\sum_{j=0}^{1} b_j c_{1-j} \Big) + a_n \Big(\sum_{j=0}^{0} b_j c_{0-j} \Big) \\ &= \sum_{k=0}^{n} a_k \Big(\sum_{j=0}^{k} b_j c_{k-j} \Big) = g_n. \end{aligned}$$

Dimostriamo che la moltiplicazione è commutativa (per passare dalla prima formula alla seconda, sostituiamo j con $k = n - j$):

$$\sum_{j=0}^{n} a_j b_{n-j} = \sum_{k=0}^{n} a_{n-k} b_k = \sum_{k=0}^{n} b_k a_{n-k},$$

poiché la moltiplicazione in A è commutativa.

L'elemento neutro di $A[X], \cdot$ è $(1, 0, 0, \dots)$. La proprietà distributiva è lasciata per esercizio.

Dunque $A[X]$ è un anello commutativo. Esiste anche un omomorfismo iniettivo $\varphi\colon A \to A[X]$, definito da

$$\varphi(a) = \widetilde{a} = (a, 0, 0, \dots).$$

La verifica che si tratta di un omomorfismo di anelli è lasciata per esercizio. È ovvio che φ è iniettivo, poiché $\ker \varphi = \{0\}$.

Consideriamo ora l'elemento $X = (0, 1, 0, 0, \dots)$. Per induzione su k, dimostriamo che $X^k = (e(k, 1)_n)$, dove $a \in A$ e

$$e(k, a)_n = \begin{cases} a & \text{se } n = k; \\ 0 & \text{se } n \neq k. \end{cases}$$

In altre parole, la successione $(e(k, a)_n)$ è quella fatta tutta di zeri, tranne un solo a, al posto di indice k. Chiaramente $X = (e(1, 1)_n)$.

Il fatto che $X^0 = (e(0, 1)_n) = (1, 0, 0, \dots)$ è ovvio. Supponiamo dunque $k > 1$ e che $X^{k-1} = (e(k-1, 1)_n)$. Allora $X^k = X^{k-1}X = (e(k-1, 1)_n)(e(1, 1)_n) = (b_n)$ dove

$$b_i = \sum_{j=0}^{i} e(k-1, 1)_j e(1, 1)_{i-j}.$$

In questa somma compaiono fattori diversi da 0 solo se $i \geq 1$ e, in tal caso, l'unico fattore eventualmente diverso da 0 si ottiene per $i - j = 1$, cioè $j = i - 1$. Quindi $b_i = e(k-1, 1)_{i-1} e(1, 1)_1 = e(k-1, 1)_{i-1}$,

che è diverso da zero se e solo se $k-1=i-1$, cioè $k=i$. In tal caso $b_k=1$ e quindi $b_i=e(k,1)_i$, $i\in\mathbf{N}$.

Non è difficile verificare anche che $\widetilde{a}X^k=(e(k,a)_n)$ (esercizio). Se ora (a_n) è un dato polinomio, abbiamo $a_n=0$, per $n>m$, e quindi

$$\begin{aligned}(a_0,a_1,a_2,\dots,a_m,\dots)&=(e(0,a_0)_n)+(e(1,a_1)_n)+(e(2,a_2)_n)+\cdots+(e(m,a_m)_n)\\&=\widetilde{a_0}+\widetilde{a_1}X+\widetilde{a_2}X^2+\cdots+\widetilde{a_m}X^m.\end{aligned}$$

Abbiamo allora ottenuto, quasi, la solita rappresentazione di un polinomio. Il passo successivo è scrivere a_i al posto di $\widetilde{a_i}$. Possiamo farlo, poiché l'applicazione $\varphi\colon A\to A[X]$ è un omomorfismo iniettivo. Perciò possiamo *identificare* a con $\widetilde{a}$ e questo non crea alcun problema nei calcoli (esattamente come quando si identifica un numero complesso di parte immaginaria nulla con un numero reale).

Un polinomio $f\in A[X]$ si può allora scrivere, *in modo unico*, come

$$f=a_0+a_1X+a_2X^2+\cdots+a_nX^n$$

con $a_n\neq 0$, con un'unica eccezione, quella di $f=0$. Diremo che n è il *grado* di f, se $f\neq 0$. Il grado di 0 (il polinomio nullo) è $-\infty$. Il grado di f si denota con il simbolo $\partial(f)$.

Porremo $-\infty+n=n+(-\infty)=-\infty+(-\infty)=-\infty$ e $-\infty<n$, dove $n\in\mathbf{N}$. In tal modo le formule sui gradi che scriveremo ora valgono per tutti i polinomi e non si devono fare distinzioni nel caso in cui compaia il polinomio nullo.

Si ha allora che gli elementi di A sono (identificati con) i polinomi $f\in A[X]$ tali che $\partial(f)\leq 0$.

Si verifica poi che il modo con il quale abbiamo definito la moltiplicazione di polinomi corrisponde esattamente al procedimento di moltiplicazione formale imparato nella scuola media, con la "riduzione dei termini simili".

Proposizione. *Siano $f,g\in A[X]$. Allora*

$$\partial(f+g)\leq\max\{\partial(f),\partial(g)\}\qquad e\qquad \partial(fg)\leq\partial(f)+\partial(g).$$

Dimostrazione. La cosa è ovvia se uno dei polinomi è nullo. Supponiamo f e g entrambi non nulli, e poniamo $f=(a_n)$ e $g=(b_n)$. Abbiamo già visto che, per $n>\partial(f)$ e $n>\partial(g)$, $a_n+b_n=0$. Perciò il grado di $f+g$ non può superare il massimo fra i gradi di f e di g.

Per la moltiplicazione, abbiamo già osservato che, posto $(c_n)=(a_n)(b_n)$, si ha

$$c_n=0,\quad \text{per } n>\partial(f)+\partial(g)$$

e quindi il grado di fg non può superare la somma dei gradi di f e di g. □

Attenzione, può succedere che $\partial(fg)<\partial(f)+\partial(g)$. Sia infatti $A=\mathbf{Z}/6\mathbf{Z}$ e consideriamo i polinomi

$$f=1+3X+2X^2,\quad g=2+4X+2X^2+3X^3.$$

Allora

$$\begin{aligned}fg&=(1+3X+2X^2)(2+4X+2X^2+3X^3)\\&=2+4X+2X^2+3X^3+6X+12X^2+6X^3+9X^4+4X^2+8X^3+4X^4+6X^5\\&=2+(4+6)X+(2+12+4)X^2+(3+6+8)X^3+(9+4)X^4+6X^5\\&=2+4X+5X^3+X^4\end{aligned}$$

perché, in A, $6=0$. Dunque il grado di fg è 4 e *non* 5.

La solita formula del grado di un prodotto non vale dunque in $A[X]$, per $A=\mathbf{Z}/6\mathbf{Z}$. Anzi, non vale in alcun anello che non sia un dominio: se A non è un dominio e $a,b\in A$ sono elementi non nulli tali che $ab=0$, abbiamo

$$aX\cdot bX=(ab)X^2=0$$

e $\partial(aX)=1$, $\partial(bX)=1$, ma $\partial(0)=-\infty\neq 2$. Ancora più facilmente: $\partial(a)=0$, $\partial(b)=0$, ma $\partial(ab)=\partial(0)=-\infty$.

La solita formula vale, viceversa, in un dominio.

Proposizione. *Sia A un dominio e siano $f,g\in A[X]$. Allora*

$$\partial(fg)=\partial(g)+\partial(g).$$

In particolare $A[X]$ è un dominio.

DIMOSTRAZIONE. Se $f = a_0 + a_1X + \cdots + a_mX^m$ ha grado m e $g = b_0 + b_1X + \cdots + b_nX^n$ ha grado n, cioè $a_m \neq 0$ e $b_n \neq 0$, allora nel prodotto fg compare il termine $a_mb_nX^{m+n}$. Poiché $a_mb_n \neq 0$ (siamo in un dominio), il grado di fg non può essere minore di $m + n = \partial(f) + \partial(g)$. Unendo questo alla proposizione precedente, abbiamo la tesi.

Il fatto che $A[X]$ sia un dominio segue allora dal fatto che i polinomi non nulli hanno un grado in $\mathbf{N}$ e la somma di due numeri naturali non è $-\infty$. Quindi il prodotto di polinomi non nulli è non nullo. □

2.2. Valutazioni

I polinomi sono spesso introdotti come "funzioni". Vedremo che, anche nel caso astratto dei polinomi a coefficienti in un anello, si possono fare analoghe considerazioni.

