Dispense del corso di
ALGEBRA 1
a.a. 2007–2008

Parte 2: ANELLI E POLINOMI

Indice

Capitolo 6

Anelli

6.1 Prime proprietà.

Il termine bf anello è usato per indicare una classe di insiemi (quella che si chiama *struttura algebrica*) dotati di due operazioni, il cui modello fondamentale è l'insieme $\mathbb{Z}$ dei numeri interi (con le operazioni usuali di somma e moltiplicazione). Infatti, il concetto di anello ha la sua origine dalla teoria di numeri, ed è sorto dall'idea di astrarre le proprietà fondamentali che caratterizzano (per quanto riguarda le due operazioni fondamentali) gli insiemi di numeri (interi, reali o complessi).

Definizione. Un **anello** è un insieme A dotato di due operazioni $+$, $\cdot$ (che saranno sempre chiamate somma e prodotto), che soddisfano le seguenti proprietà:

(S1) $a + (b + c) = (a + b) + c \quad \forall a, b, c, \in A$ (associatività della somma)

(S2) $a + b = b + a$ per ogni $a, b \in A$ (commutatività della somma)

(S3) esiste $0_A \in A$ tale che, per ogni $a \in A$, $a + 0_A = a$ (elemento neutro per la somma)

(S4) per ogni $a \in A$ esiste $a' \in A$ tale che $a + a' = 0_A$ (esistenza dell'opposto)

(P1) $a(bc) = (ab)c$ per goni $a, b, c, \in A$ (associatività del prodotto)

(P2) esiste $1_A \in A$ tale che, per ogni $a \in A$, $a1_A = a = 1_A a$ (elemento neutro per il prodotto), ed inoltre $1_A \neq 0_A$

(D) Valgono le **proprietà distributive** del prodotto rispetto alla somma, ovvero, per ogni $a, b, c \in A$:

$$a(b + c) = ab + ac$$

$$(b + c)a = ba + ca \ .$$

Riferecndoci alle definizioni di monoide e di gruppo (sezione 5.1), si riconosce che gli assiomi (S1) – (S4) esprimono la richiesta che $(A, +)$ sia un gruppo commutativo, e gli assiomi (P1) – (P2) quella che $(A, \cdot)$ sia un monoide.

Sono anelli, con le usuali operazioni di somma e prodotto, gli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e C. Altri esempi importanti (per i quali facciamo riferimento ai corsi di algebra lineare) sono gli anelli di matrici quadrate $M_n(\mathbb{R})$, in questo caso le operazioni sono quella di somma (per componenti) e di prodotto righe $\times$ colonne, di matrici quadrate. Altri esempi ancora si trovano sparsi tra gli esercizi.

Dagli assiomi che definiscono la struttura di anello, seguono di fatto molte di quelle proprietà delle operazioni che utilizziamo familiarmente nel caso di anelli numerici. Le elenchiamo nelle seguenti proposizioni: la prima riguarda la somma, le non è altro che la legge di cancellazione, valida in qualsiasi gruppo; a seconda riguarda il prodotto (si osservi come sia fondamentale la proprietà distributiva)..

Proposizione 6.1. *Sia A un anello. Allora, per ogni $a, b, c \in A$,*

$$a + b = a + c \quad \Rightarrow \quad b = c.$$

In particolare, esiste un unico elemento neutro per l'addizione, che si denota sempre con 0_A e si chiama zero di A, e per ogni $a \in A$ esiste un unico elemento opposto di a, che si denota con $-a$.

Dimostrazione. Siano per ogni $a, b, c \in A$, tali che $a + b = a + c$, e sia $a' \in A$ tale che $a' + a = 0_A$. Allora

$$b = 0_A + b = (a' + a) + b = a' + (a + b) = a' + (a + c) = (a' + a) + c = 0_A + c = c.$$

Supponiamo ora che $0'_A$ sia un elemento neutro per la somma; allora

$$0'_A = 0'_A + 0_A = 0_A.$$

Infine se a' e a'' sono opposti dell'elemento a, allora $a + a' = 0_A = a + a''$, e quindi, per quanto provato sopra, $a' = a''$. ∎

Se a e b sono elementi dell'anello A, si adotta la seguente notazione: $a - b = a + (-b)$.

Proposizione 6.2. *Sia A un anello, e siano $a, b \in A$. Allora*

1. *esiste un unico elemento neutro per il prodotto.*
2. $a0_A = 0_A a = 0_A$.
3. $a(-b) = -(ab) = (-a)b$.
4. $(-a)(-b) = ab$.

Dimostrazione. 1) Siano 1_a e $1'_A$; allora, analogamente a quanto visto per l'addizione

$$1'_A = 1'_A \cdot 1_A = 1_A.$$

2) Sia $c = a0_A$. Allora, applicando la proprietà distributiva:

$$c = a0_A = a(0_A + 0_A) = a0_A + a0_A = c + c$$

e quindi $c = c + c - c = c - c = 0_A$. Analogamente si dimostra che $0_A a = 0_A$.

3) Proviamo che $a(-b) = -(ab)$. Applicando la proprietà distributiva ed il punto 1):

$$a(-b) + ab = a(-b + b) = a0_A = 0_A$$

e quindi, $a(-b) = -(ab)$. Analogamente si dimostra che $(-a)b = -(ab)$.

4) Per il punto 2) si ha $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. ∎

Attenzione. In alcuni testi, la definizione di anello viene data senza richiedere l'esistenza dell'elemento neutro per la moltiplicazione (cioè senza inculdere l'assioma (P2)). Da questo punto di vista, un anello nel senso che invece adottiamo noi viene chiamato **anello con unità**. Ribadisco quindi che, secondo la definizione da noi adottata, un anello A ha **sempre** l'unità 1_A. Un anello R si dice *degenere* se $0_R = 1_R$; in tal caso (lo si dimostri), R è costituito dal solo elemento 0_R. Con il termine *anello* noi intenderemo **sempre** un *anello non degenere*, quindi tale che $0_R \neq 1_R$.

Esercizio 6.1. Sia A un insieme dotato di due operazioni $+$, $\cdot$ che soddisfano le condizioni (S1),(S3),(S4), (P1),(P2),(D). Provare che A è un anello.

Definizione. Un anello A si dice **commutativo** se il prodotto è commutativo, ovvero se, per ogni $a, b \in A$ si ha $ab = ba$.

Sono commutativi gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, mentre non sono commutativi gli anelli di matrici $M_n(\mathbb{R})$, con $n \geq 2$.

Potenze. Anche per un generico anello è possibile definire l'elevazione a potenza per un intero positivo, nella stessa maniera in cui si fa per gli interi. Sia quindi A un anello. Allora, per ogni $a \in A$ e per ogni $n \in \mathbb{N}$, la potenza n-esima a^n di a si definisce induttivamente nella maniera seguente:

$$a^0 = 1_A \qquad \text{e} \qquad a^{n+1} = a^n a.$$

In pratica, se $n \in \mathbb{N}$,

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{\text{n volte}}$$

Come nel caso degli interi è facile verificare le proprietà delle potenze.

Proposizione 6.3. *Sia A un anello, $a \in A$, e siano $n, m \in \mathbb{N}$. Allora*

(i) $a^{n+m} = a^n a^m$

(ii) $a^{nm} = (a^n)^m$

Dimostrazione. (i) Procediamo per induzione su $m \in \mathbb{N}$. Se $m = 0$, si ha $a^{n+0} = a^n = a^n \cdot 1_A = a^n a^0$.

Sia ora $m \geq 0$, e per ipotesi induttiva, sia $a^{n+m} = a^n a^m$. Allora,

$$\begin{aligned} a^{n+(m+1)} &= a^{(n+m)+1} = a^{n+m}a \qquad \text{(per definizione)} \\ &= (a^n a^m)a \qquad\qquad \text{(per ipotesi induttiva)} \\ &= a^n(a^m a) = a^n a^{m+1} \qquad \text{(per definizione).} \end{aligned}$$

(ii) La dimostrazione di questo punto è lasciata per esercizio: si proceda ancora per induzione su m, utilizzando anche il punto (i). ∎

Osservazione. In generale, in un anello (non commutativo) A, non è detto che, dati $a, b \in A$ e $n \in \mathbb{N}$, valga $(ab)^n = a^n b^n$ (vedi l'esercizio 7.9). Tuttavia, non è difficile provare che se $ab = ba$ allora si ha, per ogni $n \in \mathbb{N}$, $(ab)^n = a^n b^n$.
In particolare, questa ulteriore proprietà delle potenze sussiste negli anelli commutativi, ai quali non è difficile estendere quindi il Teorema del binomio di Newton. Precisamente

Proposizione 6.4. *Sia A un anello commutativo, e siano $a, b \in A$. Allora per ogni $n \in \mathbb{N}$,*

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

Un'altra semplice identità, riguardante le potenze, che vale in qualsiasi anello, è quella riguardante le somme di serie geometriche: *sia A anello, $a \in A$, e $1 \leq n \in \mathbb{N}$; allora*

$$a^n - 1 = (a-1)(a^{n-1} + \ldots + a + 1).$$

Multipli interi. Si sarà osservato come, nell'enunciato della proposizione 6.4, sia stato dato un senso anche ad una scrittura del tipo na per $a \in A$, e $n \in \mathbb{N}$ (infatti i coefficienti binomiali che compaiono nella formula sono numeri interi). Questo va definito, ed è il corrispondente per la somma di quello che le potenze sono rispetto al prodotto (e si può fare con interi anche negativi).
Se A è un anello, $a \in A$ e $n \in \mathbb{N}$, si scrive

$$\begin{aligned} &0a = 0_A; \\ &na = a + a + \ \ldots \ + a \qquad \text{(n volte);} \\ &(-n)a = n(-a) = -(na). \end{aligned}$$

L'elemento na si chiama il *multiplo n-esimo* di a.

In modo del tutto analogo a quanto visto per il prodotto, si prova facilmente che, per ogni $a, b \in A$ ed ogni $m, n \in \mathbb{Z}$,

$$(n+m)a = na + ma \qquad (nm)a = n(ma) \qquad m(a+b) = ma + mb.$$

Il concetto di *sottoanello* S di un anello A si presenta in modo naturale.

Definizione. Un sottoinsieme non vuoto S di un anello A si dice **sottoanello** di A se soddisfa alle seguenti condizioni

(1) $a - b \in S$, per ogni $a, b \in S$;

(2) $ab \in S$, per ogni $a, b \in S$ e $1_A \in S$.

Se S è un sottoanello di A, allora è chiaro che in S sono soddisfatte le proprietà distributive (in quanto casi particolari delle proprietà analoghe di A). Quindi S risulta, con le operazioni indotte da A, un anello esso stesso, con la stessa unità di A ($1_S = 1_A$). Similmente, un sottoanello di un anello commutativo è un anello commutativo.

Esempi. 1) Conviene subito mostrare che anche negli anelli che ci sono maggiormente usuali, si trovano numerosi sottoanelli. Ad esempio, consideriamo il seguente sottoinsieme di $\mathbb{R}$

$$\mathbb{Q}[\sqrt{2}] = \{\ a + b\sqrt{2} \mid a, b \in \mathbb{Q}\ \}\ ,$$

e verifichiamo che è un sottoanello dell'anello $\mathbb{R}$. Infatti, se $x = a + b\sqrt{2},\ y = c + d\sqrt{2}$ sono due elementi di $\mathbb{Q}[\sqrt{2}]$ (quindi $a, b, c, d \in \mathbb{Q}$), allora $x - y = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, e $xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$; infine $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Come vedremo più avanti, sottoanelli di questo tipo sono piuttosto importanti e si possono individuare a partire da un qualunque altro numero reale o complesso al posto di $\sqrt{2}$.

2) Introduciamo ora un anello che useremo spesso per illustrare diversi aspetti della teoria. Consideriamo l'insieme $\mathbb{R}^{\mathbb{R}}$ di tutte le applicazioni dall'insieme dei numeri reali in se stesso, con le abituali operazioni di somma e moltiplicazione di funzioni reali. Quindi, se $f, g \in \mathbb{R}^{\mathbb{R}}$ allora $f + g$ e fg sono definite da

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x) \end{aligned}$$

per ogni $x \in \mathbb{R}$ (attenzione: qui il prodotto non è la composizione di applicazioni). Si verifica facilmente che, con tali operazioni, $\mathbb{R}^{\mathbb{R}}$ è un anello commutativo, il cui zero ed uno sono, rispettivamente, le funzioni costanti c_0 e c_1 definite da, per ogni $x \in \mathbb{R},\ c_0(x) = 0,\ c_1(x) = 1$. Se denotiamo con $\mathcal{C}(\mathbb{R})$ il sottoinsieme di $\mathbb{R}^{\mathbb{R}}$ costituito dalle applicazioni *continue*, allora noti teoremi di Analisi assicurano che $\mathcal{C}(\mathbb{R})$ è un sottoanello di $\mathbb{R}^{\mathbb{R}}$.

3) Anelli che godono di proprietà piuttosto singolari sono gli anelli delle parti. Sia X un insieme non vuoto. Allora l'insieme delle parti $\mathcal{P}(X)$ con le operazioni di differenza simmetrica Δ (come somma) e intersezione $\cap$ (come prodotto) è un anello (lo si provi per esercizio, usando le proprietà di queste operazioni descritte nella sezione 1.2), con $0_{\mathcal{P}(X)} = \emptyset$ e $1_{\mathcal{P}(X)} = X$.

Concludiamo questa sezione osservando che, se A è un anello, e U, V sono sottoinsiemi non vuoti di A, è possibile definire la "somma" di U e V, nel modo seguente

$$U + V = \{\ x + y \mid x \in U,\ y \in V\ \}.$$

$U + V$ è quindi ancora un sottoinsieme non vuoto di A.

Esercizio 6.2. Si completi la dimostrazione della proposizione 6.3, e quella dell'osservazione seguente.

Esercizio 6.3. Sia $S = \{\ (x, y) \mid x, y \in \mathbb{R}\ \}$. Su S definiamo addizione e moltiplicazione ponendo, per ogni $(a, b), (c, d) \in S$:

$$(a, b) + (c, d) = (a + c, b + d) \qquad (a, b)(c, d) = (ac, ad + bc)\ ,$$

Si provi che, con tali operazioni, S è un anello commutativo, determinando esplicitamente 0_S e 1_S.

Esercizio 6.4. Sia p un numero primo fissato e sia

$$\mathbb{Q}_p = \Big\{ \frac{m}{p^i} \;\Big|\; m \in \mathbb{Z}\ , i \in \mathbb{N} \Big\}.$$

Si provi che $\mathbb{Q}_p$ è un sottoanello dell'anello $\mathbb{Q}$ dei numeri razionali.

Esercizio 6.5. Sia R un anello. Si provi che $Z(R) = \{a \in R \mid ab = ba\ \forall b \in R\}$ è un sottoanello di R. ($Z(R)$ è detto il centro di R).

6.2 Tipi di anello.

Nella Proposizione 6.2 abbiamo provato alcune proprietà degli anelli, che per $\mathbb{Z}$ siamo abituati a considerare naturali. Ora, $\mathbb{Z}$ soddisfa anche altre proprietà, quali il fatto che il prodotto di due elementi diversi da zero è diverso da zero. Il motivo per cui questa proprietà non compare nella proposizione 6.2, è che essa non discende dagli assiomi di anello; anzi, esistono anelli in cui essa non vale.

Un elemento a di un anello A si dice **divisore dello zero** se $a \neq 0_A$ ed esiste $b \neq 0_A$ tale che $ab = 0_A$.

Un primo esempio di di divisori dello zero si può trovare negli anelli di matrici; ad esempio, in $M_2(\mathbb{R})$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Definizione. Un anello commutativo privo di divisori dello zero si dice un **Dominio d'integrità**.

Quindi, gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono domini d'integrità, mentre l'anello delle matrici $M_2(\mathbb{R})$ non lo è. Un esempio di anello commutativo che non è un dominio d'integrità è l'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ (vedi pagina seguente).

Proposizione 6.5. (Legge di cancellazione). *Sia A un dominio d'integrità. Allora, per ogni $a, b \in A, 0_A \neq c \in A$:*

$$ac = bc \qquad \Rightarrow \qquad a = b\ .$$

Dimostrazione. Siano $a, b \in A,\ 0_A \neq c \in A$ con $ac = bc$. Allora $0_A = ac - bc = (a-b)c$. Poichè A è privo di divisori dello zero e $c \neq 0_A$, deve essere $a - b = 0_A$, cioè $a = b$. ∎

Un elemento a di un anello A si dice un **invertibile** di A se esiste un elemento $b \in A$ tale che $ab = 1_A = ba$.

Come abbiamo dimostrato nel caso delle applicazioni, ed in generale per i monidi (Proposizione 5.2) si prova immediatamente che un elemento invertibile a di un anello A ha un unico inverso.

Proposizione 6.6. *Sia A un anello, e sia a un elemento invertibile di A. Allora esiste un unico $b \in A$ tale che $ab = 1_A = ba$ (che si denota con $b = a^{-1}$).*

L'insieme di tutti gli elementi invertibili di un anello A lo denoteremo con $U(A)$. Chiaramente, $U(A) \neq \emptyset$ dato che $1_A \in U(A)$. Ad esempio, gli elementi invertibili dell'anello $\mathbb{Z}$ sono 1 e -1, quindi $U(\mathbb{Z}) = \{1, -1\}$; gli elementi invertibili dell'anello delle matrici $M_n(\mathbb{R})$ sono le matrici con determinante diverso da 0; gli elementi invertibili dell'anello $\mathbb{Q}$ sono tutti i numeri razionali diversi da 0, quindi $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$.

Esempio. L'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ non è un dominio d'integrità, e neppure il sottoanello delle funzioni continue $\mathcal{C}(\mathbb{R})$; ad esempio, se f, g sono le funzioni definite da

$$f(x) = \begin{cases} 0 & \text{se} \quad x \leq 0 \\ x & \text{se} \quad x \geq 0 \end{cases} \qquad g(x) = \begin{cases} x & \text{se} \quad x \leq 0 \\ 0 & \text{se} \quad x \geq 0 \end{cases}$$

allora f, g sono funzioni continue, diverse dalla funzione zero, il cui prodotto è la funzione zero (che, ricordo, è l'elemento 0 dell'anello $\mathbb{R}^{\mathbb{R}}$.
Ricordando poi che l'identità dell'anello $\mathbb{R}^{\mathbb{R}}$ è la costante 1, si ottiene immediatamente che gli elementi invertibili sono tutte e sole le funzioni $f \in \mathbb{R}^{\mathbb{R}}$ tali che $f(x) \neq 0$ per ogni $x \in \mathbb{R}$.

Esercizio 6.6. SI provi che nell'anello $\mathbb{R}^{\mathbb{R}}$ ogni elemento diverso da 0 è invertibile oppure un è un divisore dello zero. Si rifletta se la stessa affermazione vale per l'anello $\mathcal{C}(\mathbb{R})$ delle funzionin continue.

Definizione. Un anello commutativo A si dice un **campo** se ogni suo elemento non nullo è un invertibile.

Ad esempio sono campi gli anelli $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Si vede facilmente che la famiglia dei campi è una sottofamiglia di quella dei domini d'integrità (propria: ad esempio $\mathbb{Z}$ è un dominio d'integrità ma non un campo).

Proposizione 6.7. *Ogni campo è un dominio d'integrità.*

Dimostrazione. Sia F un campo e $0_F \neq a \in F$. Supponiamo che $b \in F$ sia tale che $ab = 0_F$. Allora $b = 1_F b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0_F = 0_F$, quindi a non è un divisore dello zero. ∎

Esercizio 6.7. Provare che ogni dominio d'integrità finito è un campo.

Soluzione. Sia R un dominio d'integrità finito, e sia $0_R \neq a \in R$. Consideriamo l'applicazione $\lambda_a : R \to R$, definita da $\lambda_a(x) = ax$ per ogni $x \in R$. Siano ora $x, y \in R$ tali che $\lambda(x) = \lambda(y)$, allora $ax = ay$ che, per la legge di cancellazione, implica $x = y$. Dunque λ_a è iniettiva; poichè R è un insieme finito, λ_a è anche suriettiva. In particolare esiste $b \in R$ tale che $1_R = \lambda(b) = ab$. Essendo R commutativo, $ab = 1_R = ba$, quindi a è invertibile. Dunque R è un campo.

Prodotto diretto. Siano A e B anelli. Sull'insieme $A \times B$ si definiscono operazioni di somma e prodotto ponendo, per ogni $(a,b),(a',b') \in A \times B$,

$$(a,b)+(a',b') = (a+a', b+b') \qquad \text{e} \qquad (a,b)\cdot(a',b') = (aa', bb').$$

Si verifica facilmente (lo si svolga come esercizio) che, con le operazioni così definite, $A \times B$ è un anello, che si chiama anello *prodotto diretto* degli anelli A e B. Chiaramente, $0_{A\times B} = (0_A, 0_B)$ e $1_{A\times B} = (1_A, 1_B)$.
Inoltre, $A \times B$ è commutativo se e solo se A e B sono commutativi; mentre si provi per esercizio che $A \times B$ non è mai un dominio d'integrità.

Un elemento e di un anello A si dice **idempotente** se $e^2 = e$. In ogni anello A, 1_A e 0_A sono idempotenti. Se A è un dominio d'integrità questi sono i suoi soli elementi idempotenti, infatti se $e \in A$ è idempotene, allora $e^2 = e$ e quindi $e(e-1) = 0$ (se A è un dominio d'integrità, ciò forza $e \in \{0_A, 1_A\}$). Per trovare elementi idempotenti non-banali, possiamo ad esempio considerare il prodotto diretto $\mathbb{Z} \times \mathbb{Z}$; in tale anello (che è commutaivo) gli elementi idempotenti sono $(0,0),(1,1),(0,1)$ e $(1,0)$.