TEOREMA. *Sia B un anello commutativo e sia A un suo sottoanello. Fissiamo $b \in B$; allora esiste uno ed un solo omomorfismo di anelli*

$$v_b \colon A[X] \to B$$

tale che: (1) *per ogni $a \in A$, $v_b(a) = a$;* (2) *$v_b(X) = b$.*

DIMOSTRAZIONE. (Unicità) Sia $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$; allora, poiché v_b deve essere un omomorfismo, avremo

$$\begin{aligned} v_b(f) &= v_b(a_0 + a_1X + \cdots + a_nX^n) \\ &= v_b(a_0) + v_b(a_1)v_b(X) + \cdots + v_b(a_n)v_b(X^n) \\ &= a_0 + a_1b + \cdots + a_nb^n \end{aligned}$$

e quindi v_b è univocamente determinato.

(Esistenza) Il fatto che l'applicazione v_b definita dalla formula appena scritta è un omomorfismo è una facile verifica. □

Useremo spesso il teorema nel caso in cui $B = A$. L'applicazione v_b si chiama *valutazione in b* e si pone, come al solito

$$v_b(f) = f(b).$$

Ogni polinomio $f \in A[X]$ definisce dunque un'applicazione $\hat{f} \colon A \to A$, ponendo

$$\hat{f}(a) = f(a) = v_a(f),$$

che si chiama la *funzione polinomiale associata a f*. Occorre osservare che polinomi distinti possono definire la stessa funzione polinomiale. Infatti se $A = \mathbf{Z}/5\mathbf{Z}$, il polinomio $f = X(X-1)(X-2)(X-3)(X-4)$ definisce la stessa funzione polinomiale del polinomio nullo: $\hat{f} = \hat{0}$, poiché, per ogni $a \in \mathbf{Z}/5\mathbf{Z}$, $\hat{f}(a) = v_a(f) = 0$. Di fatto $\hat{f} = \hat{g}$ se e solo se $\widehat{f-g} = \hat{0}$ (esercizio).

Vedremo più avanti una condizione che garantisce che polinomi distinti abbiano funzioni polinomiali distinte.

2.3. Divisione

Anche per i polinomi, come per i numeri interi, è possibile la divisione con resto; tuttavia, in generale, bisognerà porre qualche condizione sul divisore. Se $f \in A[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, con $a_n \neq 0$, diremo che a_n è il *coefficiente direttivo* di f; diremo che f è *monico* se il suo coefficiente direttivo è 1. In particolare un polinomio monico è non nullo.

LEMMA. *Siano $f, g \in A[X]$ e supponiamo che g sia monico. Allora $\partial(fg) = \partial(f) + \partial(g)$.*

DIMOSTRAZIONE. Se $f = 0$, non c'è nulla da dimostrare. Se $f \neq 0$ ha grado n, il coefficiente direttivo di f è a e g ha grado m, allora il coefficiente del termine di posto $n + m$ nella successione fg è a (esercizio). □

COROLLARIO. *Se $fg = 0$ e g è monico, allora $f = 0$.*

PROPOSIZIONE. *Siano $f, g \in A[X]$ e supponiamo g monico. Allora esistono e sono unici due polinomi $q, r \in A[X]$ tali che $f = gq + r$ e $\partial(r) < \partial(g)$.*

DIMOSTRAZIONE. (Unicità) Supponiamo che $f = gq + r = gq + r'$, con $\partial(r) < \partial(g)$ e $\partial(r') < \partial(g)$. Allora $r - r' = g(q' - q)$ e quindi

$$\partial(g) + \partial(q' - q) = \partial(g(q' - q)) = \partial(r - r') \leq \max\{\partial(r), \partial(r')\} < \partial(g)$$

e ciò è assurdo, a meno che non sia $\partial(q' - q) = -\infty$, cioè $q' - q = 0$ e quindi anche $r = r'$.

(Esistenza) Il caso di $f = 0$ è banale. Facciamo allora induzione su $\partial(f)$. Se $\partial(f) = 0$, allora $f = g0 + f$ è la divisione richiesta, purché $\partial(g) > 0$. Se anche $\partial(g) = 0$, abbiamo $g = 1$ e quindi $f = gf + 0$.

Supponiamo $\partial(f) = n > 0$ e che la tesi sia vera per i polinomi di grado minore di n. Indichiamo con m il grado di g.

Se $n < m$, non c'è nulla da dimostrare: $f = g0 + f$.

Se $n \geq m$, scriviamo $f = a_0 + a_1X + \cdots + a_nX^n$ e consideriamo $h = a_nX^{n-m}$. Allora il polinomio $f_1 = f - gh$ ha grado minore di n: infatti gh ha grado n ed ha lo stesso coefficiente direttivo di f. Per l'ipotesi induttiva, possiamo scrivere $f_1 = gq_1 + r$, con $\partial(r) < \partial(g)$. Ma allora

$$f = gh + f_1 = gh + gq_1 + r = g(h + q_1) + r$$

e possiamo porre $q = h + q_1$. □

Notiamo che la dimostrazione dell'esistenza di quoziente e resto rispecchia esattamente il procedimento di divisione fra polinomi imparato nella scuola media: si ordina f secondo le potenze decrescenti di X; poi si divide il termine di grado massimo di f per il termine di grado massimo di g (nel nostro caso X^m) e si trascrive il risultato (nel nostro caso h). Poi si moltiplica questo risultato per ciascuno dei termini di f e si esegue la sottrazione (cioè si calcola f_1) e si continua con f_1 (cioè si applica il passo induttivo).

Tradizionalmente si usa uno schema del tipo di quello in Tabella 1.

Notiamo che, quando l'anello A è un campo, è possibile anche dividere per polinomi non monici; lo schema è lo stesso e l'esistenza di quoziente e resto è garantita dal fatto che, ovviamente, se g è un polinomio con coefficiente direttivo invertibile a, allora il quoziente e il resto della divisione di f per g sono gli stessi del quoziente e del resto della divisione di af per $a^{-1}g$ e $a^{-1}g$ è monico.

2.4. Radici di polinomi

Sia $f \in A[X]$ e sia $a \in A$; diciamo che a è una *radice* di f se $f(a) = 0$.

Se l'anello A è arbitrario, possono accadere cose strane sulle radici di un polinomio. Ad esempio, se $A = \mathbf{Z}/8\mathbf{Z}$ e $f = X^2 + 2X$, allora

$$f(0) = 0, f(1) = 3, f(2) = 0, f(3) = 7, f(4) = 0, f(5) = 3, f(6) = 0, f(7) = 7$$

e quindi f ha *quattro* radici.

Per comprendere meglio questa apparente stranezza, dimostriamo il famoso *Teorema di Ruffini*.

TEOREMA. *Sia A un anello commutativo e siano $f \in A[X]$ e $a \in A$; allora a è una radice di f se e solo se il polinomio $X - a$ divide f.*

DIMOSTRAZIONE. Se $X - a$ divide f, allora $f = (X - a)q$ e quindi $v_a(f) = v_a(X - a)v_a(q) = 0$, cioè $f(a) = 0$.

Viceversa, supponiamo che a sia una radice di f; possiamo eseguire la divisione di f per $X - a$, che è monico. Allora $f = (X - a)q + r$, dove $\partial(r) < \partial(X - a) = 1$. Perciò $r \in A$ e quindi, in particolare $v_a(r) = r$. Ma allora

$$0 = f(a) = v_a(f) = v_a((X - a)q + r) = v_a(X - a)v_a(q) + v_a(r) = r$$

cioè la tesi. □

Se eseguiamo la divisione del polinomio $X^2 + 2X \in \mathbf{Z}/8\mathbf{Z}[X]$ successivamente per X, $X - 2$, $X - 4$ e $X - 6$, troviamo allora

$$f = X(X + 2) = (X - 2)(X - 4) = (X - 4)(X - 2) = (X - 6)X,$$

in accordo con il teorema di Ruffini. La stranezza nasce dunque dal fatto che, in $\mathbf{Z}/8\mathbf{Z}$, vale $2 \cdot 4 = 0$. Invece non accadono cose spiacevoli quando l'anello è un dominio. Il teorema seguente fa vedere che un polinomio non nullo a coefficienti in un dominio non può avere più radici del suo grado.

TEOREMA. *Sia A un dominio e sia $f \in A[X]$, con $\partial(f) > 0$, e se $a_1, a_2, \ldots, a_n \in A$ sono radici distinte di f, allora $n \leq \partial(f)$.*

Tabella 1 Esempi di divisioni fra polinomi.

(1) Divisione di $4X^3+2X^2+3X+7$ per X^2+5 in $\mathbf{Z}[X]$.

$$\begin{array}{rr|l} 4X^3+2X^2+3X+7 & X^2+5 & \\ \cline{2-2} 4X^3+20X & 4X+2 & \\ \cline{1-1} 2X^2-17X+7 & & \\ 2X^2+10 & & \\ \cline{1-1} -17X-3 & & \end{array}$$

Il quoziente è $4X+2$ e il resto è $-17X-3$.

(2) Divisione di $3X^4+5X^2-3X+2$ per X^2-3X+1 in $\mathbf{Z}/7\mathbf{Z}$.

$$\begin{array}{rr|l} 3X^4+5X^2-3X+2 & X^2-3X+1 & \\ \cline{2-2} 3X^4-2X^3+3X^2 & 3X^2+2X+1 & \\ \cline{1-1} 2X^3+2X^2-3X+2 & & \\ 2X^3-6X^2+2X & & \\ \cline{1-1} X^2-5X+2 & & \\ X^2-3X+1 & & \\ \cline{1-1} -2X+1 & & \end{array}$$

Il quoziente è $3X^2+2X+1$ e il resto è $-2X+1=5X+1$.

(3) Divisione di X^5+2X^4+X+2 per X^3+X+1 in $\mathbf{Z}/3\mathbf{Z}$.

$$\begin{array}{rr|l} X^5+2X^4+X+2 & X^3+X+1 & \\ \cline{2-2} X^5+X^3+X^2 & X^2+2X-1 & \\ \cline{1-1} 2X^4-X^3-X^2+X+2 & & \\ 2X^4+2X^2+2X & & \\ \cline{1-1} -X^3-X+2 & & \\ -X^3-X-1 & & \\ \cline{1-1} 0 & & \end{array}$$

Il quoziente è $X^2+2X-1=X^2+2X+2$ e il resto è 0.

DIMOSTRAZIONE. Facciamo induzione su $\partial(f)$, partendo da 1. Se $\partial(f)=1$, possiamo scrivere $f=aX+b$, con $a\neq 0$. Se a_1 e a_2 sono radici di f, abbiamo

$$aa_1+b=0=aa_2+b$$

e quindi, in particolare $aa_1=aa_2$, da cui $a(a_1-a_2)=0$ e, poiché A è un dominio e $a\neq 0$, $a_1=a_2$. Perciò f ha al più una radice.

Supponiamo ora la tesi vera per polinomi di grado minore del grado di f.

Eseguiamo la divisione di f per $X-a_n$: poiché a_n è una radice, possiamo scrivere $f=(X-a_n)q$. Valutiamo in a_1: allora

$$0=f(a_1)=(a_1-a_n)q(a_1)$$

e, essendo per ipotesi $a_1\neq a_n$, necessariamente a_1 è radice di q. Analogamente $a_2,\dots,a_{n-1}$ sono radici di q e, per l'ipotesi induttiva, applicabile in quanto $\partial(q)=\partial(f)-1$,

$$n-1\leq\partial(q)=\partial(f)-1,$$

cioè $n\leq\partial(f)$. □

Naturalmente un polinomio può non avere radici; ad esempio, $2X+1\in\mathbf{Z}[X]$ non ha radici. Analogamente, se $\mathbf{R}$ indica il campo dei reali, $X^2+1\in\mathbf{R}[X]$ non ha radici.

Un dominio è un campo precisamente quando tutti i polinomi di grado 1 hanno una radice: infatti, se A è un dominio di questo tipo, una radice di $aX-1$ (con $a\neq 0$) è proprio l'inverso di a.

2.5. Fattorizzazione di polinomi

Per il resto del capitolo lavoreremo in un campo A: in tal caso, infatti, $A[X]$ *è un dominio euclideo*, prendendo come applicazione grado proprio il grado. In particolare i polinomi in $A[X]$ possiedono una fattorizzazione unica come prodotto di polinomi irriducibili. È evidente che, in tal caso, possiamo considerare una "forma normale" di una fattorizzazione: infatti gli elementi invertibili di $A[X]$ sono esattamente gli elementi non nulli di A e quindi ogni polinomio è associato ad uno ed un solo polinomio monico.

Useremo spesso il seguente fatto: se B è un sottoanello del campo A, allora ogni polinomio $f \in B[X]$ può essere considerato come un polinomio a coefficienti in A: infatti B è anche un sottoanello di $A[X]$ e l'omomorfismo $v_X \colon A[X] \to B[X]$ è iniettivo. Questa considerazione permette talvolta di ottenere risultati sui polinomi in $A[X]$.

TEOREMA. *Sia $f \in A[X]$, con $\partial(f)\,0$. Allora f si può scrivere in modo unico, a meno dell'ordine come*

$$f = ag_1g_2 \dots g_k$$

dove $a \in A$, $a \neq 0$, e $g_1, g_2, \dots, g_k$ sono polinomi irriducibili monici.

Il coefficiente a è proprio il coefficiente direttivo di f.

Il problema di trovare quali sono i polinomi irriducibili, in generale, non è risolubile. Vedremo allora alcuni casi particolari.

Osserviamo che dal teorema di Ruffini segue immediatamente che un polinomio irriducibile di grado maggiore di 1 non ha radici (altrimenti sarebbe riducibile). Il viceversa vale, in generale, solo per polinomi di grado "basso".

PROPOSIZIONE. *Ogni polinomio di grado 1 è irriducibile; un polinomio di grado 2 o 3 è irriducibile se e solo se non ha radici.*

DIMOSTRAZIONE. La prima affermazione è ovvia. Sia f di grado 2 o 3; se f è irriducibile, certamente non ha radici. Se f è riducibile, allora $f = f_1f_2$, con $0 < \partial(f_i) < \partial(f)$ $(i = 1, 2)$. Perciò uno fra f_1 e f_2 deve avere grado 1 e quindi avere una radice, che è anche radice di f. □

Fattorizzazione in $\mathbf{C}[X]$. Il teorema seguente fu dimostrato rigorosamente, per la prima volta, da Gauss nella sua tesi di laurea. È storicamente noto come "teorema fondamentale dell'algebra", anche se non ricopre più un ruolo molto importante. Indichiamo con $\mathbf{C}$ il campo dei numeri complessi.

TEOREMA. *Se f è un polinomio di grado positivo a coefficienti in $\mathbf{C}$, allora f ha una radice.*

La dimostrazione algebrica di questo teorema è piuttosto complicata; esiste anche una dimostrazione analitica, che usa le cosiddette *funzioni olomorfe*.

Se prendiamo per buono questo teorema, abbiamo allora un facile corollario.

COROLLARIO. *Un polinomio in $\mathbf{C}[X]$ è irriducibile se e solo se ha grado 1.*

DIMOSTRAZIONE. Se $\partial(f) = 1$, certamente f non è invertibile in $\mathbf{C}[X]$ e non è 0; inoltre, se $f = gh$, allora $\partial(g) + \partial(h) = 1$ e quindi uno fra g e h ha grado 0, quindi è invertibile. Ne segue che f è irriducibile.

Viceversa, sia f irriducibile. Allora $\partial(f) > 0$ e quindi f ha una radice, sia a; allora $f = (X - a)q$ e, per l'irriducibilità, q deve essere invertibile in $\mathbf{C}[X]$, perché $X - a$ non lo è. Ma allora $\partial(q) = 0$ e quindi $\partial(f) = 1$. □

Fattorizzazione in $\mathbf{R}[X]$. Dal teorema sui polinomi in $\mathbf{C}[X]$ è facile ricavare la caratterizzazione dei polinomi irriducibili in $\mathbf{R}[X]$.

PROPOSIZIONE. *Ogni polinomio in $\mathbf{R}[x]$ di grado dispari ha almeno una radice in $\mathbf{R}$.*

DIMOSTRAZIONE. Sia $f \in \mathbf{R}[x]$ di grado dispari; non è restrittivo supporre che f sia monico. Allora la funzione $\hat{f} \colon \mathbf{R} \to \mathbf{R}$ è continua; inoltre

$$\lim_{t \to -\infty} \hat{f}(t) = -\infty \qquad \text{e} \qquad \lim_{t \to +\infty} \hat{f}(t) = +\infty;$$

in particolare $\hat{f}$ assume valori positivi e negativi. Per un noto teorema di Analisi, $\hat{f}$ assume il valore 0 e quindi f ha una radice. □

TEOREMA. *Sia $f \in \mathbf{R}[X]$; allora f è irriducibile se e solo se $\partial(f) = 1$ oppure $\partial(f) = 2$ e f non ha radici in $\mathbf{R}$.*

DIMOSTRAZIONE. Basta dimostrare una sola direzione. Supponiamo f irriducibile e monico, con $\partial(f) > 1$. Allora $\partial(f)$ è pari e f non ha radici in $\mathbf{R}$.