Proposizione 6.8. *Sia R anello in cui ogni elemento è idempotente; allora $-1_R = 1_R$ e R è commutativo.*

Dimostrazione. Sia R come nelle ipotesi, e sia $a \in R$. Allora

$$-a = (-a)^2 = (-a)(-a) = a^2 = a;$$

in particolare $-1_R = 1_R$. Inoltre, per ogni $a, b \in R$ si ha

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

da cui segue $ab + ba = 0$ e dunque, per quanto visto sopra $ba = -(ab) = ab$. Quindi R è commutativo. ∎

Un anello in cui ogni elemento è idempotente si chiama **anello di Boole**. I casi fondamentali di anelli di Boole sono gli anelli delle parti, ovvero gli anelli del tipo $(\mathcal{P}(X), \Delta, \cap)$ (con X insieme non vuoto): infatti, per ogni elemento Y di un tale anello (quindi $Y \subseteq X$) si ha $Y^2 = Y \cap Y = Y$.
Diversamente dai domini d'integrità e dai campi, gli anelli di Boole non saranno oggetto di ulteriore approfondimento in questo corso; li abbiamo citati per la loro rilevanza nelle applicazioni alla logica e all'informatica.

Un elemento a di un anello R si dice **nilpotente** se esiste un intero $n \geq 1$ (che dipende in genere da a) tale che $a^n = 0_R$. Un esempio di elemento nilpotente non nullo lo troviamo, ad esempio, nell'anello di matrici $M = M_2(\mathbb{R})$:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_M.$$

Esempi di elementi nilpotenti $\neq 0$ in anelli commutativi li incontreremo più avanti (vedi Esercizio 7.7). Per il momento, osserviamo i due fatti seguenti:

1) In un dominio di integrità R il solo elemento nilpotente è 0_R.

2) Sia a un elemento nilpotente dell'anello R. Allora $1-a$ è un elemento invertibile. Infati, se per $a \in R$ e $1 \leq n \in \mathbb{N}$ si ha $a^n = 0$, allora

$$1 = 1 - a^n = (1-a)(1 + a + a^2 + \ldots + a^{n-1}).$$

Esercizio 6.8. Sia S l'anello dell'esercizio 6.3. Si determinino gli elementi invertibili di S e si dica se S è un dominio di integrità.

Esercizio 6.9. Sia A un dominio d'integrità, e $a \in A$. Si provi che se esistono interi positivi coprimi n, m tali che $a^n = a^m$ allora $a = 1_A$.

Esercizio 6.10. Si provi che l'anello $\mathbb{Q}[\sqrt{2}]$ è un campo.

Esercizio 6.11. Si determinino gli elementi invertibili e i divisori dello zero nell'anello $\mathbb{Z} \times \mathbb{Z}$.

Esercizio 6.12. Sia A un anello commutativo, e $a, b \in A$. Si provi che

(1) Se a è invertibile e b è nilpotente, allora $a+b$ è invertibile.

(2) Se a è divisore dello zero, b è nilpotente e $a+b \neq 0_A$, allora $a+b$ è divisore dello zero.

6.3 Ideali.

Gli ideali costituiscono il tipo più importante di sottoinsieme di un anello, e uno dei singoli argomenti più importanti di questo corso. Ecco la definizione.

Sia A un anello. Un **ideale** di A è un sottoinsieme <u>non vuoto</u> I di A che gode delle seguenti proprietà:

(i) $a - b \in I$ per ogni $a, b \in I$;

(ii) $ax \in I,\ xa \in I$ per ogni $a \in I,\ x \in A$.

Osserviamo subito che la proprietà (i), assieme alla richiesta che I non sia vuoto, comporta che *ogni ideale di A contiene* 0_A. Notiamo anche che ogni anello A ammette almeno due ideali; l'ideale *improprio* A e l'ideale *nullo o banale* $\{0_A\}$.

Esempio. Sia $\mathbb{R}^{\mathbb{R}}$ l'anello delle applicazioni dall'insieme dei numeri reali in se stesso definito nella sezione 6.1. Sia $a \in \mathbb{R}$ un numero reale fissato. Allora $Z_a = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\}$ è un ideale di $\mathbb{R}^{\mathbb{R}}$. Infattti

1) $Z_a \neq \emptyset$ (la costantte 0 appartiene a Z_a);

2) se $f_1, f_2 \in Z_a$ allora $(f_1 - f_2)(a) = f(_1a) - f_2(a) = 0 - 0 = 0$ e dunque $f_1 - f_2 \in Z_a$,

3) se $f \in Z_a$ e $g \in \mathbb{R}^{\mathbb{R}}$, allora $fg(a) = f(a)g(a) =) \cdot g(a) = 0$ e dunque $fg \in Z_a$, similmente si ha $gf \in Z_a$.

Ideali di $\mathbb{Z}$. Un caso molo importante riguarda l'anello degli interi $\mathbb{Z}$, i cui ideali si descrivono facilmente. Infatti, sia fissato un intero $n \geq 0$; allora l'insieme di tutti i multipli interi di n, ovvero

$$n\mathbb{Z} = \{\ nz \mid z \in \mathbb{Z}\ \}$$

è un ideale di $\mathbb{Z}$ (un facile esercizio). La cosa rilevane è che vale il viceversa.

Teorema 6.9. *Gli ideali dell'anello $\mathbb{Z}$ dei numeri interi, sono tutti e soli i sottoinsiemi del tipo $n\mathbb{Z}$ con $n \geq 0$.*

Dimostrazione. Per quanto osservato prima, è sufficiente provare che ogni ideale di $\mathbb{Z}$ è del tipo $n\mathbb{Z}$. Sia dunque I un ideale di $\mathbb{Z}$. Se $I = \{0\}$ allora $I = 0\mathbb{Z}$.
Supponiamo quindi che $I \neq \{0\}$. Allora esiste $0 \neq a \in I$; poichè I è un ideale, si ha anche $-a \in I$. Ora, uno di questi due elementi di I è un numero positivo non nullo, quindi l'insieme

$$\mathcal{S} = \{\ m \in I \mid m > 0\ \}$$

è un sottoinsieme non vuoto dei numeri naturali. Sia $n = min(\mathcal{S})$. Proviamo che $I = n\mathbb{Z}$.
Poichè $n \in I$ ed I è un ideale, I contiene tutti i multipli di n, cioè $n\mathbb{Z} \subseteq I$. Viceversa, sia $b \in I$; poichè $n \neq 0$ possiamo dividere b per n; esistono cioè $q, r \in \mathbb{Z}$ tali che

$$b = nq + r \qquad \text{e} \qquad 0 \leq r < n\ .$$

Ora, $nq \in I$ per quanto osservato sopra, e quindi

$$r = b - nq \in I\ ;$$

se fosse $r > 0$ allora $r \in \mathcal{S}$ e quindi, per la scelta di $n = min(\mathcal{S})$, sarebbe $n \leq r$ che contraddice la proprietà del resto. Dunque $r = 0$, cioè $b = nq \in n\mathbb{Z}$. Quindi $I \subseteq n\mathbb{Z}$ e pertanto $I = n\mathbb{Z}$. ∎

Ideali Principali. Sia A un anello *commutativo* e sia $a \in A$; allora l'insieme

$$(a) = \{ax \mid x \in A\}$$

è un ideale di A.
Infatti, $0_A = a0_A \in (a)$ e quindi $(a) \neq \emptyset$; se $u = ax, w = ay \in (a)$ (con $x, y \in A$) allora $u - w = ax - ay = a(x - y) \in (a)$; infine se $u = ax \in (a)$ e $y \in A$, allora $y(ax) = (ax)y = a(xy) \in (a)$ (osservate come la commutatività di A sia essenziale in questo punto).

Un ideale del tipo (a) di un anello commutativo A si dice **ideale principale** generato da (a), ed è il minimo ideale di A che contiene l'elemento a (nel senso generale che vedremo tra breve). In particolare, l'ideale nullo e quello improprio di qualsiasi anello commutativo A sono principali, infatti si ha $(0_a) = \{0_a\}$ e $(1_A) = A$.

Osserviamo quindi che tutti gli ideali dell'anello $\mathbb{Z}$ sono principali (infatti, per ogni $n \geq 0$, $n\mathbb{Z}$ è l'ideale principale generato da n, cioè $n\mathbb{Z} = (n)$). Non tutti gli anelli commutativi godono di questa proprietà.

Esempio. Nell'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ consideriamo il sottoinsieme

$$I = \{f \in \mathbb{R}^{\mathbb{R}} \mid \exists r_f \in \mathbb{R} \text{ tale che } f(x) = 0 \text{ per ogni } x \geq r_f\}.$$

I è un ideale di $\mathbb{R}^{\mathbb{R}}$ (lo si verifichi per esercizio), ma non è principale. Infatti, sia $f \in I$ e poniamo $r = r_f$, allora per ogni $g \in \mathbb{R}^{\mathbb{R}}$ si ha, per ogni $x \geq r$. $fg(x) = f(x)g(x) = 0 \cdot g(x) = 0$. Consideriamo ora $h \in \mathbb{R}^{\mathbb{R}}$ definita da, per ogni $x \in \mathbb{R}$,

$$h(x) = \begin{cases} 1 & \text{se} \quad x < r+1 \\ 0 & \text{se} \quad x \geq r+1. \end{cases}$$

Allora $h \in I$, ma, per quanto osservato prima, $h \notin (f)$. Questo prova che I non è un ideale principale.

Esercizio 6.13. Sia $a \in \mathbb{R}$; si provi che l'ideale $Z_a = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\}$ è un ideale principale di $\mathbb{R}^{\mathbb{R}}$.

Soluzione. Sia $g \in \mathbb{R}^{\mathbb{R}}$ definita da, per ogni $x \in \mathbb{R}$,

$$g(x) = \begin{cases} 1 & \text{se} \quad x \neq a \\ 0 & \text{se} \quad x = a. \end{cases}$$

Allora $Z_a = (g)$. Infatti $g \in Z_a$, e se $f \in Z_a$, si ha $f = gf$ (come si vede subito tenendo conto che $f(a) = 0$).

Per altre proprietà degli ideali di $\mathbb{R}^{\mathbb{R}}$ si vedano gli esercizi 6.38 e 6.40.

Un dominio d'integrità in cui ogni ideale è principale si chiama **dominio a ideali principali** (abbreviato: P.I.D.). Dunque $\mathbb{Z}$ è un dominio ad ideali principali. Esempi di domini d'integrità che non sono a ideali principali li vedremo più avanti nel corso.

Il concetto di generazione di ideali si estende agli anelli non necessariamente commutativi, ed a più di un generatore.
Infatti, si vede immediatamente che, se I, J sono ideali di un anello A, allora anche $I \cap J$ è un ideale di A. Più in generale, se $\mathcal{F}$ è una famiglia di ideali di A, allora

$$\bigcap_{I \in \mathcal{F}} I$$

è un ideale di A.
Dunque, dato un sottoinsieme X di un anello A, l'intersezione di tutti gli ideali che contengono X è un ideale, che è detto *ideale generato da* X e che si denota con (X). Se $X = \{a_1, \ldots, a_n\}$ è un sottoinsieme finito di A, si scrive di solito $(X) = (a_1, \ldots, a_n)$ (trascurando, cioè, le graffe) e si dice che (X) è un ideale *finitamente generato*. Nel caso in cui A è commutativo e $X = \{a\}$, l'ideale generato da X è proprio l'ideale principale generato da a. Sempre nel caso commutativo non è difficile descrivere gli elementi di un ideale finitamente generato:

Esercizio 6.14. Sia A un anello commutativo e $a, b \in A$. Sia (a, b) l'ideale di A generao da $\{a, b\}$. Si provi che

$$(a, b) = \{ax + by \mid x, y \in A\}.$$

In generale, se $a_1, \ldots, a_n \in A$, allora $(a_1, \ldots, a_n) = \{a_1x_1 + \ldots + a_nx_n \mid x_1, \ldots, x_n \in A\}$.

Se A non è commutativo, la descrizione dell'ideale generato anche da un singolo elemento è più complicata. Infatti, se $a \in A$, allora l'ideale generato da a deve contenere tutti gli elementi del tipo $x_1 a y_1 + \dots x_n a y_n$, al variare di $1 \leq n \in \mathbb{N}$, e $x_1, y_1, \dots, x_n, y_n \in A$.

L'unione insiemistica di due ideali non è in genere un ideale (vedi esercizio 6.15). Per ottenere un ideale che contenga due ideali dati I e J di un anello A, occorre sommare i due ideali secondo la definizione alla fine della sezione 6.1.

Proposizione 6.10. *Siano I e J sono ideali di un anello A, Allora*

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

è un ideale di A, ed è il più piccolo ideale che contiene $I \cup J$.

Dimostrazione. Intanto $I + J$ non è vuoto dato che tali sono I e J. Siano ora $a, a' \in I$ e $b, b' \in J$, allora

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I + J,$$

dato che $a - a' \in I$ e $b - b' \in J$. Similmente se $a \in I$, $b \in J$ e $x \in A$, allora $ax, xa \in I$ e $bx, xb \in J$, e quindi

$$(a + b)x = ax + bx \in I + J \quad \text{e} \quad x(a + b) = xa + xb \in I + J.$$

Dunque $I + J$ è un ideale di A. Infine, per definizione di ideale, ogni ideale che contiene I e J deve necessariamente contenere $I + J$; quindi $I + J$ è il più piccolo ideale di A che contiene sia I che J. ∎

A questo punto, ci poniamo la questione di descrivere gli ideali degli anelli $\mathbb{Q}, \mathbb{R}$ e C. Tali anelli sono campi, e per i campi la descrizione degli ideali è molto semplice e assolutamente generale: come vediamo subito, gli ideali di un campo sono soltanto l'ideale nullo e quello improprio (in particolare, quindi, i campi sono domini a ideali principali). Inoltre, nell'ambito degli anelli commutativi, questa proprietà è caratteristica dei campi.

Lemma 6.11. *Sia I un ideale dell'anello R. Se I contiene un elemento invertibile allora $I = R$.*

Dimostrazione. Sia I un ideale di R e supponiamo che esista un elemento invertibile a di R contenuto in I. Sia $x \in R$; allora, per la proprietà (ii) degli ideali, $x = x1_R = x(a^{-1}a) = (xa^{-1})a \in I$. Dunque $R \subseteq I$, e quindi $R = I$. ∎

Teorema 6.12. *Sia R un anello commutativo. Allora R è un campo se e solo se i soli ideali di R sono $\{0_R\}$ e R.*

Dimostrazione. ($\Rightarrow$) Sia R un campo, e sia I ideale di R con $I \neq \{0_R\}$. Allora I contiene un elemento $a \neq 0_R$. Poichè R è un campo, a è invertibile e quindi, per il Lemma precedente, $I = R$.

($\Leftarrow$) Viceversa, supponiamo che R sia un anello commutativo i cui soli ideali sono $\{0_R\}$ e R. Sia $0_R \neq a \in R$ e consideriamo l'ideale principale $(a) = \{ ax \mid x \in R \}$ generato da a. Poichè $(a) \neq \{0_R\}$, deve essere $(a) = R$. In particolare, $1_R \in (a)$, cioè esiste $b \in R$ tale che $1_R = ab$; poichè R è commutativo, concludiamo che a è invertibile. Ciò vale per qualunque $0_R \neq a \in R$ e dunque R è un campo. ∎

Questo Teorema non vale per anelli non commutativi; vedremo nella sezione 7.2 che l'anello di matrici $M_2(\mathbb{R})$, che è ben lontano dall'essere un campo, ha due soli ideali (quello banale e quello improprio).

Esercizio 6.15. Siano I e J ideali dell'anello A. Si provi che se $I \cup J$ è un ideale allora $I \subseteq J$ oppure $J \subseteq I$.

Esercizio 6.16. Siano n e m interi positivi. Si provi che $n\mathbb{Z} \subseteq m\mathbb{Z}$ se e solo se m divide n. Si deduca che

$$n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z} \quad \text{e} \quad n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}.$$

Esercizio 6.17. Sia u un elemento invertibile dell'anello commutativo R. Si provi che $(ua) = (a)$ per ogni $a \in R$.

Esercizio 6.18. Siano a, b elementi di una anello A (non necessariamente commutativo. Si provi che $(a, b) = (a) + (b)$.

Esercizio 6.19. Sia R un anello commutativo; si provi che l'insieme degli elementi nilpotenti di R è un ideale.

Esercizio 6.20. Siano R, S anelli. Si provi che i sottoinsiemi $\{(a, 0_S) \mid a \in R\}$ e $\{(0_R, x) \mid x \in S\}$ sono ideali di $R \times S$. Si determinino quindi tutti gli ideali dell'anello $\mathbb{R} \times \mathbb{R}$.

6.4 Omomorfismi e isomorfismi.

Definizione. 1) Siano R ed S anelli. Un **omomorfismo** (di anelli) di R in S è una applicazione $\phi : R \to S$ tale che:

(i) $\phi(a + b) = \phi(a) + \phi(b)$ per ogni $a, b \in R$;

(ii) $\phi(ab) = \phi(a)\phi(b)$ per ogni $a, b \in R$;

(iii) $\phi(1_R) = 1_S$.

2) Un **isomorfismo** tra anelli è un **omomorfismo biettivo**.

Due anelli R ed S si dicono **isomorfi** se esiste un isomorfismo da R in S. In tal caso scriveremo $R \simeq S$. Da un punto di vista algebrico astratto, due anelli isomorfi sono considerai come "lo stesso" anello: l'isomorfismo trasferisce infatti tutte le proprietà

algebriche (cioè derivanti dalle sole operazioni che lo definiscono come anello) da uno dei due anelli all'altro (come ad esempio è illustrato dal Lemma 6.13).
Un endomorfismo di un anello R è un omomorfismo da R in se stesso; mentre un isomorfismo di R in se stesso si dice **automorfismo** di R.

Esempi. 1) Il coniugio $\mathbb{C} \to \mathbb{C}$ che ad ogni $z = x + iy \in \mathbb{C}$ $(x, y \in \mathbb{R})$ associa $\overline{z} = x - iy$ è un automorfismo del campo $\mathbb{C}$.

3) Consideriamo le applicazioni $\phi_1, \phi_2 : \mathbb{R} \to M_2(\mathbb{R})$ definite da, per ogni $a \in \mathbb{R}$

$$\phi_1(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \qquad \phi_2(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

Per $i = 1, 2$, ed ogni $a, b \in \mathbb{R}$ si ha $\phi_i(a + b) = \phi_i(a) + \phi_i(b)$ e $\phi_i(ab) = \phi_i(a)\phi_i(b)$; ma ϕ_1 è un omomorfismo dato che $\phi_1(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{M_2(\mathbb{R})}$, mentre ϕ_2 non è un omomorfismo dato che $\phi_2(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq 1_{M_2(\mathbb{R})}$.

Lemma 6.13. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

(i) $\phi(0_R) = 0_S$ e, per ogni $a \in R$, $\phi(-a) = -\phi(a)$;

(ii) se $a \in R$ è invertibile, $\phi(a)$ è invertibile in S e $\phi(a)^{-1} = \phi(a^{-1})$.

(iii) $\phi(a^n) = (\phi(a))^n$, per ogni $a \in R$ e ogni $n \in \mathbb{N}$.

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo di anelli.

(i) Denotiamo con $e = \phi(0_R)$. Allora

$$e + e = \phi(0_R + 0_R) = \phi(0_R) = e = e + 0_S$$

e quindi $e = 0_S$.
Sia ora $a \in R$; allora

$$\phi(a) + \phi(-a) = \phi(a + (-a)) = \phi(0_R) = 0_S$$

e pertanto $\phi(-a) = -\phi(a)$.

(ii) Sia a un elemento invertibile di R. Allora

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_R) = 1_S$$

e, similmente, $\phi(a^{-1})\phi(a) = 1_S$. Quindi $\phi(a)$ è un invertibile di S, e $\phi(a^{-1})$ è il suo inverso.

(iii) Induzione su n. ∎

Gli omomorfismi (e gli isomorfismi) di anelli si comportano bene rispetto alla composizione di applicazioni, come suggerisce la seguente proposizione.

Proposizione 6.14. *Siano $\phi : R \to S$ e $\psi : S \to T$ omomorfismi di anelli. Allora*

1) $\psi \circ \phi : R \longrightarrow T$ è un omomorfismo di anelli.

2) Se ϕ è un isomorfismo, allora anche ϕ^{-1} è un isomorfismo.

Dimostrazione. 1) Per esercizio.
2) Se ϕ è un isomorfismo, allora è per definizione una applicazione biettiva, e quindi esiste l'applicazione inversa $\phi^{-1} : S \longrightarrow R$, che è pure biettiva. Mostramo che ϕ^{-1} è un isomorfismo.
Siano $x, y \in S$. Allora, siccome ϕ è un omomorfismo

$$\phi(\phi^{-1}(x) + \phi^{-1}(y)) = \phi(\phi^{-1}(x)) + \phi(\phi^{-1}(y)) = x + y = \phi(\phi^{-1}(x + y)).$$

Poichè ϕ è iniettiva, si ha $\phi^{-1}(x + y) = \phi^{-1}(x) + \phi^{-1}(y)$. In modo analogo si prova che $\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y)$. Infine,

$$\phi^{-1}(1_S) = \phi^{-1}(\phi(1_R)) = 1_R.$$

Dunque ϕ^{-1} è un isomorfismo. ∎

Sia $\phi : R \to S$ un omomorfismo di anelli. Com'è usuale, denotiamo con $Im(\phi)$ l'immagine dell'applicazione ϕ, cioè

$$Im(\phi) = \phi(R) = \{\phi(x) \mid x \in R\}.$$

La dimostrazione della seguente proposizione è molto facile, e si lascia per esercizio.