Se consideriamo f come polinomio in $\mathbf{C}[X]$, allora f ha certamente una radice $b \in \mathbf{C}$; scriviamo $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$. Allora (la sopralineatura indica il numero complesso coniugato)

$$\begin{aligned} f(\bar{b}) &= a_0 + a_1\bar{b} + a_2\bar{b}^2 + \cdots + a_n\bar{b}^n \\ &= \overline{a_0} + \overline{a_1}\bar{b} + \overline{a_2}\bar{b}^2 + \cdots + \overline{a_n}\bar{b}^n \\ &= \overline{a_0 + a_1b + a_2b^2 + \cdots + a_nb^n} \\ &= \overline{f(b)} = \bar{0} = 0 \end{aligned}$$

e quindi anche $\bar{b}$ è una radice di f in $\mathbf{C}$. Tuttavia $b \in \mathbf{C} \setminus \mathbf{R}$ e quindi $b \neq \bar{b}$. Ne segue che $g = (X-b)(X-\bar{b})$ divide f in $\mathbf{C}[X]$. Ma $g = X^2 - (b+\bar{b})X + b\bar{b}$ è un polinomio a coefficienti reali e quindi g divide f in $\mathbf{R}[X]$. Per l'irriducibilità di f, $f = g$. □

I polinomi monici di grado 2 in $\mathbf{R}[X]$ che non hanno radici sono precisamente quelli della forma $(X-b)(X-\bar{b})$, con $b \in \mathbf{C} \setminus \mathbf{R}$.

Fattorizzazione in $\mathbf{Q}[X]$. La situazione in $\mathbf{Q}[X]$ è molto più complicata. Se $f \in \mathbf{Q}[X]$ e determiniamo la fattorizzazione di f in $\mathbf{R}[X]$, allora è possibile stabilire se f è riducibile o no in $\mathbf{Q}[X]$.

Ad esempio, $X^4 + 1 \in \mathbf{Q}[X]$ è irriducibile. Infatti, in $\mathbf{R}[X]$,

$$X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2+1)^2 - (\sqrt{2}\,X)^2 = (X^2 - \sqrt{2}\,X + 1)(X^2 + \sqrt{2}\,X + 1)$$

e questa è l'unica fattorizzazione (come prodotto di irriducibili) di $X^4 + 1$ in $\mathbf{R}[X]$. Se esistesse una fattorizzazione in $\mathbf{Q}[X]$, dovrebbe coincidere con questa: assurdo, poiché $\sqrt{2} \notin \mathbf{Q}$.

Un altro metodo che a volte funziona è quello di cercare radici razionali.

PROPOSIZIONE. *Sia $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbf{Z}[X]$ ($n > 0$) e sia $b/c \in \mathbf{Q}$, con $\mathrm{mcd}(b,c) = 1$. Se b/c è una radice di f, allora b divide a_0 e c divide a_n.*

DIMOSTRAZIONE. Abbiamo $f(b/c) = a_0 + a_1(b/c) + a_2(b/c)^2 + \cdots + a_n(b/c)^n = 0$ e perciò

$$a_0c^n + a_1bc^{n-1} + a_2b^2c^{n-2} + \cdots + a_{n-1}b^{n-1}c + a_nb^n = 0.$$

Ne segue che c divide a_nb^n e quindi c divide a_n. Analogamente, b divide a_0c^n e quindi b divide a_0. □

Ad esempio, $f = 8X^3 - 6X + 1$ è irriducibile in $\mathbf{Q}[X]$, poiché ha grado 3 e non ha radici; infatti le possibili radici in $\mathbf{Q}$ sono 1, -1, $1/2$, $-1/2$, $1/4$, $-1/4$, $1/8$ e $-1/8$; un facile calcolo mostra che nessuno di questi razionali è una radice di f.

Fattorizzazione in $\mathbf{Z}[X]$. L'anello $\mathbf{Z}[X]$ non è un dominio euclideo, poiché l'ideale $2\mathbf{Z}[X] + X\mathbf{Z}[X]$ non è principale (esercizio). Tuttavia si può dimostrare che anche in $\mathbf{Z}[X]$ vale il teorema sulla fattorizzazione unica: *se $f \in \mathbf{Z}[X] \setminus \{0, 1, -1\}$, allora f è, in modo unico a meno dell'ordine e di elementi associati, prodotto di polinomi irriducibili.* Bisogna fare un po' di attenzione, perché ogni numero primo, considerato come polinomio in $\mathbf{Z}[X]$, è irriducibile.

Un polinomio $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbf{Z}[X]$ tale che $\mathrm{mcd}(a_0, a_1, \ldots, a_n) = 1$ si dice *primitivo*. Allora è chiaro che ogni polinomio in $f \in \mathbf{Z}[X]$ si può scrivere, in modo unico, come $f = ag$, dove $a \in \mathbf{Z}$, $a > 0$ e g è primitivo. Gli unici polinomi primitivi di grado 0 sono 1 e -1.

Per il polinomi a coefficienti interi esiste un criterio, che è a volte utile, noto come *Criterio di Eisenstein*.

PROPOSIZIONE. *Sia $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbf{Z}[X]$ ($n > 0$) un polinomio primitivo; supponiamo che esista un numero primo p tale che:*

(1) *p divide a_0, a_1, …, a_{n-1};*
(2) *p non divide a_n;*
(3) *p^2 non divide a_0.*

Allora f è irriducibile in $\mathbf{Z}[X]$.

DIMOSTRAZIONE. Supponiamo che f sia riducibile, cioè che

$$f = (b_0 + b_1X + b_2X^2 + \cdots + b_rX^r)(c_0 + c_1X + c_2X^2 + \cdots + c_sX^s),$$

con $r, s > 0$. Infatti f non può avere fattori irriducibili di grado zero, per l'ipotesi che f è primitivo.

Allora $a_0 = b_0c_0$ e quindi uno solo fra b_0 e c_0 è divisibile per p; sia, per fissare le idee, b_0. Dimostriamo, per induzione, che p divide b_i, $i = 1, 2, \dots, r$. Poniamo $a_j = 0$ per $j > n$, $b_j = 0$ per $j > r$ e $c_j = 0$ per $j > s$ e supponiamo di avere dimostrato che p divide b_i $(i < r)$. Perciò

$$a_{i+1} = \sum_{j=0}^{i+1} b_j c_{i+1-j} = b_{i+1}c_0 + \sum_{j=0}^{i+1} b_j c_{i+1-j}$$

e quindi, essendo $i < r < n$, dal fatto che p divide a_{i+1} e non divide c_0, segue che p divide b_{i+1}. In particolare possiamo scrivere $b_r = pb'_r$ e quindi $a_n = b_r c_s = pb'_r c_s$, contro l'ipotesi. □

Il seguente risultato è noto come *lemma di Gauss*.

LEMMA. *Il prodotto di due polinomi primitivi in* $\mathbf{Z}[X]$ *è primitivo.*

DIMOSTRAZIONE. Siano $f, g \in \mathbf{Z}[X]$ primitivi. Scriviamo

$$f = a_0 + a_1X + \cdots + a_mX^m, \qquad g = b_0 + b_1X + \cdots + b_nX^n,$$
$$fg = c_0 + c_1X + \cdots + c_{m+n}X^{m+n}, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Dire che il prodotto fg non è primitivo, equivale a dire che esiste un numero primo p che divide tutti i coefficienti di fg. Siccome f e g non sono primitivi, esistono i minimi indici i e j tali che p non divida a_i e b_j rispettivamente. Ma ora

$$a_ib_j = c_{i+j} - (a_0b_{i+j} + \cdots + a_ib_{j-1} + a_{i-1}b_j + \cdots + a_{i+j}b_0)$$

ma p divide c_{i+j} e ciascuno degli addendi nella somma. Perciò deve dividere anche a_ib_j. Siccome p primo, deve dividere a_i oppure b_j: contraddizione. □

PROPOSIZIONE. *Sia* $f \in \mathbf{Z}[X]$ *un polinomio primitivo. Allora* f *è irriducibile in* $\mathbf{Z}[X]$ *se e solo se è irriducibile in* $\mathbf{Q}[X]$.

DIMOSTRAZIONE. Se f è riducibile in $\mathbf{Z}[X]$, allora esistono $g, h \in \mathbf{Z}[X] \setminus \{0, 1, -1\}$ tali che $f = gh$. Poiché f è primitivo, possiamo escludere il fatto che uno fra g e h abbia grado 0. Quindi f è riducibile anche in $\mathbf{Q}[X]$.

Supponiamo ora f irriducibile in $\mathbf{Z}[X]$ e che $f = gh$, con $g, h \in \mathbf{Q}[X]$. Eseguiamo le seguenti operazioni:

(1) riduciamo ai minimi termini tutti i coefficienti di g;
(2) chiamiamo a il massimo comun divisore dei numeratori dei coefficienti di g così ottenuti;
(3) chiamiamo b il minimo comune multiplo dei numeratori dei coefficienti di g così ottenuti.