Proposizione 6.15. *Sia $\phi : R \to S$ un omomorfismo di anelli; allora $Im(\phi)$ è un sottoanello di S.*

Definizione. Sia $\phi : R \to S$ un omomorfismo di anelli. Il **nucleo** $Ker(\phi)$ di ϕ è l'insieme degli elementi di R la cui immagine tramite ϕ è 0_S; cioè

$$Ker(\phi) = \{x \in R \mid \phi(x) = 0_S\}.$$

Esempio. Sia a un fissato numero reale. Allora la *sostiuzione* $\sigma_a : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$, definita da, per ogni $f \in \mathbb{R}^{\mathbb{R}}$, $\sigma_a(f) = f(a)$, è un omomorfismo di anelli. Infatti, per ogni $f, g \in \mathbb{R}^{\mathbb{R}}$,

$$\sigma_a(f + g) = (f + g)(a) = f(a) + g(a) = \sigma_a(f) + \sigma_a(g)$$

$$\sigma_a(fg) = (fg)(a) = f(a)g(a) = \sigma_a(f)\sigma_a(g),$$

inoltre, se $\underline{1}$ è la funzione costante 1 (che è l'identità di $\mathbb{R}^{\mathbb{R}}$), $\sigma_a(\underline{1}) = \underline{1}(a) = 1$. Il nucleo di un tale omomorfismo è

$$Ker(\sigma_a) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\},$$

che, per quano visto in un esempio precedene, è un ideale di $\mathbb{R}^{\mathbb{R}}$.

Il fatto che, in queso esempio, il nucleo sia un ideale di $\mathbb{R}^{\mathbb{R}}$ (ovvero del dominio dell'omomorfismo) non è accidentale. Infatti vale il seguente fondamentale risultato.

Teorema 6.16. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

(1) *$Ker(\phi)$ è un ideale di R.*

(2) *ϕ è iniettivo se e solo se $Ker(\phi) = \{0_R\}$.*

Dimostrazione. (1) Poichè $\phi(0_R) = 0_S$, $Ker(\phi)$ non è vuoto. Siano $a, b \in Ker(\phi)$ e $r \in R$; allora

$$\phi(a-b) = \phi(a) - \phi(b) = 0_S - 0_S = 0_S$$

quindi $a - b \in Ker(\phi)$; inoltre

$$\phi(ar) = \phi(a)\phi(r) = 0_S\phi(r) = 0_S \qquad \text{e} \qquad \phi(ra) = \phi(r)\phi(a) = \phi(r)0_S = 0_S$$

quindi $ar, ra \in Ker(\phi)$. Dunque $Ker(\phi)$ è un ideale di R.

(2) Poichè $\phi(0_R) = 0_S$, $Ker(\phi) = \{0_R\}$ se ϕ è iniettivo. Viceversa, sia $Ker(\phi) = \{0_R\}$ e siano $a, b \in R$ tali che $\phi(a) = \phi(b)$; allora $\phi(a-b) = \phi(a) - \phi(b) = 0_S$, quindi $a - b \in Ker(\phi)$ che implica $a - b = 0_R$, cioè $a = b$. Dunque ϕ è iniettivo. ∎

L'iniettività di un certo omomorfismo è una proprietà molto importante (e ricercata): infatti, se $\phi : R \to S$ è un omomorfismo iniettivo di anelli, allora, restringendo il codominio S all'immagine di ϕ (che è ancora un anello), si ricava un *isomorfismo* da R in $Im(\phi)$ (quindi, se ϕ è iniettivo, $R \simeq Im(\phi)$). In particolare abbiamo,

Corollario 6.17. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora, ϕ è un isomorfismo se e soltanto se $Im(\phi) = S$ e $\ker(\phi) = \{0_R\}$.*

Esercizio 6.21. Sia $\phi : R \to S$ un omomorfismo di anelli. Provare che se R è un campo allora ϕ è iniettivo.

Soluzione. $Ker(\phi)$ è un ideale di R. Se R è un campo, per il Teorema 6.12, $Ker(\phi) = R$ oppure $Ker(\phi) = \{0_R\}$. Ma $Ker(\phi) \neq R$ perchè $\phi(1_R) = 1_S \neq 0_S$; quindi $Ker(\phi) = \{0_R\}$ e dunque ϕ è iniettivo per il Teorema precedente.

Esercizio 6.22. Sia $\phi : R \to S$ un omomorfismo di anelli.

1) Sia T un ideale di S. Si provi che $\phi^{-1}(T)$ è un ideale di R.

2) Sia I un ideale di R. Si provi che, se ϕ è suriettivo allora $\phi(I)$ è un ideale di S.

3) Sia $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita da $\phi(z) = (z, z)$, per ogni $z \in \mathbb{Z}$. Si provi che ϕ è un omomorfismo di anelli; si dimostri che se I è un ideale di $\mathbb{Z}$ tale che $\phi(I)$ è un ideale di $\mathbb{Z} \times \mathbb{Z}$, allora $I = \{0\}$..

Esercizio 6.23. Siano ϕ e ψ due endomorfismi di uno stesso anello A (cioè omomorfismi di A in se stesso). Si provi che $B = \{a \in A \mid \phi(a) = \psi(a)\}$ è un sottoanello di A, e che se A è un campo allora anche B è un campo.

Esercizio 6.24. Sull'insieme $\mathbb{Q}$ dei numeri razionali si considerino l'usuale addizione $+$ e la moltiplicazione $*$ definita ponendo, per ogni $x, y \in \mathbb{Q}$, $x * y = 3/4\, xy$. Si dimostri che $(\mathbb{Q}, +, *)$ è un campo isomorfo al campo dei numeri razionali $(\mathbb{Q}, +, \cdot)$.

Esercizio 6.25. Detrminare tutti gli automorfismi dell'anello $\mathbb{Q}[\sqrt{2}]$ definito nella sezione 6.1.

6.5 Esercizi.

Esercizio 6.26. (Interi di Gauss). (a) Si provi che

$$\mathbb{Z}[i] = \{\mathrm{a} + \mathrm{ib} \mid \mathrm{a}, \mathrm{b} \in \mathbb{Z}\}$$

è un sottoanello di $\mathbb{C}$.

$\mathbb{Z}[i]$ è detto *l'anello degli interi di Gauss*. Si consideri la restrizione della norma complessa a $\mathbb{Z}[i]$ (cioè l'applicazione $N : \mathbb{Z}[i] \to \mathbb{Z}$ definita da $N(\mathrm{a} + \mathrm{ib}) = \mathrm{a}^2 + \mathrm{b}^2$, per ogni $\mathrm{a} + \mathrm{ib} \in \mathbb{Z}[i]$), e si osservi che $N(z_1 z_2) = N(z_1)N(z_2)$ per ogni $z_1, z_2 \in \mathbb{Z}[i]$.

(b) Si dimostri che se z è un elemento invertibile dell'anello $\mathbb{Z}[i]$ allora $N(z) = 1$.

(c) Si dimostri che gli elementi invertibili di $\mathbb{Z}[i]$ sono $1, -1, i, -i$.

Esercizio 6.27. Sia R un anello, X un insieme non vuoto, e sia $A = R^X$ l'insieme di tutte le applicazioni da X in R. Su A si definiscano una addizione e una moltiplicazione ponendo, per ogni $f, g \in A$:

$$(f + g)(x) = f(x) + g(x), \quad fg(x) = f(x)g(x) \ \ \textit{per ogni} \ \ x \in X.$$

Allora $(A, +, \cdot)$ è un anello commutativo.

(a) Si determini l'identità dell'anello A.

(b) Si determinino i divisori dello zero di A e si dica se il loro insieme costituisce un ideale di A.

(c) Si determinino gli elementi invertibili di A (assumendo di conoscere quelli di R).

(d) Posto $X = \{0, 1\}$, si provi che l'anello R^X è isomorfo a $R \times R$.

Esercizio 6.28. Sia R l'anello $\mathbb{Z} \times \mathbb{Z}$, e sia $S = \{(x, y) \in R \mid 3 \ \text{divide} \ x - y\}$. Si provi che S è sottoanello ma non è ideale di R. Si determinino quindi gli elementi invertibili di S.

Esercizio 6.29. Sia R un anello commutativo. Si provi che R è un dominio d'integrità se e solo se soddisfa la legge di cancellazione.

Esercizio 6.30. Sia R un anello commutativo e sia $a \in R$. Si provi che l'insieme $N(a) = \{x | x \in R, xa = 0_R\}$ è un ideale di R. Più in generale, si provi che, se I un ideale di R, allora

$$N_I(a) = \{x \in R \mid xa \in I\}.$$

è un ideale di R .

Esercizio 6.31. Siano I, L, K ideali dell'anello A tali che

$$I + L = A \qquad \text{e} \qquad L \cap K \subseteq I \ ;$$

si provi che $K \subseteq I$.

Esercizio 6.32. Sia $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$ una catena ascendente di ideali *propri* di un anello R. Si provi che $\bigcup_{n \in \mathbb{N}} I_n$ è un ideale proprio di R.

Esercizio 6.33. Sia p un primo fissato e sia $R = \{ \frac{m}{n} \in \mathbb{Q} \mid p \text{ non divide } n \}$.

(a) Si dimostri che R un anello. (basta provare che un sottoanello di $(\mathbb{Q}, +, \cdot)$).

Sia $U(R)$ l'insieme degli elementi invertibili di R, e sia $I = R \setminus U(R)$.

(b) Si determinino gli elementi di $U(R)$.

(c) Si provi che I è un ideale di R.

(d) Si dimostri che ogni ideale proprio di R è contenuto in I.

Esercizio 6.34. Sia R un anello e sia e un elemento idempotente (cioè tale che $e^2 = e$) con $e \neq 0_R, 1_R$..

(a) Sia $I = \{a \in R \mid ea = a\}$. Si provi che se R è commutativo allora I è un ideale di R, e contiene (e).

(b) Considerando l'elemento $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ nell'anello delle matrici $M_2(\mathbb{R})$, si provi che l'affermazione del punto (b) non vale se R non è commutativo.

Esercizio 6.35. Sia I un ideale dell'anello commutativo R.

(a) Siano $x, y \in R$, si provi che se x^2, $x + y \in I$ allora $y^2 \in I$.

(b) Sia $x \in R$ tale che $x^2 \in I$; si provi che $K = \{ y \in R \mid x(x + y) \in I \}$ è un ideale di R.

Esercizio 6.36. Sia R un sottoanello dell'anello $\mathbb{Q}$ dei numeri razionali.

(a) Si provi che se $\frac{a}{b} \in R$ con $(a, b) = 1$ allora $\frac{1}{b} \in R$.

(b) Si provi che se I è un ideale di R esiste $n \in \mathbb{Z}$ tale che $I = (n) = nR$.

Esercizio 6.37. Sia p un numero primo; si provi che

$$\mathbb{Q}_p = \left\{ \frac{n}{p^i} \mid n \in \mathbb{Z},\ i \in \mathbb{N} \right\}$$

è un dominio a ideali principali.

Esercizio 6.38. Dato $f \in \mathbb{R}^{\mathbb{R}}$, poniamo $Z(f) = \{x \in \mathbb{R} \mid f(x) = 0\}$. Siano $f, g \in \mathbb{R}^{\mathbb{R}}$; si provi che se $Z(f) \cap Z(g) = \emptyset$, allora l'ideale generato (f, g) di $\mathbb{R}^{\mathbb{R}}$ è principale.

Esercizio 6.39. Si provi che l'insieme

$$\{f \in \mathbb{R}^{\mathbb{R}} \mid \mathbb{R} \setminus Z_f \text{ è finito } \}$$

è un ideale dell'anello $\mathbb{R}^{\mathbb{R}}$, e che non è un ideale principale.

Esercizio 6.40. Si provi che ogni ideale finiamente generato dell'anello $\mathbb{R}^{\mathbb{R}}$ è principale.

Esercizio 6.41. Sia R un anello commutativo. Si provi che se esistono ideali non banali I e J di R tali che $I \cap J = \{0\}$ allora R non è un dominio d'integrità.

Esercizio 6.42. Sia $f : R \longrightarrow S$ un omomorfismo di anelli e sia H un ideale di S. Si dimostri che

$$f^{-1}(f(H)) = H + Ker(f).$$

Esercizio 6.43. Si provi che non esistono omomorfismi dell'anello $\mathbb{Q}$ nell'anello $\mathbb{Z}$. Si provi che l'applicazione identica è l'unico automorfismo di $\mathbb{Z}$ ed è l'unico automorfismo di $\mathbb{Q}$.

Esercizio 6.44. Sia $\mathbb{R}^{\mathbb{R}}$ l'anello delle funzioni reali. Si provi che non esiste alcun omomorfismo di anelli da $\mathbb{C}$ in $\mathbb{R}^{\mathbb{R}}$.

Esercizio 6.45. Sia R un dominio d'integrità e sia $f : R \to R$ l'applicazione definita da $f(a) = a^2$ per ogni $a \in R$. Si provi che f è iniettiva se e solo se è un omomorfismo. [sugg.: si provi che se f è iniettiva allora per ogni $a \in R$ si ha $a + a = 0_R$].

Esercizio 6.46. Sia R un anello commutativo. Si assuma che $x^2 \neq 0$ per ogni $0 \neq x \in R$, e che esista un ideale non banale minimo I di R (cioè $I \subseteq J$ per ogni ideale non banale J di R). Si provi che R è un dominio d'integrità. Si concluda infine che R è un campo (ovvero che $I = R$). [sugg.: si osservi che I è principale, quindi si assuma per assurdo che esistano $x, y \in R$ tali che $xy = 0$ ...]

Esercizio 6.47. Sia R un dominio di integrità (anello commutativo privo di divisori dello zero), e sia $a \in R$, $a \neq 0$ ed a non invertibile. Si provi che l'ideale (a^2) é contenuto propriamente nell'ideale (a). Si dimostri quindi che un dominio di integritá con un numero finito di ideali è un campo.

Esercizio 6.48. Sia A un anello commutativo, e sia $I = \{a \in A \mid a \text{ non è invertibile}\}$. Si provi che le seguenti condizioni sono equivalenti:

(i) I è un ideale di A;

(ii) esiste un ideale proprio di A che contiene tutti gli ideali propri di A.

Esercizio 6.49. (Ideali di un anello di parti). Sia X un insieme non vuoto, e consideriamo l'anello delle parti $(\mathcal{P}(X), \Delta, \cap)$.

(a) Si provi che per ogni $Y \in \mathcal{P}(X)$, l'ideale principale generato da Y è $\mathcal{P}(Y)$.

(b) Si provi che se $\mathcal{I}$ è un ideale di $\mathcal{P}(X)$ e $Y, Z \in \mathcal{I}$, allora $Y \cup Z \in \mathcal{I}$. Si deduca che se X è finito, ogni ideale di $\mathcal{P}(X)$ è principale.

(c) Sia X un insieme *infinito*; si provi che $\mathcal{F} = \{Y \in \mathcal{P}(X) \mid |Y| < \infty\}$ è un ideale di $\mathcal{P}(X)$, e che non è principale.

Esercizio 6.50. (Sugli anelli di Boole) Sia A un anello di Boole (vedi Proposizione 6.8). Su A si definisca la relazione $\leq$ ponendo, per ogni $a, b \in A$, $a \leq b$ se $ab = a$.

(a) Si provi che $\leq$ è una relazione d'ordine su A.

(b) Si provi che $(A, \leq)$ è un reticolo, con $\max A = 1$ e $\min A = 0$.

(c) Si provi che il reticolo $(A, \leq)$ è *complementato*: per ogni $a \in A$ esiste $a' \in A$ tale che $a \vee a' = 1$ e $a \wedge a' = 0$.

Capitolo 7

Anelli notevoli

7.1 Anelli di classi di congruenza.

Sia $n \geq 2$. L'insieme $\mathbb{Z}/n\mathbb{Z}$ di tutte le classi di congruenza modulo n, fornisce un importante caso di anello commutativo.
Ovviamente, dobbiamo iniziare con il definire opportune operazioni di somma e di prodotto sull'insieme $\mathbb{Z}/n\mathbb{Z}$.

Sia quindi fissato il modulo $n \geq 2$. Denotando con $\overline{a}$ la classi di congruenza modulo n di $a \in \mathbb{Z}$, si ha $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}]|$. Siano $a, b \in \mathbb{Z}$; allora

$$\overline{a} = a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\} \qquad \overline{b} = b + n\mathbb{Z} = \{b + nz \mid z \in \mathbb{Z}\}.$$

sono sottoinsiemi non vuoti dell'anello $\mathbb{Z}$, che possiamo quindi sommare secondo la regola descritta nella sezione 4.2:

$$\begin{aligned} \overline{a} + \overline{b} &= \{\ x + y \mid x \in \overline{a},\, y \in \overline{b}\ \} = \{\ (a + nz_1) + (b + nz_2) \mid z_1, z_2 \in \mathbb{Z}\ \} = \\ &= \{\ (a + b) + n(z_1 + z_2) \mid z_1, z_2 \in \mathbb{Z}\ \} = \{\ (a + b) + nz \mid z \in \mathbb{Z}\ \} = \\ &= \overline{a + b}. \end{aligned}$$

In pratica, *la somma di classi di congruenza modulo n è ancora una classe di congruenza modulo n*, che è descritta dalla regola

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Questo definisce un'operazione di somma sull'insieme $\mathbb{Z}/n\mathbb{Z}$ di tutte le classi di congruenza modulo n. In modo simile è possibile definire un prodotto per classi di congruenza. Con gli stessi n, a e b di sopra, si pone

$$\overline{a} \cdot \overline{b} = \{\ xy \mid x \in \overline{a},\, y \in \overline{b}\ \}.$$

Quindi,

$$\begin{aligned} \overline{a} \cdot \overline{b} &= \{(a + nz_1)(b + nz_2) \mid z_1, z_2 \in \mathbb{Z}\} = \\ &= \{ab + n(az_2 + bz_1 + nz_1z_2) \mid z_1, z_2 \in \mathbb{Z}\} = \\ &= \{ab + nz \mid z \in \mathbb{Z}\ \} = \overline{ab}. \end{aligned}$$

Dunque, anche in questo caso, *il prodotto di due classi di congruenza modulo n è una classe di congruenza modulo n*, ed è descritto da

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Ciò definisce pertanto un'operazione di prodotto su $\mathbb{Z}/n\mathbb{Z}$.

A questo punto, risulta laborioso ma non difficile provare che l'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$, con le operazioni di somma e prodotto definite sopra, è un anello commutativo, che si chiama **anello delle classi resto modulo n**. Inoltre si ha

$$0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0} = n\mathbb{Z} \qquad \text{e} \qquad 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1} = 1 + n\mathbb{Z}.$$

(Si tratta di verificare proprietà che discendono naturalmente da quelle analoghe in $\mathbb{Z}$, e dalle definizioni delle operazioni. Per esempio verifichiamo la proprietà distributiva.
Siano $\overline{a}, \overline{b}, \overline{c}$, generici elementi di $\mathbb{Z}/n\mathbb{Z}$. Allora

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$$

Le altre verifiche si conducono in modo simile. È altresì immediato verificare che, per ogni $k \in \mathbb{N}$, ed ogni $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, si ha $\overline{a}^k = \overline{a^k}$.)

Per comidità, se $2 \leq n \in \mathbb{N}$, denoteremo talvolta con $\mathbb{Z}_n$ l'anello $\mathbb{Z}/n\mathbb{Z}$.

Esempi. 1) Nell'anello $\mathbb{Z}/6\mathbb{Z}$ eseguiamo il calcolo seguente

$$\begin{aligned}
\overline{5} - \overline{2}^3 \cdot (\overline{3} + \overline{4} \cdot \overline{5}) + (\overline{2} + \overline{3})^3 (\overline{3} - \overline{5}) &= \overline{5} - \overline{8} \cdot (\overline{3} + \overline{20}) + (\overline{2+3})^3 (\overline{3-5}) = \\
&= \overline{5} - \overline{2} \cdot \overline{23} + \overline{5}^3 \cdot (\overline{-2}) = \\
&= \overline{5} - \overline{2} \cdot \overline{5} + \overline{(-1)^3} \cdot \overline{4} = \\
&= \overline{5} - \overline{2} \cdot \overline{5} + \overline{(-1)} \cdot \overline{4} = \overline{5 - 10 - 4} = \overline{-9} = \overline{3}.
\end{aligned}$$

2) Sia p un numero primo. Il Teorema di Fermat (Teorema 4.7) può essere interpretato come una eguaglianza nell'anello $\mathbb{Z}/p\mathbb{Z}$; esso afferma che

$$\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z} \quad \Rightarrow \quad \overline{a}^{p-1} = \overline{1}.$$

Facciamo subito un'importante osservazione. Sia $n \geq 1$, e sia $\mathbb{Z}/n\mathbb{Z}$ l'anello delle classi di congruenza modulo n. Allora l'applicazione

$$\begin{array}{rccc} \rho_n : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & a & \mapsto & a + n\mathbb{Z} \end{array}$$

è un omomorfismo suriettivo di anelli, che si chiama *riduzione modulo n*. Come avremo anche modo di vedere più avanti, sii tratta di uno strumento semplice ma basilare in molti campi della teoria (elementare e no) dei numeri. Osserviamo anche che, se ρ_n è la riduzione modulo n, allora $ker(\rho_n) = n\mathbb{Z}$.

Abbiamo già osservato che, per $n \geq 2$, l'anello $\mathbb{Z}/n\mathbb{Z}$ è commutativo. In generale però non è un dominio d'integrità: ad esempio, nell'anello $\mathbb{Z}/12\mathbb{Z}$ delle classi resto modulo 12, $\overline{4} \neq \overline{0}$, $\overline{3} \neq \overline{0}$, ma $\overline{4} \cdot \overline{3} = \overline{12} = \overline{0} = 0_{\mathbb{Z}/6\mathbb{Z}}$, e quindi $\overline{4}$ e $\overline{3}$ sono divisori dello zero.

D'altra parte è possibile che $\mathbb{Z}/n\mathbb{Z}$ contenga elementi invertibili che non provengono da invertibili di $\mathbb{Z}$. Ad esempio, sempre in $\mathbb{Z}/12\mathbb{Z}$, l'elemento $\overline{5}$ è diverso sia da $\overline{1}$ che da $\overline{-1}$, e purtuttavia è invertibile. Infatti, in $\mathbb{Z}/12\mathbb{Z}$,

$$\overline{5} \cdot \overline{5} = \overline{25} = \overline{1} = 1_{\mathbb{Z}/12\mathbb{Z}},$$

quindi $\overline{5}$ è un elemento invertibile di $\mathbb{Z}/12\mathbb{Z}$ (e coincide con il proprio inverso). Queste osservazioni sono estese e chiarite dal Teorema seguente.