In tal modo otteniamo che

$$g = \frac{a}{b}g'$$

dove $\mathrm{mcd}(a, b) = 1$ e $g' \in \mathbf{Z}[X]$ è un polinomio primitivo. Possiamo allora eseguire le stesse operazioni, ottenendo $h = (c/d)h'$, con $\mathrm{mcd}(c, d) = 1$ e $h' \in \mathbf{Z}[X]$ primitivo. Per il lemma di Gauss, il prodotto $f' = g'h'$ è primitivo. Perciò abbiamo, in $\mathbf{Z}[X]$,

$$bdf = acf'.$$

Ora, il massimo comun divisore dei coefficienti di bdf è necessariamente bd e il massimo comun divisore dei coefficienti di acf' è necessariamente ac. Quindi $bd = ac$ e dunque $a/b = d/c$. In definitiva, $f = g'h'$ e, essendo f irriducibile, uno dei due polinomi g' e h' è invertibile in $\mathbf{Z}$, cioè $g' = 1$ oppure $h' = 1$. Quindi f è irriducibile in $\mathbf{Q}[X]$. □

Fattorizzazione in $\mathbf{Z}/p\mathbf{Z}[X]$. Se p è un primo, l'anello $\mathbf{Z}/p\mathbf{Z}$ è un campo. La fattorizzazione in $\mathbf{Z}/p\mathbf{Z}[X]$ è, in linea di principio, possibile, poiché esistono esattamente p^k polinomi monici di grado k.

In $\mathbf{Z}/p\mathbf{Z}[X]$ esistono polinomi irriducibili di ogni grado (positivo).

Ogni polinomio in $\mathbf{Z}[X]$ può essere considerato, formalmente, come un polinomio in $\mathbf{Z}/p\mathbf{Z}[X]$, interpretando i coefficienti come multipli. Se $f \in \mathbf{Z}[X]$, indicheremo con $f_{(p)}$ il polinomio interpretato in $\mathbf{Z}/p\mathbf{Z}[X]$. Un polinomio irriducibile in $\mathbf{Z}[X]$ può diventare, in tal modo, riducibile. Ad esempio $f = X^2 + X + 1 \in \mathbf{Z}[X]$ è irriducibile. Invece $f_{(3)} = X^2 + X + 1 \in \mathbf{Z}/3\mathbf{Z}[X]$ è riducibile; infatti

$$X^2 + X + 1 = X^2 - 3X + X + 1 = X^2 - 2X + 1 = (X - 1)^2,$$

essendo $-3X = 0$. Viceversa, invece, se $f \in \mathbf{Z}[X]$ è riducibile, anche $f_{(p)}$ è riducibile, per ogni primo p. Basta infatti interpretare la fattorizzazione in $\mathbf{Z}[X]$ come una fattorizzazione in $\mathbf{Z}/p\mathbf{Z}[X]$. Ad esempio, se

$$f = X^4 - 4X^3 + 2X^2 + X + 6 = (X-2)(X-3)(X^2+X+1) \in \mathbf{Z}[X],$$

allora

$$\begin{aligned} f_{(2)} &= X(X+1)(X^2+X+1) && \text{in } \mathbf{Z}/2\mathbf{Z}[X]; \\ f_{(3)} &= X(X-1)^2(X-2) && \text{in } \mathbf{Z}/3\mathbf{Z}[X]; \\ f_{(5)} &= (X-2)(X-3)(X^2+X+1) && \text{in } \mathbf{Z}/5\mathbf{Z}[X]; \\ f_{(7)} &= (X-2)^2(X-3)(X-4) && \text{in } \mathbf{Z}/7\mathbf{Z}[X]. \end{aligned}$$

Infatti, per $p = 7$, abbiamo sicuramente $f_{(7)} = (X-2)(X-3)(X^2+X+1)$. Se poniamo $g = X^2+X+1$, otteniamo che $g(2) = 2^2 + 2 + 1 = 7 = 0$ e $g(4) = 4^2 + 4 + 1 = 21 = 0$, cioè $g = (X-2)(X-4)$.

CAPITOLO 3

Campi

3.1. Estensioni algebriche

Ricordiamo che un *campo* è un anello commutativo F con $1 \neq 0$ in cui ogni elemento non nullo è invertibile. Diremo che un campo K è *estensione* di un campo F se F è un sottoanello di K. Scriveremo, per abbreviare, K/F, anche se questa notazione non ha nulla a che fare con insiemi quoziente.

Se K è un'estensione di F, ogni polinomio nell'indeterminata X a coefficienti in F può essere considerato anche a coefficienti in K; per essere più precisi, $F[X]$ è un sottoanello di $K[X]$.

Un'altra proprietà importante è che K può essere considerato come spazio vettoriale su F, quindi si possono applicare tutte le nozioni che conosciamo sugli spazi vettoriali.

DEFINIZIONE. L'estensione K/F si dice *finita* se la dimensione di K come spazio vettoriale su F è finita. In tal caso questa dimensione si indica con $[K : F]$.

È talvolta importante considerare estensioni di estensioni. Vale un'importante proprietà.

TEOREMA. *Sia K un'estensione di F e sia L un'estensione di K. Allora L/F è finita se e solo se L/K e K/F sono finite e, in tal caso, $[L : F] = [L : K][K : F]$.*

DIMOSTRAZIONE. Supponiamo che L/K e K/F siano finite; allora esistono $\mathscr{B} = \{l_1, \ldots, l_m\}$, base di L come spazio vettoriale su K, e $\mathscr{C} = \{k_1, \ldots, k_n\}$, base di K come spazio vettoriale su F. Dimostriamo che

$$\mathscr{D} = \{\, l_i k_j \mid 1 \leq i \leq m, 1 \leq j \leq n \,\}$$

è una base di L come spazio vettoriale su F.

(1) *$\mathscr{D}$ è un insieme di generatori.* Infatti, se $l \in L$, possiamo scrivere $l = \sum_{i=1}^{m} \alpha_i l_i$, con $\alpha_1, \ldots, \alpha_m \in K$, dal momento che $\mathscr{B}$ è una base di L/K. Siccome $\mathscr{C}$ è una base di K/F, ciascun k_i può essere scritto come

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} k_j$$

con $\beta_{ij} \in F$. Ne segue che

$$l = \sum_{i=1}^{m} \alpha_i l_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} k_j \right) l_i = \sum_{i,j} \beta_{ij} l_i k_j.$$

(2) *$\mathscr{D}$ è linearmente indipendente.* Supponiamo che

$$\sum_{i,j} \beta_{ij} l_i k_j = 0$$

con $\beta_{ij} \in F$. Allora

$$0 = \sum_{i,j} \beta_{ij} l_i k_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} k_j \right) l_i$$

e quindi, essendo $\mathscr{B}$ linearmente indipendente,

$$\sum_{j=1}^{n} \beta_{ij} k_j = 0 \qquad (i = 1, 2, \ldots, m).$$

Siccome anche $\mathscr{C}$ è linearmente indipendente, abbiamo che

$$\beta_{ij} = 0$$

per ogni i e j.

Viceversa, supponiamo che L/F sia finita. Allora esiste un insieme di generatori finito di L come spazio vettoriale su F e, a maggior ragione, sarà anche un insieme di generatori di L come spazio vettoriale su K. Per finire, K è un sottospazio vettoriale di L/F, quindi ha dimensione finita. □

DEFINIZIONE. Sia K un'estensione di F. Un elemento $b \in K$ si dice *algebrico* su F se esiste un polinomio $f \in F[X]$ non nullo tale che $f(b) = 0$. Un elemento $b \in K$ si dice *trascendente* su F se non è algebrico. Diciamo che l'estensione K/F è algebrica se ogni elemento di K è algebrico su F.

Come esempio classico, $\sqrt{2} \in \mathbf{R}$ è algebrico su $\mathbf{Q}$, poiché è radice del polinomio $X^2 - 2$. Un famoso risultato di Lindemann e Weierstrass dice che π è trascendente su $\mathbf{Q}$.

TEOREMA. *Se K/F è finita, allora è algebrica.*

DIMOSTRAZIONE. Sia $n = [K : F]$ e sia $b \in K$. Allora gli elementi 1, b, $\dots$, b^n sono linearmente dipendenti (sono più della dimensione) e perciò esistono $a_0, a_1, \dots, a_n \in F$, non tutti nulli, tali che $a_0 \cdot 1 + a_1 b + \cdots + a_n b^n = 0$. Questo significa proprio che il polinomio $f = a_0 + a_1 X + \cdots + a_n X^n$ è non nullo e che $f(b) = 0$. □

Il viceversa non è vero, come vedremo più avanti.