Teorema 7.1. *Sia $n \geq 2$. Allora*

1. *Un elemento $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $(a, n) = 1$. Quindi $U(\mathbb{Z}/n\mathbb{Z}) = \{\ \overline{a} \mid 1 \leq a \leq n-1,\ (a, n) = 1\ \}$.*
2. *$\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo. Se n non è primo, allora $\mathbb{Z}/n\mathbb{Z}$ non è un dominio d'integrità.*

Dimostrazione. 1) Sia $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Possiamo prendere $1 \leq a \leq n-1$ (escludiamo $\overline{a} = \overline{0}$ perchè chiaramente lo zero di un anello non è mai un invertibile - e d'altra parte, $(0, n) = n$). Per definizione, $\overline{a}$ è invertibile se e solo se esiste $1 \leq b \leq n-1$ tale che

$$\overline{ab} = \overline{a} \cdot \overline{b} = 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1}$$

ovvero, $ab \equiv 1 \pmod{n}$. Quindi, $\overline{a}$ è invertibile se e solo se esiste $1 \leq b \leq n-1$ ed un $z \in \mathbb{Z}$ tali che

$$ab + zn = 1$$

cioè se e solo se $(a, n) = 1$.

2) $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se ogni elemento non nullo è invertibile. Quindi, per il punto 1), $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo $(a, n) = 1$ per ogni $1 \leq a \leq n-1$, e questo avviene se e solo se n è un numero primo.
Supponiamo, infine, che n non sia un numero primo. Dunque n si fattorizza propriamente, e quindi esistono interi $2 \leq a,\ b \leq n-1$, tali che $ab = n$. Ma allora, nell'anello $\mathbb{Z}/n\mathbb{Z}$, $\overline{a}$ e $\overline{b}$ sono diversi da $0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0}$, mentre $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{n} = \overline{0}$. Dunque $\overline{a}$ e $\overline{b}$ sono divisori dello zero, e quindi $\mathbb{Z}/n\mathbb{Z}$ non è un dominio d'integrità. ∎

Un aspetto della massima importanza del risultato precedente, e che merita di essere ribadito, è che se p è un numero primo positivo, allora $\mathbb{Z}/p\mathbb{Z}$ è un campo.

Corollario 7.2. *Per ogni numero primo p esiste un campo di ordine p.*

Esercizio 7.1. Determinare le soluzioni dell'equazione $\overline{3}x^2 - \overline{2} = \overline{0}$, nel campo $\mathbb{Z}/7\mathbb{Z}$.

Soluzione. Poichè tutti gli elementi non nulli di $F = \mathbb{Z}/7\mathbb{Z}$ sono invertibili, possiamo moltiplicare per l'inverso di $\overline{3}$, che è $\overline{5}$ (infatti $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$), ottenendo l'equazione equivalente

$$\overline{0} = x^2 - \overline{2} \cdot \overline{5} = x^2 - \overline{3}.$$

A questo punto, possiamo testare più facilmente gli elementi di F, trovando che $\overline{1}^2 = \overline{6}^2 = \overline{1}$, $\overline{2}^2 = \overline{5}^2 = \overline{4}$, $\overline{3}^2 = \overline{4}^2 = \overline{2}$; concludendo così che l'equazione data non ha soluzioni in F.

Esercizio 7.2. Si determinino tutti gli elementi invertibili ed i divisori dello zero negli anelli $\mathbb{Z}/24\mathbb{Z}$ e $\mathbb{Z}/16\mathbb{Z}$.

Esercizio 7.3. Trovare le soluzioni di $x^2 = \overline{1}$, e di $x^3 = \overline{1}$, negli anelli $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ e $\mathbb{Z}/11\mathbb{Z}$.

Caratteristica di un anello. Sia a un elemento di un anello R. Allora, per ogni numero intero n è definito il multiplo n-esimo na di a nel modo che conosciamo

$$na = \underbrace{a + a + \cdots + a}_{n} \qquad \text{se } n \geq 1$$

e $na = (-n)(-a)$ se $n \leq -1$, $0a = 0_R$. Valgono le regole descritte nella sezione 6.1.

Proposizione 7.3. *Sia R un anello. Esiste un solo omomorfismo da $\mathbb{Z}$ in R, ed è definito da, per ogni $z \in \mathbb{Z}$, $z \mapsto z1_R$.*

Dimostrazione. Sia ϕ un omomorfismo da $\mathbb{Z}$ in R. Allora $\phi(1) = 1_R$ e $\phi(0) = 0_R$, da cui segue $\phi(-1) = -1_R$ e, per ogni $n \geq 0$

$$\phi(n) = \phi(1 + 1 + \cdots + 1) = \phi(1) + \phi(1) + \cdots + \phi(1) = n1_R$$

e $\phi(-n) = -\phi(n) = -(n1_R) = (-n)1_R$.
Viceversa, si verifica usando le regole sopra ricordate, che l'applicazione

$$\begin{array}{ccc} \mathbb{Z} & \to & R \\ z & \mapsto & z1_R \end{array}$$

è un omomorfismo di anelli. ∎

Ora, dato un anello R, sia ϕ l'unico omomorfismo da $\mathbb{Z}$ in R. Il suo nucleo è un ideale di $\mathbb{Z}$, quindi $\ker(\phi) = n\mathbb{Z}$ per un numero naturale n univocamente determinato. Tale naturale n si dice la **caratteristica** dell'anello R. Osserviamo che se la caratteristica è diversa da 0 allora deve essere almeno 2.
Quindi la caratteristica di R è 0 se e solo se l'omomorfismo ϕ è iniettivo; se invece la caratteristica è $n \geq 2$, allora (ricordando come si trova il generatore positivo di un ideale di $\mathbb{Z}$ - Teorema 6.9) n è il minimo intero > 0 che appartiene al nucleo di ϕ. Possiamo dunque dedurre la seguente definizione alternativa di caratteristica:

La caratteristica di un anello R è

0 *se* $n1_R \neq m1_R$ *per ogni* $n, m \in \mathbb{Z}$, $n \neq m$;

$n > 0$ *se* n *è il minimo numero naturale non nullo tale che* $n1_R = 0_R$.

Ad esempio, gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ hanno caratteristica 0, mentre, per $n \geq 2$, l'anello $\mathbb{Z}/n\mathbb{Z}$ ha caratteristica n. La Proposizione 6.8 afferma, in particolare, che un anello di Boole ha caratteristica 2.

Esercizio 7.4. Determinare la caratteristica dell'anello $A = \mathbb{Z}_6 \times Z_4$.

Soluzione. Poiché $1_A = (\overline{1}, \overline{1})$ (dove, ovviamente, la barra denota classi di congruenza modulo 6 e modulo 4 rispettivamente nelle due coordinate), si ha $12 \cdot 1_A = (\overline{12}, \overline{12}) = (\overline{0}, \overline{0}) = 0_A$. Ciò significa che, posto n la caratteristica di A, si ha $12 \in n\mathbb{Z}$. In altre parole, $n \geq 2$ è un divisore di 12. Ma $6 \cdot 1_A = (\overline{6}, \overline{6}) = (\overline{0}, \overline{2}) \neq 0_A$, e similmente $4 \cdot 1_A = (\overline{4}, \overline{4}) = (\overline{4}, \overline{2}) \neq 0_A$. Si conclude quindi che $n = 12$.

Esaminiamo ora più a fondo l'immagine dell'unico omomorfismo ϕ da $\mathbb{Z}$ in R definito nella Proposizione 7.3

$$Im(\phi) = \{z1_R \mid z \in \mathbb{Z}\},$$

che si denota con P_R. Si tratta di un sottoanello di R, che è contenuto in ogni altro sottoanello di R (perché ?). Per questo motivo P_R è detto *sottoanello fondamentale* o sottoanello *primo* di R.
Sia n è la caratteristica di R. Se $n = 0$, l'omomorfismo ϕ è iniettivo e dunque $P_R \simeq \mathbb{Z}$. Sia $n \geq 2$; allora è ben definita l'applicazione

$$\begin{array}{rcl} \overline{\phi} : \mathbb{Z}/n\mathbb{Z} & \to & P_R \\ \overline{z} & \mapsto & z1_R \end{array}$$

Siano infatti $z, z_1 \in \mathbb{Z}$ tali che $\overline{z} = \overline{z_1}$; allora n divide $z_1 - z$, e conseguentemente $0_R = (z_1 - z)1_R = z_1 1_R - z1_R$, da cui $z_1 1_R = z1_R$. Ora, $\overline{\phi}$ è suriettiva (per definizione di P_R), e si verifica facilmente che è un omomorfismo di anelli; è inoltre iniettiva, perché $0_R = \overline{\phi}(\overline{z}) = z1_R \ \Rightarrow \ n|z \ \Rightarrow \overline{z} = \overline{0}$. Dunque $\overline{\phi}$ è un isomorfismo. Abbiamo così una completa descrizione dei sottoanelli fondamentali, che ricapitoliamo nella seguente proposizione.

Proposizione 7.4. *Sia R una anello, e sia P_R il suo sottoanello fondamentale. Allora*

(1) la caratteristica di R è zero se e solo se $P_R \simeq \mathbb{Z}$;

(2) la caratteristica di R è $n > 0$ se e solo se $P_R \simeq \mathbb{Z}/n\mathbb{Z}$.

Osserviamo che se n è la caratteristica di un anello R, allora $na = 0_R$ per ogni $a \in R$. Ciò è per definizione se $n = 0$; mentre se $n > 0$ per ogni $a \in R$ si ha

$$na = a + \cdots + a = 1_R a + \cdots + 1_R a = (1_R + \cdots 1_R)a = (n1_R)a = 0_R a = 0_R \ .$$

Concludiamo con la seguente importante osservazione:

Proposizione 7.5. *La caratteristica di un dominio d'integrità è 0 oppure un numero primo.*

Dimostrazione. Sia R un dominio d'integrità di caratteristica $n > 0$. Allora il sottoanello fondamentale P_R è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Poiché P_R è anch'esso un dominio d'integrità, n deve essere un numero primo (Teorema 7.1). ∎

Esercizio 7.5. Provare che gli anelli $\mathbb{Z}_5 \times \mathbb{Z}_5$ e $\mathbb{Z}_{25}$ non sono isomorfi.

Esercizio 7.6. Si determini la caratteristica dell'anello $R = (\mathbb{Z}/12\mathbb{Z}) \times \mathbb{Z}$.

Esercizio 7.7. Ricordiamo che un elemento a di un anello A è detto *nilpotente* se esiste un intero $n \geq 1$ tale che $a^n = 0_A$. Si determinino gli elementi nilpotenti dell'anello $\mathbb{Z}/18\mathbb{Z}$, e quelli di $\mathbb{Z}/12\mathbb{Z}$.

Esercizio 7.8. Si provi che l'insieme $\{3x + 12\mathbb{Z} \mid x \in \mathbb{Z}\}$ è un ideale dell'anello $\mathbb{Z}/12\mathbb{Z}$.

7.2 Anelli di matrici.

Esempi principali di anelli non commutativi sono gli anelli di matrici. Lo studio sistematico delle matrici è parte del corso di Algebra lineare (Geometria 1). Richiamiamo qui, per comidità del lettore e senza dimostrazioni, solo alcuni fatti significativi dal nostro punto di vista, limitandoci, almeno per quanto riguarda le descrizioni dettagliate, al caso di matrici a coefficienti reali.

Sia $1 \leq n \in \mathbb{N}$. Una **matrice quadrata di ordine n** a coefficienti reali è una tabella

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

dove i coefficienti a_{ij} sono numeri reali. L'insieme di tutte le matrici quadrate di ordine n a coefficienti reali si denota con $M_n(\mathbb{R})$.

La **somma** $A + B$ di due matrici (reali, di ordine n) $A = (a_{ij})$ e $B = (b_{ij})$, è la matrice (di ordine n) i cui coefficienti si ottengono sommando tra loro i coefficienti corrispondenti di A e B. Ovvero, posto $(s_{ij}) = S = A + B$, si pone $s_{ij} = a_{ij} + b_{ij}$ (per ogni $i, j = 1, \ldots, n$). Un esempio è forse superfluo, ma eccone uno con $n = 2$:

$$\begin{pmatrix} 1 & -2 \\ 6 & 3 \end{pmatrix} + \begin{pmatrix} -3 & 0 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} -2 & -2 \\ 7 & -1 \end{pmatrix}.$$

Si verifica facilemente che tale somma soddisfa gli assiomi (S1) – (S4) di anello. È cioè un'operazione transitiva, commutativa, con un elemento neutro che è la matrice nulla 0_M (ovvero quella con tuti i coefficienti uguali a 0), e tale che ogni matrice ha una matrice 'opposta' (definita prendendo gli opposti dei coefficienti). Ad esempio, per $n = 2$,

$$0_{M_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}.$$

Se $A = (a_{ij}) \in M_n(\mathbb{R})$, allora, per ogni $i = 1, 2, \ldots, n$, la n-upla di numeri reali

$$(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

è detta **i-esima riga** della matrice A. Mentre la **i-esima colonna** di A è

$$(a_{1i}\ a_{2i}\ \cdots\ a_{ni}).$$

Il **prodotto** di due matrici quadrate di ordine n, $A = (a_{ij})$, $B = (b_{ij})$ è definito nella maniera seguente: $(a_{ij})(b_{ij}) = (c_{ij})$ dove, per ogni $i, j = 1, 2, \ldots, n$

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}. \tag{7.1}$$

Cioè il coefficiente di posto ij nella matrice prodotto è

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \ldots + a_{in}b_{nj}$$

ovvero il prodotto (scalare) della i-esima riga di A per la j-esima colonna di B.

Esempi:

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + (-\frac{1}{2} \cdot \frac{1}{2}) & 1 \cdot (-1) + (-\frac{1}{2}) \cdot (-2) \\ -2 \cdot 0 + 3 \cdot \frac{1}{2} & -2 \cdot (-1) + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{3}{2} & -4 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 1 \\ 3 & 0 & 1 \\ -2 & \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 5 & \frac{1}{4} & 2 \\ 3 & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Si verifica che, per ogni $n \geq 1$ il prodotto di matrici quadrate di ordine n è una operazione associativa. Inoltre la **matrice identica**

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

è l'elemento identico. Sono quindi soddisfatti anche gli assiomi (P1) (P2) (ovvero $(M_n(\mathbb{R}), \cdot)$ è un monoide). Si verifica poi che sussistono anche le proprietà distributive. Dunque, per ogni $n \geq 1$, $M_n(\mathbb{R})$ **è un anello**.

Se $n \geq 2$ il prodotto di matrici *non è commutativo*, ad esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

(per $n = 1$, $M_1(\mathbb{R})$ coincide con $\mathbb{R}$).

Sempre per $n \geq 2$, $M_2(\mathbb{R})$ contiene elementi unipotenti non nulli (quindi divisori dello zero): si provi ad esempio che se

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

allora $A^3 = 0$.

Esercizio 7.9. Nell'anello $M_2(\mathbb{R})$ si trovino due elementi a e b tali che $(ab)^2 \neq a^2b^2$.

Ad ogni matrice quadrata reale A è associato un numero reale $|A| = Det(A)$ detto **determinante** di A. La definizione generale di determinante di una matrice e le sue proprietà sono parte del corso di Geometria. Qui ricordo solo il caso di matrici di ordine $n = 2, 3$. (Una matrice di ordine 1 è un numero reale e coincide con il suo determinante)

$$Det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$$Det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}Det\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + (-1)a_{12}Det\begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13}Det\begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Ad esempio

$$Det\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} = 1 \cdot Det\begin{pmatrix} 2 & \frac{1}{2} \\ 1 & 0 \end{pmatrix} + (-1)0 \cdot Det\begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} + (-1) \cdot Det\begin{pmatrix} 0 & 2 \\ -\frac{1}{2} & 1 \end{pmatrix} =$$

$$= 1(2 \cdot 0 - 1\frac{1}{2}) - 0 - 1(0 \cdot 1 - 2(-\frac{1}{2})) = -\frac{1}{2} - 0 - 1 = -\frac{3}{2}.$$

Una proprietà molto importante del determinante è che per ogni $A, B \in M_n(\mathbb{R})$:

$$Det(A \cdot B) = Det(A)Det(B). \tag{7.2}$$

Inoltre, per ogni $n \geq 1, Det(I_n) = 1$.

Un altro fatto fondamentale è che

$$A \in M_n(\mathbb{R}) \text{ è invertibile se e solo se } Det(A) \neq 0. \tag{7.3}$$

Dunque $U(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) \mid Det(A) \neq 0\}$ (che è quindi un gruppo con l'operazione di prodotto righe per colonne, ed è denotato con $GL(n, \mathbb{R})$).

Rimandiamo ancora al corso di Geometria per le regole generali per determinare l'inversa di una matrice invertibile. Qui riporto, al fine di comprendere esempi ed esercizi, il caso $n = 2$.

Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$ con $\Delta = Det(A) \neq 0$. Allora

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}. \tag{7.4}$$

Le definizioni di matrice e le operazioni che abbiamo dato nel caso di coefficienti in $\mathbb{R}$, si estendono senza differenze a matrici con coefficienti in un qualunque anello A, ottenendo anche in tal caso degli anelli. In generale, quindi, per $n \geq 1$, con $M_n(A)$ si denota l'anello delle matrici quadrate di ordine n a coefficienti in A (negli esempi ed esercizi, i casi che potranno occorrere con maggiore frequenza saranno $A = \mathbb{Z}$ e $A = \mathbb{Z}/d\mathbb{Z}$) con le operazioni di somma per componenti e di moltiplicazione righe×colonne. Funziona

tutto in modo parallelo a quello del caso dei coefficienti in $\mathbb{R}$, fino alla definizione di determinante. Per quest'ultima, e la susseguente caratterizzazione degli elementi invertibili, è necessario richiedere che l'anello A sia commutativo. In questi casi, il determinante è una applicazione $M_n(A) \to A$, che formalmente si definisce come nel caso a coefficienti reali. La formula per il prodotto (7.2) vale invariata, mentre la caratterizzazione degli elementi invertibili (7.3) diventa in generale la seguente: sia A un anello commutativo, e sia $U \in M_n(A)$, allora U è invertibile in $M_n(A)$ se e solo se $Det(U)$ è un elemento invertibile di A.
Ad, esempio gli elementi invertibili di $M_n(\mathbb{Z})$ sono tutte e sole le matrici intere (di ordine n) il cui determinante è 1 o -1.

Concludiamo questa sezione con un esercizio: proviamo che i soli ideali di $M_2(\mathbb{R})$ sono $\{0\}$ e $M_2(\mathbb{R})$ (cosa che si generalizza a qualsiasi anello di matrici a coefficienti su un campo). Poiché $M_2(\mathbb{R})$ contiene elementi non nulli e non invertibili, questo mostra che il Teorema 6.12 non si estende al caso non–commutativo (che, d'altra parte, esistano anelli non–commutativi in cui ogni elemento non nullo è invertibile sarà dimostrato nella sezione 7.4).
Sia dunque I un ideale di $M_2(\mathbb{R})$, e supponiamo che I contenga un elemento non-nullo

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Se $Det(A) \neq 0$, A è invertibile e dunque $I = M_2(\mathbb{R})$. Assumiamo quindi $Det(A) = 0$. Poiché I contiene gli elementi

$$A\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} c & d \\ a & b \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$$

possiamo anche assumere $a \neq 0$. Ora, I contiene la matrice

$$B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d+a \end{pmatrix}.$$

Si ha $Det(B) = ad + a^2 - bc = a^2 + Det(A) = a^2 \neq 0$; quindi B è invertibile, e pertanto $I = M_2(\mathbb{R})$, il che completa la dimostrazione.

Nella teoria generale degli anelli non commutativi, il concetto di ideale è affiancato da quelli di *ideale destro* e di *ideale sinistro*. Un sottoinsieme non–vuoto I di un anello R è un ideale destro se, per ogni $a, b \in I$, $x \in R$, $a - b \in I$ e $ax \in I$ (non si richiede, cioè, $xa \in I$). L'ideale sinistro è definito richiedendo invece $a - b \in I$ e $xa \in I$, per ogni $a, b \in I$, $x \in R$. Se R è commutativo, è chiaro che ogni ideale destro (o sinistro) è un ideale; ma per anelli non–commutativi questi due concetti assumono significato (si veda l'esercizio 7.14). Se $a \in R$, allora l'insieme $\{ax \mid x \in \mathbb{R}\}$ è un ideale destro, che si denota con aR ed è il minimo ideale destro di R che contiene a (similmente si definisce l'ideale sinistro $Ra = \{xa \mid x \in R\}$).

Esercizio 7.10. Si provi che ogni elemento non nullo di $M_2(\mathbb{R})$ è invertibile, oppure un divisore dello zero. Si dica se la stessa cosa vale in $M_2(\mathbb{Z})$.

Esercizio 7.11. Sia A un anello commutativo, e sia I un ideale di A. Sia $1 \leq n \in \mathbb{N}$; si provi che

$$M_n(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in I \right\}$$

è un ideale di $M_n(A)$.

Esercizio 7.12. Sia $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.

a) Si provi che A è un sottoanello dell'anello $M_2(\mathbb{R})$.

b) Si provi che l'applicazione $\phi : A \to \mathbb{C}$, definita da

$$\phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + ib$$

è un isomorfismo di anelli.

c) Si trovi un automorfismo $A \to A$ che sia diverso dall'applicazione identitica.

Esercizio 7.13. Sia $n \geq 2$; si provi che l'insieme degli elementi nilpotenti di $M_n(\mathbb{R})$ non è un ideale di $M_n(\mathbb{R})$.

Esercizio 7.14. Sia A un anello commutativo. Si provi che l'insieme

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A \right\}$$

è un ideale destro ma non è un ideale sinistro di $M_2(A)$. Si dica poi se esiste un elemento $X \in M_2(A)$ tale che $J = XM_2(A)$.

7.3 Campo delle frazioni.

Sia $\phi : R \to S$ un omomorfismo *iniettivo* di anelli. Allora R è isomorfo a $\phi(R)$ che è un sottoanello di S; in tal caso si identificano gli elementi di R con le loro immagini tramite ϕ, e si dice che l'anello S è una **estensione** dell'anello R. L'istanza più semplice è quando R è già un sottoanello di S e ϕ associa ogni elemento di R con se stesso.

In questa sezione, per ogni dominio di integrità D costruiremo una estensione F di D che è un campo. Inoltre tale campo F ha la proprietà che ogni campo che sia estensione di D è anche estensione di F. Quindi, in questo senso, F è la *minima* estensione di D che è un campo. Tale F si chiamerà il **campo delle frazioni** di D. Applicata al caso $D = \mathbb{Z}$ questa costruzione fornisce il campo $\mathbb{Q}$ dei numeri razionali.

Sia D un dominio di integrità. Assumiamo perciò che D sia commuatativo e privo di divisori dello zero: entrambe queste condizioni sono necessarie per la costruzione del campo F. Iniziamo considerando l'insieme

$$D \times D^* = \{(a, b) \mid a, b \in D,\ b \neq 0_D\}$$

di tutte le coppie ordinate di elementi di D la cui seconda componente non è zero. Su tale insieme definiamo una relazione $\sim$ ponendo, per ogni $(a, b), (c, d) \in D \times D^*$,

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

Si verifica facilmente che $\sim$ è una relazione di equivalenza. Infatti:

1) $(a,b) \sim (a,b)$ per ogni $(a,b) \in D \times D^*$ perchè $ab = ba$ essendo D commutativo.

2) Se $(a,b) \sim (c,d)$ allora $ad = bc$, quindi $cb = da$, cioè $(c,d) \sim (a,b)$.

3) Siano $(a,b),(c,d),(r,s) \in D \times D^*$ tali che $(a,b) \sim (c,d)$, $(c,d) \sim (r,s)$, allora $ad = bc$ e $cs = dr$; quindi $(as)d = (ad)s = (bc)s = b(cs) = b(dr) = (br)d$; poichè $d \neq 0_D$ e D è un dominio d'integrità, per la legge di cancellazione, si ha $as = br$ e dunque $(a,b) \sim (r,s)$.

Per ogni $(a,b) \in D \times D^*$ indichiamo con $\frac{a}{b}$ la classe di equivalenza di (a,b) modulo $\sim$, e chiamiamo F l'insieme quoziente modulo $\sim$, cioè

$$F = \frac{D \times D^*}{\sim} = \left\{ \frac{a}{b} \mid (a,b) \in D \times D^* \right\} .$$

Definiamo quindi su F le operazioni di somma e prodotto nel modo seguente. Per ogni $\frac{a}{b}, \frac{c}{d} \in F$,

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

Occorre verificare che si tratta di buone definizioni. Siano dunque $\frac{a}{b}, \frac{c}{d}, \frac{a'}{b'}, \frac{c'}{d'} \in F$ con $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$; allora $(a,b) \sim (a',b')$ e $(c,d) \sim (c',d')$, cioè $ab' = ba'$ e $cd' = dc'$. Dunque:

$$\begin{aligned} (ad+bc)b'd' &= adb'd' + bcb'd' = ab'dd' + cd'bb' = \\ &= ba'dd' + dc'bb' = a'd'bd + b'c'bd = (a'd' + b'c')bd \end{aligned}$$

e quindi

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

Similmente

$$(ac)(b'd') = ab'cd' = ba'dc' = (a'c')(bd)$$

e quindi

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

Ora, è facile provare che, con tali operazioni, F è un anello commutativo con $0_F = \frac{0}{1}$, $1_F = \frac{1}{1}$. Vediamo ad esempio la distributività; osserviamo preliminarmente che per ogni $\frac{a}{b} \in F$, e $0 \neq c \in D$ si ha $\frac{a}{b} = \frac{ac}{bc}$; siano quindi $\frac{a}{b}, \frac{c}{d}, \frac{r}{s} \in F$, allora

$$\begin{aligned} \frac{a}{b}(\frac{c}{d} + \frac{r}{s}) &= \frac{a}{b}\frac{cs+dr}{ds} = \frac{a(cs+dr)}{b(ds)} = \frac{acs+adr}{bds} = \\ &= \frac{acsb+adrb}{bdsb} = \frac{ac}{bd} + \frac{ar}{sb} = \\ &= \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{r}{s}. \end{aligned}$$

Lasciamo le altre verifiche per esercizio.

Per dimostrare che F è un campo, resta da provare che ogni elemento non nullo di F è invertibile. Sia $\frac{a}{b} \neq 0_F = \frac{0}{1}$, allora $(a,b) \not\sim (0,1)$, cioè $a = a1 \neq b0 = 0$ e quindi $\frac{b}{a} \in F$ e si ha

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1_F$$

dunque $\frac{b}{a} = (\frac{a}{b})^{-1}$. Quindi F è un campo.

Proviamo che F è una estensione di D mediante l'applicazione

$$\begin{array}{rccc} \phi: & D & \to & F \\ & a & \mapsto & \frac{a}{1} \end{array}$$

ϕ è un omomorfismo, infatti $\phi(1) = \frac{1}{1} = 1_F$, e per ogni $a, a' \in D$

$$\phi(a + a') = \frac{a + a'}{1} = \frac{a1 + a'1}{1 \cdot 1} = \frac{a}{1} + \frac{a'}{1} = \phi(a) + \phi(a')$$

$$\phi(aa') = \frac{aa'}{1} = \frac{aa'}{1 \cdot 1} = \frac{a}{1} \cdot \frac{a'}{1} = \phi(a)\phi(a') \ ,$$

ed è iniettivo, infatti

$$\phi(a) = 0_F \quad \Leftrightarrow \quad \frac{a}{1} = \frac{0}{1} \quad \Leftrightarrow \quad (a,1) \sim (0,1) \quad \Leftrightarrow \quad a = a1 = 1 \cdot 0 = 0$$

dunque $Ker(\phi) = \{0\}$.

Il campo F così costruito si chiama **campo delle frazioni** del dominio D, ed identificando D con la sua immagine $\phi(D)$, possiamo dire che F contiene D. Abbiamo quindi provato la prima parte del seguente

Teorema 7.6. *Sia D un dominio d'integrità. Allora esiste un campo F che è una estensione di D. Inoltre, se K è un campo che è una estensione di D, allora K è una estensione di F.*

Dimostrazione. Rimane da provare la seconda parte dell'enunciato. Sia quindi F il campo delle frazioni del dominio D, e sia $\phi : D \to K$ una estensione di D ad un campo K. Allora per ogni $b \neq 0_D$, $\phi(b) \neq 0_K$ (perchè ϕ è iniettivo), e quindi $\phi(b)$ è invertibile in K. È possibile dunque definire

$$\begin{array}{rccc} \overline{\phi}: & F & \to & K \\ & \frac{a}{b} & \mapsto & \phi(a)\phi(b)^{-1} \end{array}$$

per ogni $a, b \in D,\ b \neq 0_D$. Tale applicazione è ben definita; infatti se $\frac{a}{b} = \frac{c}{d}$ allora $ad = bc$ e quindi $\phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1}$. Si verifica poi facilmente che $\overline{\phi}$ è un omomorfismo (esercizio). Infine, $\overline{\phi}$ è iniettiva, infatti (tenendo conto che D è un campo e quindi, in particolare, un dominio d'integrità)

$$0_K = \overline{\phi}(\frac{a}{b}) = \phi(a)\phi(b)^{-1} \quad \Leftrightarrow \quad \phi(a) = 0_K \quad \Leftrightarrow \quad a = 0_D \quad \Leftrightarrow \quad \frac{a}{b} = 0_F \ .$$

Osserviamo infine che per ogni $a = \frac{a}{1} \in D$ si ha $\overline{\phi}(\frac{a}{1}) = \phi(a)$. ∎

Se applicata all'anello $\mathbb{Z}$, questa procedura conduce alla costruzione del campo $\mathbb{Q}$ dei numeri razionali. Anzi, volendo essere rigorosi, il campo $\mathbb{Q}$ è *definito* come il campo delle frazioni di $\mathbb{Z}$.

Esercizio 7.15. Sia F un campo. Qual è il campo delle frazioni di F?

Esercizio 7.16. Sia A un dominio d'integrità, e $a, b \in A$. Si provi che se esistono interi positivi coprimi n, m tali che $a^n = b^m$ e $a^m = b^m$, allora $a = b$.

Esercizio 7.17. Sia A un dominio d'integrità e sia $\emptyset \neq S$ un sottoinsieme *moltiplicativamente chiuso* di A (cioè, per ogni $s_1, s_2 \in S$, $s_1 s_2 \in S$) tale che $0_A \notin S$. Su $A \times S$ si definisca la relazione $\sim$ ponendo $(a, s) \sim (b, t)$ se $at = bs$ (per ogni $a, b \in A$ e $s, t \in S$).

(1) Si provi che $\sim$ è un'equivalenza, e si denoti con A_S l'insieme quoziente. Su A_S si definiscano quindi operazioni di somma e prodotto come nel caso del campo delle frazioni, e si provi che A_S è un dominio d'integrità.

(2) Si definisca un omomorfismo iniettivo $\phi : A \to A_S$.

(3) Si provi che per ogni $s \in S$, $\phi(s)$ è invertibile in A_S.

[Si noti che non si assume $1 \in S$, e quindi si faccia attenzione nel definire correttamente l'identità di A_S e l'omomorfismo ϕ.]

Esercizio 7.18. Sia p un numero primo e sia $S = \{p^n \mid n \in \mathbb{N}\}$. Si provi, con le notazioni dell'esercizio precedente, che $\mathbb{Z}_S$ è isomorfo all'anello $\mathbb{Q}_p$ dell'esercizio 6.4.

Esercizio 7.19. Qual è il campo delle frazioni di $\mathbb{Q}_p$?

7.4 Quaternioni.

Un anello in cui ogni elemento non nullo è invertibile si dice **anello con divisione** o anche *corpo*. Un campo è quindi un anello con divisione commutativo. Il fatto che esistano anelli con divisione non commutativi non è scontato e, come vedremo in questa sezione, la costruzione di esempi del genere non è banale (anche se di anelli con divisione non commutativi ce ne sono in abbondanza). Citiamo, ad esempio, un Teorema di Wedderburn (la cui dimostrazione esula da questo corso), che afferma che ogni anello con divisione finito è commutaivo ed è, quindi, un campo.

L'anello dei **Quaternioni** è il più importante e, storicamente, il primo esempio di anello con divisione non commutativo (cioè che non sia un campo). Esso fu scoperto (o, se preferite, costruito) da W.R. Hamilton nel 1843. Dopo numerosi tentativi di costruire strutture algebriche (campi) che contenessero il campo $\mathbb{C}$ dei complessi, ed avessero dimensione 3 sui reali (i complessi hanno dimensione 2), Hamilton si rese conto che ciò non era possibile, e di dover quindi di dover salire a dimensione 4 e al contempo rinunciare alla commutatività del prodotto. Ma bando alle chiacchere e vediamo la costruzione.

Nell'anello $M_2(\mathbb{C})$ delle matrici quadrate complesse di ordine 2, consideriamo il seguente sottoinsieme:

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} .$$

Dove se $a = x + iy \in \mathbb{C}$ (con $x, y \in \mathbb{R}$), allora $\overline{a} = x - iy$ è il suo **coniugato**. Ricordo le proprietà fondamentali che riguardano i coniugati (vedi sezione 5.2):

- per ogni $a, b \in \mathbb{C}$: $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{ab} = \overline{a}\overline{b}$
- se $a = x + iy \in \mathbb{C}$ allora $a\overline{a} = x^2 + y^2$ è un numero reale positivo, e $a\overline{a} = 0 \Leftrightarrow a = 0$
- $\overline{\overline{a}} = a$ per ogni $a \in \mathbb{C}$ e $\overline{a} = a$ se e solo se $a \in \mathbb{R}$.

Utilizzando tali proprietà si dimostra facilmente che $\mathbb{H}$ è un sottoanello dell'anello $M_2(\mathbb{C})$. $\mathbb{H}$ si chiama *anello dei Quaternioni*. $\mathbb{H}$ non è commutativo: ad esempio

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Osserviamo subito che $\mathbb{H}$ è *un'estensione* di $\mathbb{C}$, e quindi di $\mathbb{R}$; infatti, porre

$$z \mapsto \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$$

definisce un omomorfismo iniettivo $\mathbb{C} \to \mathbb{H}$.

Verifichiamo ora che $\mathbb{H}$ è un anello con divisione. Quello che manca è la seguente

Proposizione 7.7. *In $\mathbb{H}$ ogni elemento non nullo è invertibile.*

Dimostrazione. Sia

$$0_{\mathbb{H}} \neq x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H}$$

(con $a, b \in \mathbb{C}$, $(a, b) \neq (0, 0)$) e sia $d = a\overline{a} - (-\overline{b}b) = Det(x)$. Allora $d = a\overline{a} + \overline{b}b \in \mathbb{R}$ e $d \neq 0$ perchè $(a, b) \neq (0, 0)$, dunque

$$y = \begin{pmatrix} \overline{a}d^{-1} & -bd^{-1} \\ \overline{b}d^{-1} & ad^{-1} \end{pmatrix} = \begin{pmatrix} \overline{a}d^{-1} & -bd^{-1} \\ -\overline{(-bd^{-1})} & \overline{\overline{a}d^{-1}} \end{pmatrix} \in \mathbb{H},$$

e inoltre

$$xy = yx = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{\mathbb{H}} ,$$

quindi x è invertibile in $\mathbb{H}$. ∎

Consideriamo ora i seguenti elementi di $\mathbb{H}$:

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} .$$

Inoltre identifichiamo ogni numero reale α con l'elemento $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ di $\mathbb{H}$. Si verificano facilmente le seguenti uguaglianze:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k} \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i} \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}\ .$$

In particolare, ritroviamo che $\mathbb{H}$ non è commutativo.

Osserviamo infine che se $a = \alpha + i\beta,\ b = \gamma + i\delta \in \mathbb{C}$ (con $\alpha, \beta, \gamma, \delta \in \mathbb{R}$), allora

$$\begin{aligned} \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} &= \begin{pmatrix} \alpha + i\beta & \gamma + i\delta \\ -\gamma + i\delta & \alpha - i\beta \end{pmatrix} = \\ &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} i\beta & 0 \\ 0 & -i\beta \end{pmatrix} + \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix} + \begin{pmatrix} 0 & i\delta \\ i\delta & 0 \end{pmatrix} = \\ &= \alpha \cdot 1 + \beta \cdot \mathbf{i} + \gamma \cdot \mathbf{j} + \delta \cdot \mathbf{k} \end{aligned}$$

e tale scrittura è unica ($\mathbb{H}$ è dunque anche uno spazio vettoriale di dimesione 4 sui reali, con una base costituita da $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$).

Esercizio 7.20. Si determini il centro di $\mathbb{H}$ (vedi esercizio 6.5).

Esercizio 7.21. Il *coniugio* su $\mathbb{H}$ è l'applicazione $\overline{\ \cdot\ } : \mathbb{H} \to \mathbb{H}$ definita da, per ogni $u = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$,

$$\overline{u} = a_0 - a_1 i - a_2 j - a_3 k.$$

La *norma* su $\mathbb{H}$ è l'applicazione $N : \mathbb{H} \to \mathbb{R}$ definita da

$$N(u) = u\overline{u} = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

per ogni $u = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$.
Si provi che la norma è moltiplicativa; ovvero $N(uv) = N(u)N(v)$ per ogni $u, v \in \mathbb{H}$, e e che il coniugio è un *antiautomorfismo* moltiplicativo; ovvero che, per ogni $a, b \in \mathbb{H}$, si ha $\overline{ab} = \overline{b}\overline{a}$.

Esercizio 7.22. Sia $v = a_1 i + a_2 j + a_3 k$. Si osservi che $N(v) = -v^2$. Si concluda che per ogni $0 < r \in \mathbb{R}$, l'equazione $x^2 + r = 0$ ha infinite soluzioni in $\mathbb{H}$.

Esercizio 7.23. Si provi che $\mathbb{H}(\mathbb{Z}) = \{a1 + bi + cj + dk \in \mathbb{H} \mid a, b, c, d \in \mathbb{Z}\}$ è un sottoanello dell'anello dei quaternioni $\mathbb{H}$.

Esercizio 7.24. Sia R un anello tale che i soli ideali destri di R sono $\{0\}$ ed R. Si provi che R è un anello con divisione.

7.5 Esercizi.

Esercizio 7.25. (Omomorfismo di Frobenius) Sia p un primo, e sia R un dominio d'integrità di caratteristica p. Utilizzando la dimostrazione della Proposizione 4.8 si provi che

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

Dedurre da ciò che l'applicazione $\Phi : R \to R$ definita da, per ogni $a \in R$: $\Phi(a) = a^p$ è un omomorfismo di R in se stesso (detto endomorfismo di Frobenius). Provare infine che se R è finito allora Φ è un automorfismo.

Esercizio 7.26. Si definisca un omomorfismo non nullo dell'anello $\mathbb{Z}_{20}$ nell'anello $\mathbb{Z}_5$.

Esercizio 7.27. Siano p, q numeri primi.

(a) Provare che l'applicazione

$$\begin{array}{rccc} \theta : & \mathbb{Z} & \to & \mathbb{Z}_p \times \mathbb{Z}_q \\ & z & \mapsto & (z + p\mathbb{Z}, z + q\mathbb{Z}) \end{array}$$

è un omomorfismo di anelli, e determinare $Ker(\theta)$.

(b) Provare che θ è suriettiva se e solo se $p \neq q$.

Esercizio 7.28. Sia $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_6 \right\}$ l'anello delle matrici quadrate di ordine 2 a coefficienti in $\mathbb{Z}_6$. Si determinino l'ordine di R ed il suo sottoanello fondamentale; si dica se il sottoanello fondamentale di R è un campo.

Esercizio 7.29. Sia R un anello di caratteristica zero e sia $f : \mathbb{Z} \to R$ un omomorfismo suriettivo di anelli; si provi che f è un isomorfismo.

Esercizio 7.30. Sia A un anello commutativo di caratteristica p, dove p è un numero primo, e sia P il sottoanello fondamentale di A. Si provi che se I è un ideale *proprio* di A, allora $I \cap P = \{0_A\}$.

Esercizio 7.31. Trovare le soluzioni di $x^2 = x$ in $\mathbb{Z}/12\mathbb{Z}$, ed in $\mathbb{Z}/11\mathbb{Z}$.

Esercizio 7.32. Determinare elementi invertiibili, elementi nilpotenti e ideali dell'anello $\mathbb{Z}_4 \times \mathbb{Z}_6$.

Esercizio 7.33. Sia R un anello commutativo, e I un suo ideale. Sia

$$D(I) = \{\ x \in R \mid x + x \in I\ \}.$$

a) Si provi che $D(I)$ è un ideale di R.

b) Si consideri l'anello $\mathbb{Z}$ dei numeri interi, e $n \geq 2$. Si provi che $D(n\mathbb{Z}) = n\mathbb{Z}$ se e solo se n è dispari.

Esercizio 7.34. Sia $\varphi : R \longrightarrow S$ un omomorfismo di anelli commutativi, e sia c $\neq 0$ la caratteristica di S. Si dimostri che c divide la caratteristica di R.

Esercizio 7.35. Siano A un anello commutativo, $1 \leq n \in \mathbb{N}$, e $x, y \in M_n(A)$. Si provi che se $xy = 1$ allora $yx = 1$.

Esercizio 7.36. Nell'anello delle matrici quadrate di ordine 2 a coefficienti interi si consideri l'insieme

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}.$$

(a) Si provi che A è un anello (rispetto alle usuali operazioni di somma e di prodotto tra matrici).

(b) Si dimostri che $J = \left\{ \begin{pmatrix} 5x & y \\ 0 & 5z \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\}$ è un ideale di A.

Esercizio 7.37. Sia $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$.

(a) Si provi che R è un anello commutativo (si dimostri infatti che è un sottoanello di $M_2(\mathbb{Q})$).

(b) Si provi che, se D è l'insieme dei divisori dello zero di R, allora $I = D \cup \{0\}$ è un ideale di R.

(c) Si provi che gli ideali di R sono $\{0\}$, I, R.

Esercizio 7.38. Sia $A = \left\{ \begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$. Provare che A è un sottoanello di $M_2(\mathbb{Z})$. Provare quindi che l'applicazione $\phi : A \to \mathbb{Z}$, definita da

$$\phi\left(\begin{pmatrix} a+b & b \\ -b & a-b \end{pmatrix}\right) = a$$

è un omomorfismo suriettivo e determinare il suo nucleo.

Esercizio 7.39. Sia α un numero reale e sia

$$A_\alpha = \left\{ \begin{pmatrix} a & b \\ \alpha b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} .$$

a) Si provi che A_α è un sottoanello commutativo dell'anello $M_2(\mathbb{R})$ delle matrici quadrate di ordine due sui reali.

b) Si provi che A_α è un campo se e solo se $\alpha < 0$.

c) Posto quindi $\alpha = 1$ e $A = A_1$, si provi che l'applicazione $\Phi : A \longrightarrow \mathbb{R}$ definita da

$$\Phi \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b$$

è un omomorfismo di anelli.

Esercizio 7.40. Siano R un anello e $\emptyset \neq X \subseteq R$. Si provi che

$$An_r(X) = \{r \in \mathbb{R} \mid xr = 0 \ \forall x \in X\}$$

è un ideale destro di R, e che se X è un ideale destro, allora $An_r(X)$ è un ideale di R.