Si pone un problema: dato un polinomio non nullo in $F[X]$, è possibile trovare un'estensione K/F dove il polinomio ammetta una radice? Ad esempio, il polinomio $X^2 + 1 \in \mathbf{R}[X]$ non ha radici, ma ne ha nell'estensione $\mathbf{C}$.

Proprio come abbiamo ampliato i reali per ottenere i complessi, si può risolvere il problema di prima in generale.

LEMMA. *Sia $b \in K$ algebrico su F; allora l'insieme $I_b = \{ f \in F[X] \mid f(b) = 0 \}$ è un ideale non nullo di $F[X]$.*

DIMOSTRAZIONE. Chiaramente il polinomio nullo appartiene a I_b; se $f, g \in I_b$, abbiamo che $v_b(f + g) = v_b(f) + v_b(g) = 0 + 0$, quindi $f + g \in I_b$. Se poi $f \in I_b$ e $g \in F[X]$, abbiamo che $v_b(fg) = v_b(f)v_b(g) = 0$. □

Ricordiamo che ogni ideale di $F[X]$ è principale, quindi esiste un unico polinomio monico $f_b \in I_b$ tale che $I_b = f_b F[X]$, cioè ogni polinomio in I_b è della forma $f_b g$, per un opportuno $g \in F[X]$. Questo polinomio è il polinomio monico di grado minimo in I_b e si chiama *polinomio minimo di b*.

PROPOSIZIONE. *Sia $b \in K$ algebrico su F; allora il polinomio minimo $f_b \in F[X]$ è irriducibile.*

DIMOSTRAZIONE. Se $f_b = gh$, con $g, h \in F[X]$, allora $0 = f_b(b) = g(b)h(b)$, quindi $g \in I_b$ oppure $h \in I_b$. Nel primo caso, siccome f_b ha grado minimo, dovremo avere che il grado di g non è minore del grado di f_b, quindi g e f_b hanno lo stesso grado e h ha grado 0, cioè è invertibile. L'altro caso è analogo. □

Esercizio: dimostrare che, se $g \in I_b$ è irriducibile e monico, allora è il polinomio minimo di b.

Attenzione: occorre sempre dire qual è l'estensione che si sta considerando. Ad esempio, il polinomio minimo di $i\sqrt[4]{2} \in \mathbf{C}$ su $\mathbf{Q}$ è $X^4 + 2$, mentre su $\mathbf{R}$ è $X^2 + \sqrt{2}$.

Se consideriamo una famiglia di sottocampi del campo K, la loro intersezione è un sottocampo. Analogamente per sottoanelli. Di conseguenza i concetti di cui parleremo ora sono ben definiti.

DEFINIZIONE. Se $b \in K$, estensione di F, indichiamo con $F[b]$ il minimo sottoanello di K che contenga sia F che b. Con $F(b)$ indichiamo il minimo sottocampo di K che contiene sia F che b.

È ovvio che $F[b] \subseteq F(b)$. Quando saranno uguali? Ci occorre una descrizione di $F[b]$. Consideriamo l'omomorfismo di valutazione

$$\begin{aligned} v_b \colon F[X] &\to K \\ f &\mapsto f(b) \end{aligned}$$

e sia B la sua immagine. Allora B è un sottoanello di K che contiene sia F che b; dunque $F[b] \subseteq B$. Ma un elemento di B si scrive come $f(b)$, per un opportuno $f \in F[X]$, cioè $a_0 + a_1 b + \cdots + a_n b^n$ e questo elemento deve appartenere ad ogni sottoanello di K che contenga sia F che b. Perciò $B = F[b]$.

PROPOSIZIONE. *Se b è algebrico su F, allora $F[b]$ è un campo. Se b è trascendente su F, allora $F[b]$ è isomorfo a $F[X]$.*

DIMOSTRAZIONE. Sia b algebrico. Il teorema di omomorfismo dice che l'immagine di v_b è un anello isomorfo a $F[X]/I_b$, perché I_b è il nucleo di v_b. Siccome I_b è l'ideale principale generato da un elemento irriducibile, esso è massimale, quindi l'immagine di v_b, che è proprio $F[b]$ è un campo.

Se invece b è trascendente, il nucleo di v_b è l'ideale nullo, quindi v_b è iniettivo. Ne segue che $F[b]$ è isomorfo a $F[X]$. □

COROLLARIO. *Se b è algebrico su F, allora $F[b] = F(b)$.*

Notiamo come la dimostrazione "astratta" permetta di evitare la verifica che ogni elemento di $F[b]$ è invertibile. La stessa dimostrazione però può essere resa "algoritmica": vogliamo trovare un metodo per calcolare gli inversi. Prendiamo dunque $b \in K$ algebrico su F e il suo polinomio minimo f_b. Un elemento di $F[a]$ è della forma $c = g(b)$, per un opportuno $g \in F[X]$. L'algoritmo della divisione in $F[X]$ dice che esistono e sono unici $q, r \in F[X]$ tali che

$$g = f_b q + r, \qquad \partial(r) < \partial(f_b).$$

Ne segue che

$$c = g(b) = v_b(g) = v_b(f_b q + r) = v_b(f_b)v_b(q) + v_b(r) = v_b(r).$$

Perciò $c \neq 0$ se e solo se $r(b) \neq 0$. Nel caso in cui $c \neq 0$ possiamo allora dire che $\mcd(f_b, r) = 1$, in quanto $r \neq 0$ ha grado minore del grado di f_b che è irriducibile. Per il teorema di Bézout, che vale anche il $F[X]$, esistono due polinomi $s, t \in F[X]$ tali che

$$sr + tf_b = 1.$$

Valutiamo questa identità in b:

$$1 = v_b(1) = v_b(sr + tf_b) = v_b(s)v_b(r) + v_b(t)v_b(f_b) = s(b)r(b).$$

Non solo abbiamo trovato l'inverso di c, cioè $s(b)$; abbiamo anche visto che ogni elemento di $F[b]$ si scrive come $r(b)$, dove $r \in F[X]$ e $\partial(r) < \partial(f_b)$. Questa scrittura è unica: infatti, se $r_1(b) = r_2(b)$ con $\partial(r_1), \partial(r_2) < \partial(f_b)$, abbiamo che $r_1 - r_2 \in I_b$ e ha grado minore di $\partial(f_b)$, quindi $r_1 - r_2 = 0$.

TEOREMA. *Sia $b \in K$ algebrico su F. Allora $F[b]$ è il minimo sottocampo di K che contiene sia F che b. Inoltre*

$$[F[b] : F] = \partial(f_b)$$

cioè la dimensione di $F[b]$ come spazio vettoriale su F è uguale al grado n del polinomio minimo di b su F e una base è data da $\{1, b, \dots, b^{n-1}\}$.

DIMOSTRAZIONE. Ci basta dimostrare l'asserzione sulla base. Abbiamo visto che ogni elemento di $F[b]$ si scrive in modo unico come $r(b)$, dove $r \in F[X]$ e $\partial(r) < \partial(f)$. Un polinomio r di questo tipo è della forma $a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$ e quindi gli elementi di $F[b]$ si scrivono in modo unico come

$$a_0 \cdot 1 + a_1 b + \cdots + a_{n-1}b^{n-1}$$

e questo dice proprio che ogni elemento di $F[b]$ si scrive in modo unico come combinazione lineare a coefficienti in F di 1, b, …, b^{n-1}. □

Ritorniamo allora al problema di trovare un'estensione opportuna di F in cui un certo polinomio $f \in F[X]$ abbia radici. La costruzione sarà iterativa; intanto, siccome è possibile scomporre f in fattori irriducibili, non è restrittivo supporre che f sia irriducibile. In questo caso l'ideale $I = fF[X]$ è massimale in $F[X]$ e quindi l'anello quoziente $F[X]/I$ è un campo. Inoltre l'applicazione

$$\begin{aligned} \alpha \colon F &\to F[X]/I \\ a &\mapsto [a] \end{aligned}$$

è un omomorfismo iniettivo di anelli. Perciò, invece di scrivere $[a]$ possiamo scrivere a, identificando questi elementi. In tal modo $K = F[X]/I$ diventa un'estensione di F. Poniamo $b = [X] \in K$. Abbiamo allora, scrivendo $f = a_0 + a_1 X + \cdots + a_n X^n$,

$$\begin{aligned} v_b(f) &= a_0 + a_1 b + \cdots + a_n b^n = [a_0] + [a_1]b + \cdots + [a_n]b^n \\ &= [a_0] + [a_1][X] + \cdots + [a_n][X]^n = [a_0 + a_1 X + \cdots + a_n X^n] = [0] = 0. \end{aligned}$$

Il problema è risolto! Infatti K è proprio un'estensione di F in cui f ammette una radice. Possiamo allora scrivere $f = (X - b)f_1$, dove $f_1 \in K[X]$ ha grado più piccolo di f. Questo dà il via alla procedura iterativa.