Esercizio 7.41. Sia R un anello e sia J un ideale destro proprio (cioè $J \neq R$) di R. Si assuma che J contenga tutti gli ideali destri propri di R e si provi che allora J è un ideale.

Esercizio 7.42. Sia $u \in \mathbb{H}(\mathbb{Z})$. Si provi che le seguenti proprietà sono equivalenti:

(i) u è invertibile in $\mathbb{H}(\mathbb{Z})$;

(ii) $N(u) = 1$;

(ii) $u \in \{\pm 1, \pm i, \pm j, \pm k\}$.

Esercizio 7.43. si verifichi che l'insieme $Q = \{1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ è un gruppo non commutativo (rispetto alla moltiplicazione). Esso è detto *gruppo dei Quaternioni*.

Esercizio 7.44. Sia $y \in \mathbb{H} \setminus \mathbb{R}$. Si provi che esistono $a, b \in \mathbb{R}$ tali che $y^2 + ay + b = 0$. [sugg.: Se $y = a_0 + a_1 i + a_2 j + a_3 k$, considerare $v = y - a_0$ e osservare che $\overline{v} = -v$, quindi $v^2 = \ldots$]

Esercizio 7.45. Sia K un sottoanello di $\mathbb{H}$, con $\mathbb{R} \subseteq K$ e $\mathbb{R} \neq K$. Si provi che esiste $u \in K$ tale che $u^2 = -1$. Si deduca che K contiene un campo isomorfo a $\mathbb{C}$.

Esercizio 7.46. (Anello degli endomorfismi, I) Sia R un anello; denotiamo con $End(R)$ l'insieme di tutti gli endomorfismi della *struttura additiva* di R, ovvero le applicazioni $f : R \to R$ tali che $f(a + b) = f(a) + f(b)$ per ogni $a, b \in \mathbb{R}$.

(a) Si provi che per ogni $f \in End(R)$, $f(0_R) = 0_R$, e che f è iniettivo se e solo se $Ker f = \{a \in R \mid f(a) = 0_R\} = \{0_R\}$.

(b) Si provi che per ogni $a \in R$, l'applicazione $\lambda_a : R \to R$ definita da $\lambda_a(x) = ax$ (per ogni $x \in R$) appartiene a $End(R)$.

(c) Sia $R = \mathbb{Z}$, si provi che ogni elemento di $End(\mathbb{Z})$ è del tipo λ_a per qualche $a \in \mathbb{Z}$.

Esercizio 7.47. (Anello degli endomorfismi, II) Sia R una anello; su $End(R)$ si definisca l'addizione ponendo $(f + g)(a) = f(a) + g(a)$, per ogni $f, g \in End(R)$ ed ogni $a \in R$,

(a) Si provi che $E = (End(R), +, \circ)$ (dove $\circ$ è la composizione di applicazioni) è un anello, con 0_E l'applicazione costante 0, e 1_E l'applicazione identica ι_E.

(b) Sia $f \in End(R)$; si provi che f è invertibile in $End(R)$ se e solo se è biettiva.

Esercizio 7.48. (Anello degli endomorfismi, III) Sia R un anello. Utilizzando opportunamente il punto (b) dell'esercizio 7.46 si definisca un omomorfismo iniettivo $R \to End(R)$. Si provi quindi che se $R = \mathbb{Z}$ oppure $R = \mathbb{Z}_n$ (per qualche $n \geq 2$), allora $R \simeq End(R)$.

Esercizio 7.49. (Anello degli endomorfismi, IV) Sia $R = \mathbb{Z} \times \mathbb{Z}$. Si provi che $End(R) \simeq M_2(\mathbb{Z})$.

Esercizio 7.50. (Anello degli endomorfismi, V) Sia R un anello. Si provi che se $End(R)$ è un campo, allora R è un campo.

Capitolo 8

Fattorizzazioni

In questo capitolo approfondiremo lo studio degli anelli commutativi, ed in special modo dei domini d'integrità, avendo come riferimento le proprietà dell'anello $\mathbb{Z}$ dei numeri interi. In particolare, cercheremo di generalizzare l'idea di fattorizzazione unica. Come si vedrà. il ruolo svolto dal concetto di ideale (ed in particolare di ideale principale) è fondamentale.

8.1 Divisibilità e fattorizzazioni

In queste prime sezioni estenderemo ai domini d'integrità i concetti di divisibilità, primalità. MCD, etc. già introdotti nel caso dell'anello degli interi; mediante tale processo di astrazione ne chiariremo gli aspetti fondamentali.
Cominciamo col generalizzare certe definizioni.

Definizioni. Sia R un anello commutativo, e siano $a, b \in R$.

(1) Diciamo che a *divide* b (o anche a è un fattore di b) se esiste $c \in R$ tale che $ac = b$. In tal caso si scrive $a|b$.

(2) Diciamo che a, b sono *associati* se $a|b$ e $b|a$, e scriviamo allora $a \sim b$.

Osserviamo subito che se u è un elemento invertibile di R allora $u|b$ per ogni $b \in R$: infatti $b = u(u^{-1}b)$.

Se $a, b \in R$ sono associati, esistono $c, d \in R$ tali che $ac = b$ e $bd = a$; da ciò segue $a = a(cd)$ e, per la legge di cancellazione, $cd = 1$; quindi c, d sono invertibili. Viceversa, se u è invertibile allora $a \sim ua$. Quindi a, b sono associati se e solo se differiscono per un fattore invertibile.

Un divisore a di b si dice *proprio* se non è invertibile e non è associato a b.

Questi concetti hanno una immediata interpretazione in termini di ideali principali. Ricordo che, se R è un anello commutativo e $a \in R$, l'ideale principale generato da a è

$$(a) = \{\ ax \mid x \in R\ \},$$

ed è il minimo ideale di R contenente a.

Proposizione 8.1. *Sia R un anello commutativo, e siano $a, b \in R$. Allora*

(1) *$a|b$ se e solo se $(b) \subseteq (a)$.*

(2) *$a \sim b$ se e solo se $(a) = (b)$.*

Dimostrazione. (1) Siano $a, b \in R$. Allora

$$(b) \subseteq (a) \;\Leftrightarrow\; b \in (a) \;\Leftrightarrow\; (\text{esiste } c \in R :\; b = ac\;) \;\Leftrightarrow\; a|b\;.$$

(2) Discende immediatamente da (1) e dalla definizione di elementi associati. ∎

Definizione. Un elemento a di un dominio d'integrità R si dice **irriducibile** se

(i) a non è 0_R e non è invertibile;

(ii) i soli divisori di a sono gli invertibili e gli elementi associati (detto altrimenti: a non ha divisori propri).

Quindi, gli elementi irriducibili di $\mathbb{Z}$ sono i numeri primi, mentre un campo non contiene elementi irriducibili.

Fattorizzazione in irriducibili. Si dice che un elemento a di un dominio d'integrità R ammette una *fattorizzazione in irriducibili* se a si può scrivere come prodotto di irriducibili di R, e si dice che la fattorizzazione è *essenzialmente unica* se due diverse decomposizioni di a come prodotto di irriducibili hanno lo stesso numero di fattori e, a meno di scambiare i termini di una delle due fattorizzazioni, i fattori irriducibili delle due decomposizioni sono a due a due tra loro associati. Detto formalmente:

La fattorizzazione $a = s_1 s_2 \dots s_n$ come prodotto di elementi irriducibili è essenzialmente unica se per ogni altra fattorizzazione $a = r_1 r_2 \dots r_k$ con r_i irriducibili, si ha $k = n$ ed esiste una permutazione π (cioè una biezione in se stesso) di $\{1, 2, \dots, n\}$ tale che s_i è associato a $r_{\pi(i)}$ per ogni $i = 1, 2, \dots, n$.

Un dominio d'integrità R si dice **Dominio a Fattorizzazione Unica** (abbreviato: UFD) se ogni elemento non nullo e non invertibile di R ammette una fattorizzazione in irriducibili ed essa è essenzialmente unica.

L'anello $\mathbb{Z}$ è un UFD. Per il momento è il solo che conosciamo; ma nel prossimo capitolo vedremo quanto più ampia, e quanto importante, sia questa classe di anelli. Il risultato principale di questa sezione è una caratterizzazione degli UFD, che utilizzeremo nella prossima sezione per provare il fatto fondamentale che ogni dominio a ideali principali è un dominio a fattorizzazione unica.
Cominciamo osservando che per ogni elemento non nullo e non invertibile di un UFD, il numero di fattori che compaiono in ogni sua fattorizzazione in irriducibili è fissato (e dipende solo dall'elemento). Da questo segue facilmente il Lemma che segue, e che ci sarà utile nella dimostrazione del Teorema principale.

Lemma 8.2. *Sia $a \in R$ un elemento non nullo e non invertibile di un UFD, e sia $a = s_1 s_2 \dots s_n$ una sua fattorizzazione in irriducibili. Sia b un divisore proprio di a. Si provi che il numero di fattori irriducibili in una fattorizzazione di b è $\leq n - 1$.*

Dimostrazione. Esercizio. ∎

Ci occorre ora un'altra definizione.

Definizione. Un elemento a di un dominio d'integrità R si dice **primo** se

(i) a non è 0_R e non è invertibile;

(ii) per ogni $b, c \in R$, se $a|bc$ allora $a|b$ oppure $a|c$.

Chiaramente la terminologia è ereditata da $\mathbb{Z}$. Nell'anello $\mathbb{Z}$ elementi primi ed elementi irriducibili coincidono. Questo non vale in generale, ed una delle cose che ci servono è provare che negli UFD tale coincidenza continua a sussistere. Per una direzione è sufficiente assumere che l'anello sia un dominio d'integrità.

Lemma 8.3. *Sia R un dominio d'integrità. Allora ogni elemento primo di R è irriducibile.*

Dimostrazione. Sia a un elemento primo del dominio d'integrità R. Allora, per definizione, a non è nullo e non è invertibile. Sia quindi b un divisore di a; allora esiste $c \in R$ tale che $a = bc$. Per la definizione di elemento primo si ha allora $a|b$ oppure $a|c$. Nel primo caso b è associato ad a, nel secondo caso c è associato ad a e quindi b è invertibile. Dunque i soli divisori di a sono o associati ad a oppure gli invertibili, e pertanto a è un irriducibile. ∎

Il viceversa vale negli UFD: questo è il punto (1) del seguente risultato.

Lemma 8.4. *Sia R un Dominio a Fattorizzazione Unica. Allora*

(1) *Ogni elemento irriducibile di R è un primo.*

(2) *Non esistono catene infinite $a_0, a_1, a_2, \ldots$ di elementi di R tali che, per ogni i, a_{i+1} è un divisore proprio di a_i.*

Dimostrazione. (1) Sia a un elemento irriducibile del dominio a fattorizzazione unica R. Allora a è non nullo e non invertibile per definizione. Siano $b, c \in R$ tali che $a|bc$, e sia $u \in R$ tale che $ad = bc$. Se b è invertibile allora $adb^{-1} = c$, e quindi $a|c$; allo stesso modo, se c è invertibile allora $a|b$. Supponiamo quindi che né b né c siano invertibili. Allora entrambi ammettono una fattorizzazione in irriducibili

$$b = s_1 s_2 \ldots s_n \qquad e \qquad c = r_1 r_2 \ldots r_m$$

Osservo che allora d non è invertibile; perché, se lo fosse, si avrebbe $a = d^{-1}bc$, ed, essendo a irriducibile, uno tra b e c dovrebbe essere invertibile. Quindi d non è invertibile, e pertanto ammette una fattorizzazione $d = q_1 q_2 \ldots q_k$, in fattori irriducibili. Allora

$$aq_1 q_2 \ldots q_k = s_1 s_2 \ldots s_n r_1 r_2 \ldots r_m$$

sono due fattorizzazioni in irriducibili dello stesso elemento $bc = ad$. Per la essenziale unicità della fattorizzazione deve essere, in particolare, a associato ad un s_i o ad un r_j; nel primo caso $a|b$ e nel secondo caso $a|c$.
In ogni caso quindi $a|b$ oppure $a|c$, dunque a è un elemento primo.

(2) Siano $a_0, a_1, a_2, \ldots$ elementi di R tali che, per ogni i, a_{i+1} è un divisore proprio di a_i. Per ogni i, sia n_i il numero di fattori in una decomposizione di a_i in irriducibili. Allora, per il Lemma 8.2, si ha $n_0 > n_1 > n_2 > \ldots$; quindi per qualche $k \leq n_0$ si deve avere $n_k = 1$, che significa che a_k è irriducibile. Poichè un elemento irriducibile non ha divisori propri, la catena si arresta a a_k. ∎

Il bello è che questo Lemma si può invertire, fornendo così la caratterizzazione degli UFD che cerchiamo.

Teorema 8.5. *Sia R un dominio d'integrità. Allora R è un dominio a fattorizzazione unica se e solo se soddisfa alle proprietà (1) e (2) del Lemma precedente.*

Dimostrazione. Un verso è proprio il Lemma 8.4. Supponiamo quindi che R sia un dominio d'integrità che soddisfa alle proprietà (1) e (2) del Lemma 8.4, e proviamo che R è un UFD.
Sia a un elemento non nullo e non invertibile di R; cominciamo con il provare che

1) *esiste un irriducibile b_1 che divide a.*

Se a è irriducibile, allora $b_1 = a$. Altrimenti, $a = a_0$ ha un divisore proprio a_1; se questo è irriducibile si pone $b_1 = a_1$, altrimenti a_1 ha un divisore proprio a_2; ancora, se a_2 è irriducibile si pone $b_1 = a_2$ (chiaramente $a_2 | a_0 = a$); altrimenti si prosegue trovando un divisore proprio a_3 di a_2. Per la proprietà (2) questo processo non può proseguire indefinitamente: si arriverà quindi dopo un numero finito k di passi ad un elemento a_k irriducibile che divide ogni a_i per $0 \leq i \leq k$. In particolare a_k divide $a_0 = a$ e si ha $b_1 = a_k$.

2) *a ha una fattorizzazione in irriducibili.*

Se a è irriducible siamo a posto. Supponiamo che a non sia irriducibile; allora per il punto 1) esiste un divisore irriducibile b_1 di $a = a_0$. Sia $a_1 \in R$ tale che $a = b_1 a_1$; poiché a non è irriducibile, a_1 non è invertibile; se a_1 è irriducibile allora $a = b_1 a_1$ è la fattorizzazione cercata; altrimenti ripetiamo su a_1 le operazioni fatte su a, trovando $a_1 = b_2 a_2$ con b_2 irriducibile. Se a_2 è irriducibile allora $a = b_1 b_2 a_2$ è la fattorizzazione cercata; altrimenti ripetiamo su a_2 le stesse operazioni. In questo modo otteniamo una catena $a = a_0$, a_1, $a_2, \ldots$ di elementi di R ognuno dei quali è un divisore proprio del precedente, e tale che, per ogni i, $a_i = b_{i+1} a_{i+1}$ con b_{i+1} irriducibile. Per la proprietà (2) tale catena si arresta ad un termine irriducibile $a_n = b_{n+1}$; ma allora

$$a = a_0 = b_1 a_1 = b_1 b_2 a_2 = \ \ldots = b_1 b_2 \ldots b_{n-1} b_n$$

e quindi a ammette una fattorizzazione in irriducibili.

3) *unicità della fattorizzazione in irriducibili.*

Consideriamo due fattorizzazioni in irriducibili dello stesso elemento (non nullo e non invertibile):

$$r_1 r_2 r_3 \ \ldots \ r_n = s_1 s_2 s_3 \ \ldots \ s_k \qquad (*)$$

e, procedendo per induzione su n, mostriamo che sono essenzialmente la stessa decomposizione.
Se $n = 1$ allora $r_1 = s_1 s_2 s_3 \ldots s_k$ è irriducibile, quindi $k = 1$ e $s_1 = r_1$. Sia $n \geq 2$ e supponiamo per ipotesi induttiva che due fattorizzazioni dello stesso elemento siano

essenzialmente la stessa se una delle due è costituita da al più $n-1$ fattori. Ora, r_1 è irriducibile e quindi, per la proprietà (1), r_1 è primo. Poiché $r_1|s_1s_2\dots s_k$ si ha allora che r_1 divide un s_j; a meno di riordinare i termini $s_1, s_2, \dots, s_m$ nel prodotto, possiamo assumere che r_1 divida s_1. Poiché r_1, s_1 sono irriducibili si ha quindi $r_1 \sim s_1$, dunque $s_1 = r_1 u$ con u invertibile. Allora

$$r_1 r_2 r_3 \ \dots \ r_n = r_1 u s_2 s_3 \ \dots \ s_k = r_1 s_2' s_3' \ \dots \ s_k'$$

con $s_2' = us_2 \sim s_2$ e $s_j' = s_j$ per $3 \le j \le k$. Per la proprietà di cancellazione possiamo dedurre che

$$r_2 r_3 \ \dots \ r_n = s_2' s_3' \ \dots \ s_k'$$

Applicando quindi l'ipotesi induttiva, otteniamo $n = k$ e, a meno di riordinare i fattori s_j', $r_j \sim s_j'$ per ogni $2 \le j \le n$. Dunque le fattorizzazioni $(*)$ da cui siamo partiti sono essenzialmente la stessa. Per il principio di induzione l'essenziale unicità delle fattorizzazioni è provata per ogni numero n di fattori irriducibili, così completando la dimostrazione che R è un UFD. ∎

Esempio. (dove proviamo che esistono domini d'integrità che non sono UFD) Scriviamo $\sqrt{-5} = i\sqrt{5}$ e consideriamo il sottoinsieme dei numeri complessi

$$\mathbb{Z}[\sqrt{-5}] = \{\ a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\ \}\ .$$

Si provi per esercizio che $\mathbb{Z}[\sqrt{-5}]$ è un sottoanello di $\mathbb{C}$ (e quindi è un dominio d'integrità). Per studiare le fattorizzazioni in $\mathbb{Z}[\sqrt{-5}]$, introduciamo la funzione di *norma* $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$,

$$N(z) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2\ .$$

Le solite proprietà sono di verifica immediata:

i) $N(zz_1) = N(z)N(z_1)$ per ogni $z, z_1 \in \mathbb{Z}[\sqrt{-5}]$;
ii) $z \neq 0 \ \Rightarrow\ N(z) > 0$;
iii) $N(z) = 1 \ \Leftrightarrow\ z = \pm 1$.

Con queste si prova facilmente che $1 + \sqrt{-5}$ è un elemento irriducibile di $\mathbb{Z}[\sqrt{-5}]$. Infatti se $1 + \sqrt{-5} = zz_1$ con $z, z_1 \in \mathbb{Z}[\sqrt{-5}]$ e $z = a + b\sqrt{-5}$, allora

$$6 = N(1 + \sqrt{-5}) = N(zz_1) = N(z)N(z_1)\ .$$

Se $N(z) = 1$ allora $z = \pm 1$ è invertibile, similmente se $N(z) = 6$ allora $z_1 = \pm 1$; altri casi non se ne possono verificare, poichè $N(z) = a^2 + 5b^2 \neq 2, 3$ per ogni $a, b \in \mathbb{Z}$. In modo analogo si dimostra che $2,\ 3,\ 1 - \sqrt{-5}$ sono irriducibili in $\mathbb{Z}[\sqrt{-5}]$. Quindi

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

sono due fattorizzazioni di 6 in irriducibili che non differiscono per fattori invertibili (gli invertibili di $\mathbb{Z}[\sqrt{-5}]$ sono $1, -1$). Dunque $\mathbb{Z}[\sqrt{-5}]$ non è un dominio a fattorizzazione unica.

Torniamo alla teoria generale, ed estendiamo ai domini d'integrità il concetto di MCD.

Definizione. Siano a, b elementi di un dominio d'integrità R; allora $d \in R$ si dice un **massimo comun divisore** (MCD) di a e b se $d|a$, $d|b$, e per ogni $d' \in R$, tale che $d'|a$ e $d'|b$, si ha $d'|d$.

Il massimo comun divisore, se esiste, è individuato a meno di associati. Infatti, se d, c sono due MCD di a e b, allora, per defnizione, $c|d$ e $d|c$, quindi esiste un invertbile $u \in R$ tale che $c = ud$.
Ma non sempre un MCD esiste. Nell'anello $\mathbb{Z}[\sqrt{-5}]$ dell'esempio di sopra, 2 e $1+\sqrt{-5}$ sono divisori comuni di $a = 6$ e di $b = 2(1+\sqrt{-5})$; se $d = x + y\sqrt{-5}$ fosse un massimo comun divisore di a e b, allora $N(d)|(N(a), N(b)) = (36, 24) = 12$ e, inoltre $4 = N(2)|N(d)$ e $6 = N(1+\sqrt{-5})|N(d)$ (dato che $2|d$ e $(1+\sqrt{-5})|d$); quindi deve essere $N(d) = x^2 + 5y^2 = 12$ che è impossibile per $x, y \in \mathbb{Z}$.

Sia R sia un dominio a fattorizzazione unica. Per ogni classe di elementi irriducibili associati fissiamo uno ed un solo elemento, e chiamiamo P l'insieme degli elementi così prescelti. In ogni classe la scelta dell'elemento è arbitraria, ma in certi casi può essere effetuata in modo uniforme. Ad esempio, nel caso di $\mathbb{Z}$ possiamo prendere come P l'insieme numeri primi positivi.
Allora ogni $a \in R$ non nullo si può scrivere in modo unico (a meno dell'ordine dei fattori) come il prodotto

$$a = up_1^{n_1}p_2^{n_2}p_3^{n_3} \ \dots \ p_k^{n_k}$$

con u un invertibile di R, $p_i \in P$ e $n_i \in \mathbb{N}$ per $i = 1, 2, \dots, k$ (osserviamo che se a è invertibile basta porre $n_i = 0$ per ciascun i).
Ora, siano $a = up_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$ e $c = wp_1^{s_1}p_2^{s_2}\dots p_k^{s_k}$ elementi non nulli di R, fattorizzati mediante gli elementi di P, con u, w invertbili, e dove abbiamo eventualmente aggiunto potenze di esponente zero per quegli irriducibili che sono divisori di uno solo dei due elementi. Supponiamo che c divida a; allora esiste $r = w'p_1^{r_1}p_2^{r_2}\dots p_k^{r_k} \in R$ tale che $a = cr$ quindi

$$a = ww'p_1^{s_1+r_1}p_2^{s_2+r_2}\dots p_k^{s_k+r_k}$$

da cui segue in particolare $r_i \le n_i$ per ogni $i = 1, 2 \dots, k$.

Siano ora $a, b \in R$i. Se uno dei due è zero, allora l'altro è un MCD di a e b. Supponiamo quindi che siano entrambi non nulli e fattorizziamoli mediante gli elementi di P:

$$a = up_1^{n_1}p_2^{n_2}\dots p_k^{n_k} \qquad b = vp_1^{m_1}p_2^{m_2} \ \dots p_k^{m_k}$$

con u, v invertibili ed il solito accorgimento sugli esponenti. Consideriamo ora l'elemento

$$d = p_1^{\min\{n_1,m_1\}}p_2^{\min\{n_2,m_2\}} \ \dots \ p_k^{\min\{n_k,m_k\}} \ ;$$

chiaramente d divide sia a che b, e dall'osservazione fatta sopra segue facilmente che e d è un MCD di a e b. Abbiamo quindi provato:

Proposizione 8.6. *Sia R un UFD. Allora ogni coppia di elementi non nulli di R ammette un massimo comun divisore.*

Esercizio 8.1. Sia R un dominio d'integrità tale che ogni coppia di elementi non nulli di R ammette un MCD. Siano $a, b, c \in R \setminus \{0\}$ e sia d un MCD di a, b. Si provi che dc è un MCD di ac, bc.

Soluzione. Sia d_1 un MCD di ac, bc; poichè dc divide sia ac che bc, si ha $dc|d_1$. Sia $e \in R$ tale che $d_1 = dce$, e siano $r, s \in R$ tali che $ac = d_1r$, $bc = d_1s$. Allora $ac = dcer$ e quindi, per la legge di cancellazione, $a = der$, dunque $de|a$; similmente $b = des$ e dunque $de|b$. Da ciò segue $de|d$, che implica che e è invertibile. Quindi $dc \sim d_1$ e pertanto dc è un MCD di ac, bc.

Esercizio 8.2. Usando l'esercizio 8.1, si provi che se R è un dominio d'integrità in cui ogni coppia di elementi non nulli di R ammette un MCD, allora ogni elemento irriducibile di R è primo.

Esercizio 8.3. 1) Dire quali fra gli elementi 5, 7, 11, 29 sono irriducibili in $\mathbb{Z}[\sqrt{-5}]$.
2) Si dia un esempio di un elemento irriducibile di $\mathbb{Z}[\sqrt{-5}]$ che non è primo.
3) Si provi che $\mathbb{Z}[\sqrt{-5}]$ soddisfa alla proprietà (2) del Lemma 8.4.

Esercizio 8.4. Si provi che $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ è un dominio d'integrità, ma non è a fattorizzazione unica.

Esercizio 8.5. Si dia una definizione di *minimo comune multiplo* in un dominio d'integrità. Quindi si provi che in UFD ogni coppia di elementi non nulli ammette un minimo comune multiplo.

8.2 Ideali massimali e ideali primi

In questa sezione introduciamo due importanti tipi di ideali di un anello che, come vedremo, sono strettamente legati alle proprietà di fattorizzazione. Nel prossimo capitolo svolgeranno un ruolo ancor più importante nella costruzione di nuovi campi e nello studio delle estensioni algebriche del campo $\mathbb{Q}$ dei razionali..

Definizione. Un ideale I di un anello commutativo R si dice **ideale primo** se

(i) $I \neq R$,

(ii) per ogni $a, b \in R$, se $ab \in I$ allora $a \in I$ o $b \in I$.

Ad esempio, l'ideale nullo $\{0_R\}$ è un ideale primo dell'anello commutativo R se e solo se R è un dominio d'integrità (provarlo per esercizio).

Esempio. Consideriamo l'anello $\mathbb{Z}[\sqrt{-5}]$ descritto nella sezione precedente, e i suoi ideali principali (5) e $(\sqrt{-5})$. Si ha $(5) = \{a + b\sqrt{-5} \mid a, b \in 5\mathbb{Z}\}$, e, osservando che, per ogni $u, v \in \mathbb{Z}$, $5u + v\sqrt{-5} = \sqrt{-5}(v - u\sqrt{-5})$ si deduce che $(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a \in 5\mathbb{Z}\}$. L'ideale (5) non è primo: infatti, ad esempio $\sqrt{-5} \notin (5)$ ma $\sqrt{-5}^2 \in (5)$. Invece l'ideale $(\sqrt{-5})$ è primo: infatti, siano $x = a + b\sqrt{-5}, y = c + d\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ tali che

$$(\sqrt{-5}) \ni xy = (ac - 5bd) + (ad + bc)\sqrt{-5}\,:$$

allora $5 \mid ac - 5bd$, e quindi $5 \mid ac$; da ciò segue $5 \mid a$, oppure $5 \mid b$; dunque $x \in (\sqrt{-5})$, oppure $y \in (\sqrt{-5})$.

Osserviamo subito che in $\mathbb{Z}$ gli ideali primi non nulli sono tutti e soli quelli del tipo $p\mathbb{Z}$, con p un numero primo. Questo non è un caso; infatti gli ideali primi di un dominio d'integrità sono strettamente correlati agli elementi primi dell'anello stesso.

Proposizione 8.7. *Sia R un dominio d'integrità, e sia $0_R \neq a \in R$ Allora a è un elemento primo se e solo se (a) è un ideale primo.*

Dimostrazione. Sia $a \neq 0_R$ un elemento primo del dominio d'integrità R. Allora, per definizione a non è invertibile, e quindi $(a) \neq R$. Siano ora $x, y \in R$ tali che $xy \in (a)$. Allora $a|xy$; poiché a è primo, da ciò segue che $a|x$, oppure $a|y$. Nel primo caso $x \in (a)$, ed altrimenti $y \in (a)$. Dunque (a) è un ideale primo.
Viceversa, sia $0_R \neq a \in R$, e supponiamo che l'ideale (a) sia primo. Allora $(a) \neq R$, e quindi a non è invertibile. Se $x, y \in R$ sono tali che $a|xy$, allora $xy \in (a)$. Poiché (a) è un ideale primo, da ciò segue che $x \in (a)$, oppure $y \in (a)$. Nel primo caso $a|x$, e nel secondo $a|y$. Dunque a è un elemento primo. ∎

Osserviamo che, se R è un dominio d'integrità, allora (0_R) è un ideale primo, che non è compreso tra quelli descritti nella Proposizione 8.7.

Definizione. Un ideale I di un anello R si dice **ideale massimale** se

(i) $I \neq R$,

(ii) per ogni ideale J : $I \subseteq J \subseteq R \quad \Rightarrow \quad J = I$ o $J = R$.

In altri termini, un ideale I di un anello R è massimale se e solo se è proprio ed i soli ideali compresi tra I ed R sono I stesso ed R. Il Teorema 6.12 dice che un anello commutativo R è un campo se e solo se l'ideale nullo $\{0_R\}$ è massimale.

Esempio. Nell'anello $\mathbb{R}^{\mathbb{R}}$, fissato $r \in \mathbb{R}$, consideriamo l'ideale $I_r = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(r) = 0\}$. I_r è un ideale massimale. Infatti è chiaramente proprio. Supponiamo che J sia un ideale di $\mathbb{R}^{\mathbb{R}}$ con $I \subseteq J$ e $I_r \neq J$. Allora esiste $g \in J \setminus I$; quindi $g(r) \neq 0$. Sia e_r l'applicazione data da $e_r(r) = 0$ e $e_r(x) = 1$ se $x \neq r$. Allora $e_r \in I \subseteq J$ e, poiché J è un ideale, si ha che anche $e_r + g^2$ appartiene J. Ma, come si constata subito, $e_r + g^2$ non assume mai valore 0, ed è quindi un elemento invertibile di $\mathbb{R}^{\mathbb{R}}$. Dunque J contiene un elemento invertibile e pertanto $J = \mathbb{R}^{\mathbb{R}}$. Questo prova che J è un ideale massimale.

L'esempio di sopra non è un dominio d'integrità. Vediamo cosa succede in $\mathbb{Z}$:

Proposizione 8.8. *Gli ideali massimali di $\mathbb{Z}$ sono tutti e soli gli insiemi del tipo $p\mathbb{Z}$ con p un numero primo.*

Dimostrazione. Sia p un numero primo. Allora $p\mathbb{Z}$ è un ideale proprio di $\mathbb{Z}$. Sia ora $n\mathbb{Z}$ (con $n \geq 1$) un altro ideale di $\mathbb{Z}$ contenente $p\mathbb{Z}$. Allora, per la Proposizione 8.1, n divide p. Ne consegue che $n = 1$ oppure $n = p$. Nel primo caso $n\mathbb{Z} = \mathbb{Z}$, e nel secondo $n\mathbb{Z} = p\mathbb{Z}$. Dunque i soli ideali di $\mathbb{Z}$ che contengono $p\mathbb{Z}$ sono $\mathbb{Z}$ e lo stesso $p\mathbb{Z}$; quindi $p\mathbb{Z}$ è un ideale massimale.
Viceversa sia $m\mathbb{Z}$ (con $m \geq 1$) un ideale massimale di $\mathbb{Z}$. In particolare $m\mathbb{Z} \neq \mathbb{Z}$ e quindi $m \neq 1$. Supponiamo che q sia un divisore primo di m. Allora, per la Proposizione 8.1, $m\mathbb{Z} \subseteq q\mathbb{Z}$. Siccome $m\mathbb{Z}$ è massimale, e $q\mathbb{Z} \neq \mathbb{Z}$, deve essere $q\mathbb{Z} = m\mathbb{Z}$. Ma allora $m|q$, e dunque $m = q$, che è un numero primo. ∎

Segue dalle proposizioni precedenti che nell'anello $\mathbb{Z}$ l'insieme degli ideali primi diversi da (0) coincide con quello degli ideali massimali. Come vedremo nella prossima sezione, questa è una proprietà che vale in ogni dominio a ideali principali, ma non in generale nei domini d'integrità.
C'è comunque una relazione tra ideali primi e ideali massimale che sussiste in ogni anello commutativo.

Proposizione 8.9. *Sia R un anello commutativo. Allora ogni ideale massimale di R è un ideale primo.*

Dimostrazione. Sia I un ideale massimale dell'anello commutativo R. Allora $I \neq R$ per definizione. Siano $a, b \in R$ tali che $ab \in I$, e supponiamo che $b \notin I$. Allora l'ideale (b) non è contenuto in I, e quindi l'ideale $(b) + I$ contiene propriamente I. Poiché I è massimale, si ha quindi $R = (b) + I$. In particolare, esistono $x \in R$ e $y \in I$ tali che $1 = bx + y$. Quindi $a = a(bx + y) = (ab)x + ay$ appartiene ad I. Dunque, I è un ideale primo. ∎

Questa Proposizione in genere non si inverte. Esempi banali si trovano considerando domini d'integrità che non siano campi (ad esempio, $\mathbb{Z}$): in tali casi l'ideale nullo $\{0\}$ è primo ma non è massimale. Per degli esempi riferiti ad ideali non nulli si vedano gli esercizi 8.6 e 8.23 (in questi esercizi l'anello non è un dominio d'integrità; esempi in domini d'integrità in cui esistono ideali primi che non sono massimali, li vedremo nel prossimo capitolo).

Ricordo che un dominio d'integrità si dice **Dominio a Ideali Principali** (abbreviato PID) se ogni suo ideale è principale; ovvero se per ogni ideale I di R esiste un elemento $a \in I$ tale che $I = (a)$. Con la prossima proposizione vediamo come la Proposizione 8.8 si estenda ad un PID.

Proposizione 8.10. *Sia R un dominio a ideali principali, e sia $0 \neq a \in R$. Allora a è un elemento irriducibile se e solo se (a) è un ideale massimale di R.*

Dimostrazione. Sia a un elemento irriducibile del dominio a ideali principali R. Allora a non è invertibile e quindi (a) è un ideale proprio di R. Sia J ideale di R con $(a) \subseteq J$. Poichè ogni ideale di R è principale, esiste $b \in R$ tale che $J = (b)$. Per la Proposizione 8.1, $b|a$. Poichè a è irriducibile si ha che b è associato ad a oppure è un invertibile. Nel primo caso $(b) = (a)$, nel secondo caso $(b) = R$. Quindi (a) è un ideale massimale.

Viceversa, supponiamo che per un $0 \neq a \in R$ sia (a) ideale massimale di R e proviamo che a è irriducibile. a non è invertibile perchè (a) è un ideale proprio. Sia $b \in R$ un divisore di a. Allora per la Proposizione 8.1, $(a) \subseteq (b)$. Poichè (a) è massimale si ha $(b) = (a)$ oppure $(b) = R$. Nel primo caso $b \sim a$, e nel secondo caso b è invertibile. Quindi a è un irriducibile. ∎

Esercizio 8.6. Sia $A = \mathbb{Z}^{\mathbb{R}}$ l'anello delle applicazioni da $\mathbb{R}$ in $\mathbb{Z}$. Si provi che

$$I = \{f \in \mathbb{Z}^{\mathbb{R}} \mid f(0) = 0\}$$

è un ideale primo, ma non massimale di A.

Esercizio 8.7. Ricordo che un elemento a di un anello R si dice *nilpotente* se esiste un intero $n \geq 1$ (che dipende da a) tale che $a^n = 0_R$. Si provi che se R è un anello commutativo, allora gli elementi nilpotenti di R sono contenuti nell'intersezione di tutti gli ideali primi di R.

Esercizio 8.8. Sia R un anello commutativo e sia

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

una catena (infinita) di ideali primi di R. Si provi che $\bigcup_{i\in\mathbb{N}} I_i$ è un ideale primo di R.

Esercizio 8.9. Sia I un ideale proprio dell'anello commutativo R. Si dimostri che I è massimale se e solo se per ogni a $\in R \setminus I$ esiste $x \in R$ tale che $1 - \text{ax} \in I$.

Esercizio 8.10. Sia $\phi : A \to B$ un omomorfismo di anelli commutativi.

(a) Si provi che se J è un ideale primo (massimale) di B, allora $\phi^{-1}(J)$ è un ideale primo (rispett. massimale) di A.

(b) Si provi che se ϕ è suriettivo e I è un ideale primo (massimale) di A, allora $\phi(I)$ è un ideale primo (rispett. massimale) di B.

Esercizio 8.11. Sia $n \geq 2$. Si provi che gli ideali primi di $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ sono massimali.

8.3 Domini a Ideali Principali

Vediamo subito il risultato fondamentale di questa sezione.

Teorema 8.11. *Ogni Dominio a Ideali principali è un dominio a Fattorizzazione Unica.*

Dimostrazione. Sia R un PID. Proviamo che R soddisfa le condizioni (1) e (2) del Lemma 8.4.

(1) Siano $a_0, a_1, a_2, \ldots$ elementi di R tali che, per ogni i, a_{i+1} è un divisore proprio di a_i. Allora, per la Proposizione 8.1, in R c'è la catena di ideali

$$(a_0) \subset (a_1) \subset (a_2) \subset (a_3) \subset \ldots$$

in cui ogni inclusione è propria. Sia

$$I = \bigcup_i (a_i) \ .$$

Si verifica facilmente che I è un ideale di R. (Inoltre $I \neq R$; infatti se fosse $I = R$, allora $1_R \in (a_i)$ per qualche i, il che implica $(a_i) = R$, quindi a_i è invertibile, contro l'assunzione che sia un divisore proprio di a_{i-1}).
Poiché R è un PID, esiste un elemento $b \in R$ non invertibile tale che $I = (b)$. Ora, $b \in (b) = \bigcup_i (a_i)$ e quindi $b \in (a_n)$ per qualche n, che comporta $I = (a_n)$; in particolare $(a_n) = (a_{n+1})$ e dunque la catena si arresta con a_n.

(2) Sia a un elemento irriducibile di R. Allora, per la Proposizione precedente, (a) è un ideale massimale di R, e quindi per la Proposizione 8.9, (a) è un ideale primo. Per la Proposizione 8.7, si conclude che a è un elemento primo.

Per il Teorema 8.5, R è dunque un dominio a fattorizzazione unica. ∎

Domini Euclidei. La nozione di dominio euclideo fornisce un metodo operativo per provare (quando funziona) che certi anelli sono domini a ideali principali;

Un dominio d'integrità R si dice *Dominio Euclideo* se esiste una applicazione

$$\delta : R \setminus \{0\} \ \to \ \mathbb{N}$$

(detta *valutazione euclidea*) con la seguente proprietà:

per ogni $a, b \in R,\ b \neq 0$ esistono $q, r \in R$ tali che

$$\begin{array}{ll} \text{(i)} & a = qb + r \\ \text{(ii)} & r = 0 \quad \text{oppure} \quad \delta(r) < \delta(b)\ . \end{array}$$

(osserviamo che non richiediamo l'unicità di q, r).

È un dominio euclideo l'anello $\mathbb{Z}$, con valutazione $\delta(z) = |z|$ per ogni $z \in \mathbb{Z} \setminus \{0\}$. La dimostrazione che $\mathbb{Z}$ è un dominio a ideali principali è stata possibile proprio utilizzando la divisione con resto. Un argomento analogo funziona per i domini euclidei in generale (ed è il motivo per cui questo concetto è stato introdotto).

Teorema 8.12. *Ogni Dominio Euclideo è un Dominio a Ideali Principali.*

Dimostrazione. Come detto, la dimostrazione ricalchi quella data per $\mathbb{Z}$ (Teorema 6.9), sostituendo al valore assoluto la generale valutazione euclidea.
Sia quindi R un dominio euclideo e δ una sua valutazione. Sia I un ideale di R. Se I è banale, allora $I = (0_R)$. Supponiamo pertanto $\{0_R\} \neq I$. Allora l'insieme $S = \{\delta(a) \mid 0_R \neq a \in I\}$ è un sottoinsieme non vuoto di $\mathbb{N}$, che ha dunque un minimo. Sia $b \in I$ tale che $\delta(b) = \min S$. Proviamo che $I = (b)$. Un'inclusione ($(b) \subseteq I$) è ovvia. Sia quindi $a \in I$. Per la proprietà euclidea, esistono $q, r \in R$ tali che $a = qb + r$, e $\delta(r) < \delta(b)$ oppure $r = 0_R$.
Ma $r = a - qb \in I$, e quindi, per la scelta di b, non può essere $\delta(r) < \delta(b)$. Dunque, $r = 0_R$, e pertanto $a = qb \in (b)$. Ciò prova che $I \subseteq (b)$, e dunque che $I = (b)$ (osserviamo ancora che b è un elemento non nullo di I con *valutazione minima* tra gli elementi di I). ∎

Osservazione. Non tutti i domini a ideali principali sono domini euclidei. Questo è piuttosto difficile da provare: infatti per stabilire che un certo dominio a ideali principali A non è euclideo, occorre provare che non ammette valutazioni euclidee, ovvero che *qualsiasi* applicazione $A \setminus \{0\} \to \mathbb{N}$ non soddisfa la proprietà richesta (il che, si intuisce, non è facile). Un esempio di PID che non è euclideo è l'anello $\mathbb{Z}[\sqrt{-19}]$.

Massimo comun divisore. Abbiamo già osservato che in un dominio a fattorizzazione unica A, esiste sempre il massimo comun divisore tra due elementi. Se inoltre A è un dominio a ideali principali, allora le proprietà del M.C.D. assomigliano molto a quelle per i numeri interi. Infatti, siano a, b elementi di un dominio a ideali principali A, e sia d un loro M.C.D. Allora, $d|a$ e $d|b$ e dunque, per la Proposizione 8.1, $(a) \subseteq (d)$ e $(b) \subseteq (d)$; quindi $(a) + (b) \subseteq (d)$. Ora, $(a) + (b)$ è un ideale di A (è l'ideale generato da $\{a, b\}$); poiché A è un P.I.D. esiste $c \in A$ tale che $(a) + (b) = (c)$. Dunque $(c) \subseteq (d)$; sempre per la Proposizione 8.1, $c|a$ e $c|d$, e dunque (per la definizione di massimo

comun divisore) $c|d$, ovvero $(d) \subseteq (c)$. Quindi $(c) = (d)$, dunque $(d) = (a) + (b)$, e pertanto concludiamo che *esistono* $\alpha, \beta \in A$ *tali che* $d = a\alpha + b\beta$. In particolare a e b sono coprimi se e soltanto se esistono $\alpha, \beta \in A$ tali che $1_A = a\alpha + b\beta$ (il che equivale a dire $(a) + (b) = A$).

Se inoltre A è un dominio euclideo, allora il calcolo di un MCD di due elementi non nulli può essere effettuato mediante l'algoritmo di Euclide, in modo del tutto analogo a come si opera per calcolare il MCD di due numeri interi (vedremo un'importante istanza di ciò con gli anelli di polinomi nel prossimo capitolo).

Esercizio 8.12. Sia R un PID, e $\{0\} \neq I$ un ideale di R. Si provi che I è ideale primo se e solo se è un ideale massimale.

Esercizio 8.13. Ogni campo è un dominio euclideo. Rispetto a quale valutazione?

Esercizio 8.14. Si provi che $\mathbb{Z}[\sqrt{2}]$ è un dominio euclideo.

Esercizio 8.15. Si descrivano gli elementi irriducibili di $\mathbb{Z}[\sqrt{3}]$.

Esercizio 8.16. Sia R un dominio a ideali principali, e sia $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ \ldots$ una catena infinita discendente di ideali di R. Si provi che $\bigcap_{n\in\mathbb{N}} I_n = (0)$.