TEOREMA. *Se $f \in F[X]$ è monico e ha grado $n > 0$, esiste un'estensione K di F tale che:*

(1) *$f = (X - b_1)(X - b_2)\dots(X - b_n)$ in $K[X]$;*
(2) *$K = F[b_1, b_2, \dots, b_n]$*

Se L/F è un'altra estensione con le stesse proprietà, allora esiste un isomorfismo $\alpha \colon K \to L$ tale che $\alpha(a) = a$, per ogni $a \in F$.

Non daremo la dimostrazione di questo teorema, che richiederebbe troppo tempo. L'estensione così determinata, che è allora unica a meno di isomorfismi, si chiama un *campo di riducibilità completa di f*. Con $F[b_1, b_2, \dots, b_n]$, dove gli elementi $b_i \in K$, intendiamo il minimo sottoanello di K che contiene $F \cup \{b_1, \dots, b_n\}$; è facile dimostrare per induzione che $F[b_1, b_2, \dots, b_n]$ è un sottocampo se gli elementi b_i sono algebrici su F. Analogamente $F(b_1, \dots, b_n)$ è il minimo sottocampo di K che contiene $F \cup \{b_1, \dots, b_n\}$.

C'è un'altra proprietà importante delle estensioni algebriche.

TEOREMA. *Sia K/F un'estensione di campi. Se $b, b_1, b_2 \in K$ sono algebrici su F, allora $b_1 + b_2$, $b_1 - b_2$, $b_1 b_2$ e $-b$ sono algebrici su F; se $b \neq 0$, anche b^{-1} è algebrico su F.*

DIMOSTRAZIONE. Consideriamo $F(b_1, b_2)$; è ovvio dalla definizione che $F(b_1, b_2) = F(b_1)(b_2)$. Siccome b_2 è algebrico su F, esso è a maggior ragione algebrico su $F(b_1)$; quindi

$$[F(b_1, b_2) : F] = [F(b_1)(b_2), F(b_1)][F(b_1) : F]$$

è finita e quindi ogni elemento di $F(b_1, b_2)$ è algebrico su F. Quindi lo sono $b_1 + b_2$, $b_1 - b_2$, $b_1 b_2$. Analogamente per $-b$ e b^{-1}. □

COROLLARIO. *Se K è un'estensione di F, allora l'insieme degli elementi di K che sono algebrici su F è un sottocampo di K.*

Diamo senza dimostrazione un famoso teorema dovuto a Steinitz. Prima però una definizione: un campo K si dice *algebricamente chiuso* se ogni polinomio a coefficienti in K, di grado > 0, ammette una radice. Il cosiddetto teorema fondamentale dell'algebra dice che $\mathbf{C}$ è algebricamente chiuso. Un'estensione K di F si dice una *chiusura algebrica* di F se K è algebricamente chiuso e ogni elemento di K è algebrico su F.

TEOREMA. *Ogni campo F ha una chiusura algebrica. Se K e L sono chiusure algebriche di F, allora esiste un isomorfismo $\alpha\colon K \to L$ tale che $\alpha(a) = a$, per ogni $a \in F$.*

Possiamo allora dire, usando gli ultimi due enunciati, che l'insieme $\bar{\mathbf{Q}}$ dei numeri complessi algebrici su $\mathbf{Q}$ è una chiusura algebrica di $\mathbf{Q}$. Dal momento che esistono numeri complessi trascendenti su $\mathbf{Q}$, abbiamo $\bar{\mathbf{Q}} \neq \mathbf{C}$. Chiaramente, invece, $\mathbf{C}$ è una chiusura algebrica di $\mathbf{R}$, poiché ogni numero complesso è radice di un polinomio a coefficienti reali: infatti $a + bi$ è radice di $X^2 - 2aX + (a^2 + b^2)$.

3.2. Campi finiti

Ricordiamo la definizione di *caratteristica* di un anello A: esiste un unico omomorfismo di anelli $\chi_A\colon \mathbf{Z} \to A$, definito da $\chi_A(n) = n1$, multiplo secondo n di $1 \in A$. Il nucleo di questo omomorfismo è un ideale di $\mathbf{Z}$, quindi della forma $k\mathbf{Z}$, dove $k \geq 0$. La caratteristica di A è allora questo numero k. Se k è la caratteristica di A, $ka = 0$, per ogni $a \in A$.

Sappiamo che, se A è un dominio, la sua caratteristica è zero oppure un numero primo. In particolare questo vale per un campo. Se in più sappiamo che il campo F è finito, la sua caratteristica deve essere un numero primo p: infatti l'omomorfismo χ_A non può essere iniettivo, quindi $\ker \chi_A \neq \{0\} = 0\mathbf{Z}$.

PROPOSIZIONE. *Se la caratteristica dell'anello commutativo A è un numero primo p, allora l'applicazione*

$$\begin{aligned} \Phi\colon A &\to A \\ a &\mapsto a^p \end{aligned}$$

è un omomorfismo di anelli.

DIMOSTRAZIONE. Che $\Phi(1) = 1$ e $\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b)$ è chiaro. Inoltre per il teorema del binomio

$$\Phi(a + b) = (a + b)^p = \sum_{i=1}^{p} \binom{p}{i} a^i b^{p-i}.$$

Se $0 < i < p$, abbiamo che

$$\binom{p}{i} = \frac{p!}{i!\,(p - i)!}$$

è divisibile per p, quindi $\binom{p}{i} a^i b^{p-i} = 0$. Di conseguenza $(a + b)^p = a^p + b^p$. □

Naturalmente allora anche $\Phi^2 = \Phi \circ \Phi$, ..., $\Phi^{n+1} = \Phi^n \circ \Phi$, eccetera, sono omomorfismi.

Un'altro fatto importante è che un anello commutativo di caratteristica k ha un sottoanello isomorfo a $\mathbf{Z}/k\mathbf{Z}$, precisamente l'immagine di χ_A, che si chiama *sottoanello primo* di A; nel caso in cui k è un numero primo, questo è un sottocampo.

TEOREMA. *Sia F un campo finito e sia p la sua caratteristica. Allora*

$$|F| = p^n$$

per un opportuno intero $n \geq 1$.

DIMOSTRAZIONE. Sia F_0 il sottocampo primo di F; allora $F_0 \cong \mathbf{Z}/p\mathbf{Z}$ ha p elementi. La dimensione di F come spazio vettoriale su F_0 è finita, perché F stesso è un insieme di generatori; se questa dimensione è $n = [F : F_0]$, ogni elemento di F si scrive in modo unico come combinazione lineare di n elementi a coefficienti in F_0; il numero di tali combinazioni lineari è proprio p^n. □

Il *piccolo teorema di Fermat* ammette una generalizzazione.

TEOREMA. *Sia F un campo con q elementi. Allora, per ogni $a \in F$, si ha $a^q = a$.*

DIMOSTRAZIONE. L'insieme $F \setminus \{0\}$ è, rispetto alla moltiplicazione, un gruppo con $q-1$ elementi. Perciò $a^{q-1} = 1$, per ogni $a \in F \setminus \{0\}$. Di conseguenza $a^q = a$ e l'identità vale anche per $a = 0$. □

Il teorema sull'unicità di un campo di riducibilità completa ha come conseguenza che due campi con lo stesso numero (finito) di elementi sono isomorfi. Infatti questi due campi hanno lo stesso sottocampo primo (per meglio dire sottocampi primi isomorfi, ma si possono identificare). Il polinomio $X^q - X$ ha coefficienti nel sottocampo primo; basta allora verificare che un campo con q elementi è il campo di riducibilità completa di $X^q - X$ sul sottocampo primo.

Sia dunque $F = \{a_1, a_2, \ldots, a_q\}$ un campo con q elementi. Per quanto visto prima, ogni elemento di F è radice del polinomio $f = X^q - X$; dunque f si scrive come prodotto di fattori di primo grado e certamente $F = F_0(a_1, \ldots, a_q)$, dove F_0 è il sottocampo primo.

LEMMA. *Sia F un campo di caratteristica p e sia q una potenza di p; allora il polinomio $X^q - X$ non ha radici di molteplicità ≥ 2.*

DIMOSTRAZIONE. Supponiamo che $a \in F$ sia una radice ed eseguiamo la divisione di $f = X^q - X$ per $X - a$:

$$\begin{array}{c|cccccc|c} & 1 & 0 & 0 & \ldots & 0 & -1 & 0 \\ a & & a & a^2 & \ldots & a^{q-2} & a^{q-1} & a^q - a \\ \hline & 1 & a & a^2 & \ldots & a^{q-2} & a^{q-1} - 1 & 0 \end{array}$$

Dunque il quoziente è

$$g = X^{q-1} + aX^{q-2} + a^2X^{q-3} + \cdots + a^{q-2}X + (a^{q-1} - 1)$$

e se valutiamo in a otteniamo

$$g(a) = qa^{q-1} - 1 = -1 \neq 0,$$

dal momento che q è una potenza di p. Perciò a non è una radice di g e abbiamo la tesi. □

TEOREMA. *Se $q = p^n$ è potenza di un primo p, allora esiste, a meno di isomorfismi, un unico campo con q elementi.*

DIMOSTRAZIONE. Abbiamo già osservato l'unicità. Per quanto riguarda l'esistenza, ci basta considerare di nuovo il polinomio $f = X^q - X$ a coefficienti in $\mathbf{Z}/p\mathbf{Z}$. Sia K un campo di riducibilità completa di f, che sappiamo esistere. A priori non è detto che K abbia proprio q elementi; consideriamo dunque l'insieme F delle radici di f in K. Allora F è un sottocampo di K.

Infatti $1 = 1^q \in F$; se poi $a, b \in F$, abbiamo

$$(a+b)^q = (a+b)^{p^n} = \Phi^n(a+b) = \Phi^n(a) + \Phi^n(b) = a + b$$

e lo stesso ragionamento con la moltiplicazione prova che $ab \in F$. Inoltre $(a^{-1})^q = (a^q)^{-1} = a^{-1}$, se $a \neq 0$. Per l'opposto abbiamo $(-a)^q = -a^q = -a$, se p è dispari; se invece $p = 2$, abbiamo $-a = a$, e non c'è altro da dimostrare.

Per il lemma precedente F ha q elementi, perché le sue radici in K sono tutte distinte e ne ha q per l'ipotesi che K è un campo di riducibilità completa per f. Ne segue allora che $F = K$ ha q elementi. □

Il campo con $q = p^n$ elementi, unico a meno di isomorfismi, si denota con $GF(q)$. In particolare $GF(p) = \mathbf{Z}/p\mathbf{Z}$.

Come si costruisce esplicitamente un campo con $q = p^n$ elementi? Ad esempio, supponiamo di voler determinare $GF(9)$. Secondo il teorema precedente, dobbiamo calcolare un campo di riducibilità completa di $X^9 - X$ su $GF(3)$. Prima di tutto scriviamolo come prodotto di fattori irriducibili:

$$X^9 - X = X(X-1)(X-2)(X^2+1)(X^4+1).$$

Se esaminiamo $g = X^2+1$, notiamo che è irriducibile in $GF(3)$ e quindi l'anello quoziente $GF(3)[X]/g\ GF(3)[X]$ è un campo che ha dimensione 2 su $GF(3)$ e perciò è $GF(9)$. La sua base è $\{1, b\}$, dove b ha la proprietà che $b^2 = -1$; quindi gli elementi si scrivono come $\alpha + \beta b$, con l'addizione per componenti e la moltiplicazione

$$(\alpha+\beta b)(\gamma+\delta b) = \alpha\gamma + \alpha\delta b + \beta\gamma b + \beta\delta b^2 = (\alpha\gamma - \beta\delta) + (\alpha\delta + \beta\gamma)b.$$

Le radici di X^2+1 sono $b = 0+1b$ e $-b = 0+2b$. Cerchiamo le radici di X^4+1, che sappiamo devono esistere. Si ha

$$X^4 + 1 = X^4 - b^2 = (X^2 - b)(X^2 + b).$$

Affinché $\alpha + \beta b$ sia radice di $X^2 - b$ occorre che

$$\alpha^2 - \beta^2 = 0 \qquad \text{e} \qquad 2\alpha\beta = 1.$$

Abbiamo quindi le soluzioni $1+2b$ e $2+b$. Si lascia come esercizio la verifica che gli altri due elementi $1+b$ e $2+2b$ sono proprio le radici di X^2+b.

Se prendiamo invece come polinomio irriducibile $X^2 - X - 1$ e indichiamo con c una sua radice, gli elementi di $GF(9)$ si scrivono come $\alpha + \beta c$ con moltiplicazione

$$(\alpha+\beta c)(\gamma+\delta c) = \alpha\gamma + \alpha\delta c + \beta\gamma c + \beta\delta c^2 = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma + \beta\delta)c,$$

perché c soddisfa l'identità $c^2 = 1 + c$. Questa scelta può essere più conveniente perché le potenze di c sono tutti gli elementi non nulli di $GF(9)$. Infatti

$$\begin{aligned}
c^2 &= 1 + c &&= 1 + c,\\
c^3 &= c + c^2 &&= 1 + 2c,\\
c^4 &= c + 2c^2 &&= 2,\\
c^5 &= 2c &&= 2c,\\
c^6 &= 2c^2 &&= 2 + 2c,\\
c^7 &= 2c + 2c^2 &&= 2 + c,\\
c^8 &= 2c + c^2 &&= 1.
\end{aligned}$$

Esercizio: determinare l'isomorfismo fra i campi costruiti nei due modi.

Non occorre costruire passo passo i campi $GF(p^n)$; infatti basta considerare un unico polinomio $f \in GF(p)[X]$ che abbia grado n e sia irriducibile. Un tale polinomio esiste sempre ed è determinabile in tempo finito: basta scrivere $n = i + j$ in tutti i modi possibili con $i, j \geq 1$ e calcolare tutti i prodotti dei polinomi di grado i e j in $GF(p)[X]$; quelli di grado n che non si ottengono così sono certamente irriducibili.

Vogliamo come altro esempio determinare $GF(8)$. Ci serve un polinomio $f \in GF(2)[X]$ di grado 3 e irriducibile. Una scelta possibile è $f = 1 + X + X^3$ e quindi $GF(8)$ ha come base su $GF(2)$ gli elementi 1, b e b^2, dove $1 + b + b^3 = 0$. Dunque la moltiplicazione è

$$\begin{aligned}
&(\alpha_1 + \beta_1 b + \gamma_1 b^2)(\alpha_2 + \beta_2 b + \gamma_2 b^2)\\
&= (\alpha_1\alpha_2 + \beta_1\gamma_2 + \gamma_1\beta_2) + (\alpha_1\beta_2 + \beta_1\alpha_2 + \beta_1\gamma_2 + \gamma_1\beta_2 + \gamma_1\gamma_2)b + (\alpha_1\gamma_2 + \beta_1\beta_2 + \gamma_1\alpha_2 + \gamma_1\gamma_2)b^2
\end{aligned}$$

3.3. Chiusura algebrica

Il teorema di Steinitz dice che ogni campo ammette una chiusura algebrica. La costruzione rigorosa della chiusura algebrica $GF(p^\infty)$ di $GF(p)$ richiederebbe troppo tempo, non perché sia intrinsecamente difficile, quanto perché coinvolge concetti abbastanza delicati.

Tuttavia non è necessario, per molti scopi, considerare la chiusura algebrica. Quello che basta sapere è come costruire, dato un numero finito di polinomi in $GF(p^n)[X]$, un campo che ne contenga tutte le radici. Ovviamente ci basterebbe considerare un solo polinomio f, il prodotto di quelli dati, e costruirne il campo di riducibilità completa.

Il problema è già risolto se nella decomposizione di f non compaiono fattori di grado > 1. Supponiamo allora che si trovi un fattore g di grado > 1.

(1) $F_0 = GF(p^n)$;
(2) $F_1 = F_1[X]/gF_1[X]$ è un campo in cui g ha una radice;
(3) si decompone f in fattori irriducibili in $F_1[X]$;
(4) se esiste ancora un fattore irriducibile di grado > 1 si eseguono di nuovo i passi precedenti ottenendo via via campi F_2, F_3, ..., F_l, fino a che non risultano più fattori di grado > 1.

Il procedimento ha ovviamente termine. In modo analogo si potrebbe procedere per costruire la chiusura algebrica di $GF(p)$.

(1) $F_0 = GF(p)$;
(2) si prende un polinomio irriducibile $f_1 \in F_0[X]$ di grado minimo > 1;
(3) $F_1 = F_0[X]/fF_0[X]$ è un'estensione di F_0 in cui f_1 ha una radice;
(4) si prende un polinomio irriducibile $f_2 \in F_1[X]$ di grado minimo > 1;
(5) ...

Il procedimento va ripetuto all'infinito: infatti nessun campo finito può essere algebricamente chiuso. La dimostrazione di questo fatto è analoga alla prova dell'infinità dei numeri primi.

Se $F = \{a_1, \ldots, a_q\}$ è un campo finito, si considera il polinomio

$$f = (X - a_1)(X - a_2) \ldots (X - a_q) + 1.$$

Allora nessun elemento di F è radice di f e quindi F non è algebricamente chiuso.