8.4 Interi di Gauss.

L'anello degli interi di Gauss è un esempio molto interessante di dominio euclideo, che ha diverse applicazioni, cui però noi accenneremo soltanto. Questa sezione, che non è essenziale per la comprensione del resto del corso, può essere considerata una lettura o un'esercitazione svolta. L'abbiamo inserita perché l'argomento è interessante, e perché ci consente di tirare a cinque anche le sezioni di questo capitolo.

L'anello degli interi di Gauss è l'insieme

$$\mathbb{Z}[i] = \{\ u + iv \mid u, v \in \mathbb{Z}\ \}.$$

$\mathbb{Z}[i]$ è un sottoanello dell'anello $\mathbb{C}$ (vedi esercizio 6.26), ed è quindi un dominio d'integrità. Proviamo che è un dominio euclideo, usando come valutazione la restrizione ad esso del quadrato del modulo sui complessi, ovvero la *norma* definita da, per ogni $z = u + vi \in \mathbb{Z}[i]$

$$\delta(z) = z\overline{z} = (u + iv)(u - iv) = u^2 + v^2\ .$$

Si verifica facilmente che $\delta(zz_1) = \delta(z)\delta(z_1)$ per ogni $z, z_1 \in \mathbb{Z}[i]$.

Teorema 8.13. *L'anello $\mathbb{Z}[i]$ degli interi di Gauss è un dominio euclideo; quindi è un PID.*

Dimostrazione. Siano $a, b \in \mathbb{Z}[i]$, con $b \neq 0$. Ora $ab^{-1} \in \mathbb{Q}[i]$ dunque $ab^{-1} = \alpha + \beta i$ con $\alpha, \beta \in \mathbb{Q}$. Quindi esistono numeri interi u, v con

$$|\alpha - u| \leq \frac{1}{2}\ , \qquad |\beta - v| \leq \frac{1}{2}\ .$$

Posto $\epsilon = \alpha - u,\ \eta = \beta - v$ si ha

$$a = b((u+\epsilon) + (v+\eta)i = b(u+vi) + b(\epsilon + \eta i) = bq + r$$

con $q = u + vi \in \mathbb{Z}[x]$ e $r = b(\epsilon + \eta i) = a - bq \in \mathbb{Z}[i]$. Inoltre, se $r \neq 0$

$$\delta(r) = \delta(b)(\epsilon^2 + \eta^2) \leq \frac{1}{2}\delta(b)$$

provando quindi che $\mathbb{Z}[i]$ è un dominio euclideo. ∎

L'anello degli interi di Gauss è utile in diverse applicazioni alla teoria dei numeri. Vediamo un esempio.

Proposizione 8.14. *a) Sia p un numero primo tale che $p \equiv 1 \pmod 4$; allora esiste un intero z tale che $z^2 \equiv -1 \pmod p$.*

b) Un numero primo positivo p si può scrivere come somma $p = a^2 + b^2$ dei quadrati di due interi a, b se e solo se $p = 2$ o $p \equiv 1 \pmod 4$.

Dimostrazione. a) Sia p un primo tale che $4|(p-1)$, e sia $s \in \mathbb{N}$ tale che $p - 1 = 4s$. L'affermazione a) equivale a provare che il polinomio $x^2 + \overline{1}$ ammette radici nel campo $\mathbb{Z}/p\mathbb{Z}$. Sia $\overline{a}$ un elemento non nullo di $\mathbb{Z}/p\mathbb{Z}$; allora, per il teorema di Fermat, $\overline{a}^{4s} = \overline{1}$, e quindi $\overline{a}^{2s}$ è radice di $x^2 - \overline{1}$. Siccome $\mathbb{Z}/p\mathbb{Z}$ è un campo (e $p \neq 2$), le radici di quest'ultimo polinomio sono solo due, e sono $\pm\overline{1}$. Ancora, le radici di $x^{2s} - \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}$ sono al più $2s$. Siccome $2s < p - 1$, ciò implica che esiste $\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$, tale che $\overline{a}^{2s} \neq \overline{1}$. Per quanto osservato sopra, deve essere pertanto $\overline{a}^{2s} = -\overline{1}$, e quindi $\overline{a}^s$ è radice del polinomio $x^2 + \overline{1}$, ovvero $(a^s)^2 \equiv -1 \ (mod\ p)$.

b) Supponiamo $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$ e p dispari. Allora a e b non possono essere entrambi pari o entrambi dispari e quindi possiamo supporre $a = 2h$, $b = 2k + 1$, con $h, k \in \mathbb{Z}$. Segue $a^2 \equiv 0 \ (mod\ 4)$ e $b^2 = 4k^2 + 4k + 1 \equiv 1 \ (mod\ 4)$ e dunque $p \equiv 1 \ (mod\ 4)$.
Proviamo ora l'implicazione inversa. Possiamo supporre, dato che evidentemente $2 = 1+1$, che sia $p \equiv 1 \ (mod\ 4)$. Per il punto a) esiste dunque un intero z tale che $p|(z^2+1)$. Dunque, in $\mathbb{Z}[i]$, $p|z^2 + 1 = (z+i)(z-i)$ e quindi p non può essere un elemento primo in $\mathbb{Z}[i]$, poiche' un intero di Gauss e' divisibile per $n \in \mathbb{Z}$ se e solo se ha parte reale ed immaginaria divisibili per n. Dunque p non è irriducibile in $\mathbb{Z}[i]$ ed esistono $\alpha, \beta \in \mathbb{Z}[i]$, α, β non invertibili, tali che $p = \alpha\beta$. Segue $p^2 = \delta(p) = \delta(\alpha)\delta(\beta)$ e, osservando che $\delta(\alpha)$ e $\delta(\beta)$ sono interi > 1 (poiche' α e β non sono invertibili), abbiamo $\delta(\alpha) = \delta(\beta) = p$. Pertanto, se $\alpha = a + ib$ con $a, b \in \mathbb{Z}$, concludiamo $\delta(\alpha) = a^2 + b^2 = p$. ∎

Con argomenti simili possiamo provare il seguente risultato.

Lemma 8.15. *Sia $\pi \in \mathbb{Z}[i]$. Allora, π è un primo di $\mathbb{Z}[i]$ se e solo se una delle seguenti condizioni è soddisfatta.*

i) *$\pi \sim p$ con p intero primo, $p \equiv 3 \pmod 4$;*

ii) *$\delta(\pi) = p$ con p intero primo, $p = 2$ o $p \equiv 1 \pmod 4$*

Dimostrazione. Sia $\pi = a + ib$ un primo di $\mathbb{Z}[i]$. Osserviamo che $\delta(\pi) = \pi\overline{\pi}$ è un intero > 1 e quindi esistono $p_1, p_2, \ldots, p_h \in \mathbb{Z}$, p_i primi in $\mathbb{Z}$, tali che $\pi\overline{\pi} = p_1 p_2 \ldots p_h$. Ma π è primo in $\mathbb{Z}[i]$ e quindi $\pi | p$ per un $p = p_i$, ovvero $p = \pi\alpha$ con $\alpha \in \mathbb{Z}[i]$. Segue $\delta(\pi)|\delta(p) = p^2$. Dato che $1 \neq \delta(\pi) \in \mathbb{N}$, abbiamo due possibillita': i) $\delta(\pi) = a^2 + b^2 = p$; oppure ii) $\delta(\pi) = p^2$. Nel caso ii), da $p = \pi\alpha$, segue $p^2 = \delta(p) = \delta(\pi)\delta(\alpha) = p^2\delta(\alpha)$ e quindi $\delta(\alpha) = 1$ e α e' un'unità, ovvero $\pi \sim p$. In particolare, p è primo e quindi irriducibile in $\mathbb{Z}[i]$ e quindi $p \neq 2 = (1+i)(1-i)$ e $p \not\equiv 1 \ (mod\ 4)$, dato che altrimenti per l'esercizio precedente avremmo $p = x^2 + y^2 = (x+iy)(x-iy)$ per $x+iy, x-iy \in \mathbb{Z}[i]$ non invertibili. Pertanto se π è un primo di $\mathbb{Z}[i]$ allora

i) $\pi \sim p$ con p intero primo, $p \equiv 3 \ (mod\ 4)$ oppure

ii) $\delta(\pi) = p$ con p intero primo, $p = 2$ o $p \equiv 1 \ (mod\ 4)$.

Sia, viceversa, $\pi \in \mathbb{Z}[i]$ tale che valgano I) o II). Se $\delta(\pi)$ è un primo allora si verifica subito, per la moltiplicatività della valutazione, che π è irriducibile. Sia quindi $\pi \sim p$ con p intero primo, $p \equiv 3 \ (mod\ 4)$ e supponiamo π riducibile. Allora anche p è riducibile e $p = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[i]$ non invertibili. Segue $p^2 = \delta(p) = \delta(\alpha)\delta(\beta)$ e, poichè $1 < \delta(\alpha), \delta(\beta) \in \mathbb{N}$, concludiamo $\delta(\alpha) = p$. Quindi $p = x^2 + y^2$ per opportuni $x, y \in \mathbb{Z}$ e, ancora per il precedente esercizio, abbiamo la contraddizione $p = 2$ oppure $p \equiv 1 \ (mod\ 4)$. Pertanto, $\pi \in \mathbb{Z}[i]$ è primo se e solo se valgono I) o II). Osserviamo infine che se vale I) π è un numero reale od un immaginario puro, mentre se vale II) allora $Re(\pi) \neq 0 \neq Im(\pi)$. ∎

Esercizio 8.17. Si fattorizzi $12 + 22i$ come prodotto di elementi irriducibili di $\mathbb{Z}[i]$.

Esercizio 8.18. Trovare un MCD di $5 + 10i$ e $80 + 70i$ in $\mathbb{Z}[i]$

Esercizio 8.19. Per ogni numero $k \in \mathbb{N} \setminus \{0\}$, sia

$$\mathcal{I}_k = \{z \in \mathbb{Z}[i] \mid k \text{ divide } N(z)\}$$

(dove, se $z = a + ib$, $N(z) = a^2 + b^2$).

a) Si provi che, per ogni $k \in \mathbb{N} \setminus \{0\}$, $\mathcal{I}_k$ è un ideale di di $\mathbb{Z}[i]$.

b) Si determini per quali $k \in \mathbb{N} \setminus \{0\}$, $\mathcal{I}_k$ è un ideale massimale di $\mathbb{Z}[i]$.

8.5 Esercizi.

Esercizio 8.20. Sia A un dominio d'integrità in cui per ogni $a, b \in A \setminus \{0_A\}$, a è associato a b. Si provi che A è un campo.

Esercizio 8.21. Sia A un dominio d'integrità in cui ogni elemento non nullo è irriducibile o invertibile. Si provi che A è un campo.

Esercizio 8.22. Si provi che nell'anello $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ non esiste massimo comun divisore di 4 e $2 + 2\sqrt{-3}$.

Esercizio 8.23. Si consideri l'anello $\mathbb{Z} \times Z$ (le operazioni sulle componenti). Sia $P = \{(a, 0) \mid a \in \mathbb{Z}\}$; si dimostri che P è un ideale primo di $\mathbb{Z}$x$\mathbb{Z}$.

Esercizio 8.24. Siano A e B ideali dell'anello R, e sia

$$I = \{\ r \in R \mid ar \in B \ \text{ per ogni } a \in A\ \}\ .$$

Si provi che se B è un ideale massimale e $A \not\subseteq B$, allora $I = B$.

Esercizio 8.25. Determinare gli ideali massimali dell'anello $\mathbb{R} \times \mathbb{R}$.

Esercizio 8.26. Si provi che se I è un ideale massimale dell'anello $\mathbb{R}^{\mathbb{R}}$, allora esiste $r \in \mathbb{R}$ tale che $I = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(r) = 0\}$. Si concluda che tutti gli ideali massimali di $\mathbb{R}^{\mathbb{R}}$ sono principali.

Esercizio 8.27. Si determini l'intersezione degli ideali massimali dell'anello $\mathbb{Z}_{24}$.

Esercizio 8.28. Sia $n \geq 2$. Si provi che l'intersezione degli ideali massimali di $\mathbb{Z}_n$ è $\{0\}$ se e soltanto se n è un prodotto di primi distinti. In tal caso, quali sono gli elementi nilpotenti di $\mathbb{Z}_n$?

Esercizio 8.29. Siano I e K ideali dell'anello commutativo A, e sia $a \in A$ un elemento fissato. Definiamo

$$I_{(K,a)} = \{\ x \in I \mid xa \in K\ \}\ .$$

(a) Si provi che $I_{(K,\,a)}$ è un ideale di A.

(b) Nell'anello $\mathbb{Z}$ si determini (cioè se ne trovi un generatore), l'ideale $3\mathbb{Z}_{(4\mathbb{Z},\,2)}$.

(c) Sia A un dominio a ideali principali, sia I un ideale di A, e sia $K = (c)$ un ideale massimale. Si provi che $I_{(K,\,a)} = I$ se e solo se $I \subseteq K$ o $a \in K$.

Esercizio 8.30. Sia $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$. Si provi che $\mathbb{Z}[\sqrt{10}]$ è un anello, e si provi che l'ideale $(2, \sqrt{10})$ di $\mathbb{Z}[\sqrt{10}]$ è un ideale primo.

Esercizio 8.31. Sia R un dominio d'integrità a fattorizzazione unica, e sia $0_R \neq a \in R$ un elemento non invertibile di R.

a) Si provi che il numero di ideali principali di R contenenti l'ideale (a) è finito.

b) Si provi che

$$\bigcap_{n \in \mathbb{N}} (a^n) = \{0_r\}.$$

Esercizio 8.32. Si provi che non esiste alcun omomorfismo d'anelli da $\mathbb{Z}[\sqrt{-5}]$ in $\mathbb{Z}$.

Esercizio 8.33. Si provi che l'insieme di matrici

$$A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

è un sottoanello commutativo dell'anello $M_2(\mathbb{R})$ delle matrici quadrate di ordine due sui reali. Si provi che

$$H = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

è un ideale massimale di A.

Esercizio 8.34. Sia R un anello commutativo e siano K, Y ideali primi di R. Si dimostri che $K \cap Y$ é un ideale primo di R se e solo se $K \supseteq Y$ oppure $Y \supseteq K$.

Esercizio 8.35. Sia R un anello commutativo in cui ogni ideale principale diverso da R è un ideale primo. Si provi che R un campo.

Esercizio 8.36. Provare che nell'anello $\mathbb{Z}[\sqrt{-7}]$ l'elemento 2 è irriducibile ma non primo.

Esercizio 8.37. Sia $R = \mathbb{Z}[\sqrt{-6}]$. Si provi che 1 è un massimo comun divisore di $a = 5$ e $b = 2 + \sqrt{-6}$, ma non appartiene all'ideale $(a) + (b)$.

Esercizio 8.38. Siano $\alpha = 12 + 21i$, $\beta = 25 + 10i$, $\gamma = 3 - i$, $\delta = 3 + 24i$ e $I = (\alpha, \beta)$, $J = (\gamma, \delta)$ gli ideali di $\mathbb{Z}[i]$ generati rispettivamente da α e β, e da γ e δ. Si provi che $I = J$.

Esercizio 8.39. Si provi che i seguenti sottoinsiemi di $\mathbb{Z}[\sqrt{-5}]$ sono ideali

$$A = \{\ z \in \mathbb{Z}[\sqrt{-5}] \mid 2 \text{ divide } N(z)\ \}, \qquad B = \{\ z \in \mathbb{Z}[\sqrt{-5}] \mid 5 \text{ divide } N(z)\ \}$$

e si dica quali fra essi è principale.

Esercizio 8.40. Siano $\mathbb{C}$ il campo dei numeri complessi, e $\mathbb{Z}$ l'anello degli interi. Sia quindi $A = \mathbb{C} \times \mathbb{Z}$ l'anello prodotto diretto. Definiamo,

$$C = \{(x, 0) \in A \mid x \in \mathbb{C}\} \qquad Z = \{(0, y) \in A \mid y \in \mathbb{Z}\}\ .$$

(a) Si provi che C e Z sono ideali di A.

(b) Si dica se Z è un ideale massimale di A.

(c) Sia I un ideale di A. Si provi che $C \subseteq I$ oppure $I \subseteq Z$.

Esercizio 8.41. Sia R un anello commutativo di caratteristica 2, e sia dato un ideale I di R. Si ponga $K(I) = \{x \in R \mid x^2 \in I\}$. Si dimostri che:

(i) $K(I)$ è ideale di R.

(ii) Se I è un ideale primo allora $K(I) = I$.

Esercizio 8.42. (a) Sia $\mathbb{P}$ l'insieme dei numeri primi positivi. Si provi che

$$\bigcap_{p \in \mathbb{P}} p\mathbb{Z} = \{0\}\ .$$

(b) Sia A un P.I.D. e sia $\mathcal{M}$ la famiglia di tutti gli ideali massimali di A. Si provi che, se $\mathcal{M}$ è infinita,

$$\bigcap_{I \in \mathcal{M}} I = \{0_A\}\ .$$

Esercizio 8.43. Sia S un sottoinsieme moltiplicativamente chiuso di un anello commutativo A, e tale che $0 \notin S$, Sia I un ideale di A tale che I è massimale tra gli ideali di A che hanno intersezione vuota con S (ovvero: $I \cap S = \emptyset$ e se J è ideale di A con $I \subseteq J$ e $I \neq J$, allora $J \cap S \neq \emptyset$). Si provi che I è un ideale primo di A.

Esercizio 8.44. Sia p un numero primo, e sia

$$\mathbb{Q}_p = \Big\{ \frac{a}{b} \in \mathbb{Q} \mid p \text{ non divide } b \Big\}.$$

Si provi che $\mathbb{Q}_p$ è un anello locale, ovvero che esiste un ideale (massimale) J di $\mathbb{Q}_p$ che contiene ogni ideale proprio di $\mathbb{Q}_p$.

Esercizio 8.45. Sia A un anello commutativo, e sia I un suo ideale. Si pone

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ per qualche } n \in \mathbb{N}\}.$$

(a) Si provi che $\sqrt{I}$ è un ideale di A, e che $\sqrt{\sqrt{I}} = \sqrt{I}$.
(b) Si provi che se I è un ideale primo, allora $\sqrt{I} = I$.

Esercizio 8.46. (Ideali primari, I) Un ideale P di un anello commutativo A si dice *primario* se $P \neq A$ e per ogni $a, b \in A$

$$\begin{cases} ab \in P \\ a \notin P \end{cases} \quad \Rightarrow \quad b^n \in P \ \text{ per qualche } n \geq 1.$$

Si descrivano tutti gli ideali primari dell'anello $\mathbb{Z}$.

Esercizio 8.47. (Ideali primari, II) (1) Sia A un PID e I un ideale di A; si provi che I è un ideale primario se e solo se esiste un elemento irriducibile $a \in A$ ed un intero $n \geq 1$, tali che $I = (a^n)$.
(2) Si provi che in un PID ogni ideale non nullo è l'intersezione di un numero finito di ideali primari.

Esercizio 8.48. (Anelli noetheriani, I) Un anello commutativo A si dice *noetheriano* (da Emmy Noether, 1882–1935) se ogni catena di ideali $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ con $I_i \neq I_j$, è finita. Si provi che ogni PID è un anello noetheriano.

Esercizio 8.49. (Anelli noetheriani, II) Sia A un anello commutativo. Si provi che le seguenti condizioni sono equivalenti.
(1) A è noetheriano;
(2) ogni insieme di ideali di A ammette elementi massimali (rispetto alla relazione d'inclusione):
(3) ogni ideale di A è finitamente generato.

Esercizio 8.50. (Anelli noetheriani, III) Siano A e B anelli noetheriani. Si provi che il prodooto diretto $A \times B$ è un anello noetheriano.

Capitolo 9

Polinomi

9.1 Definizioni.

Sia R un anello commutativo. Un **polinomio** a coefficienti in R nell'*indeterminata* x è una espressione del tipo

$$a_0 + a_1x + a_2x^2 + \ \ldots \ + a_nx^n$$

dove n è un numero naturale, $a_0, a_1, a_2, \ldots, a_n$ sono elementi di R (appunto, i *coefficienti* del,polinomio), ed x è un simbolo (detto indeterminata) indipendente dagli elementi di R.
L'insieme di tutti i polinomi a coefficienti in R nell'indeterminata x si denota con $R[x]$.(Questa definizione non è del tutto formale; daremo una costruzione rigorosa di $R[x]$ alla fine della sezione, nella quale anche la misteriosa indeterminata x avrà un significato formalmente preciso).

Due polinomi $a_0 + a_1x + \ \ldots \ + a_nx^n$ e $c_0 + c_1x + \ \ldots \ + c_mx^m$ a coefficienti in R sono **uguali** se $a_i = b_i$ per ogni $i \geq 0$; con la convenzione che i coefficienti non scritti sono uguali a zero (cioè $a_i = 0$ per ogni $i > n$ e $c_i = 0$ per ogni $c_i > m$; in particolare confrontando due polinomi possiamo sempre supporre $n = m$).
Un'altra convenzione familiare è che scrivendo semplicemente x^n si intende 1_Rx^n. Ogni elemento di R è un polinomio, quindi $R \subseteq R[x]$. Abitualmente, indicheremo i polinomi con lettere $f, g, h, \ldots$

Sull'insieme dei polinomi $R[x]$ si definiscono somma e prodotto nel modo seguente (che è la generalizzazione di quello familiare nel caso di polinomi a coefficienti reali). Quindi, se

$$f = a_0 + a_1x + a_2x^2 + \ \ldots \ + a_nx^n \ \text{ e } \ g = c_0 + c_1x + c_2x^2 + \ \ldots \ + c_mx^m$$

sono polinomi a coefficienti in R, con $n \geq m$, si pone

$$f + g = (a_0 + c_0) + (a_1 + c_1)x + (a_2 + c_2)x^2 + \ \ldots \ + (a_n + c_n)x^n$$

(dove abbiamo eventualmente aggiunto coefficienti $c_i = 0$ per $i > m$), e

$$fg = d_0 + d_1x + d_2x^2 + \ \ldots \ + d_{n+m}x^{n+m}$$

dove, per ogni $0 \leq i \leq n + m$

$$d_i = \sum_{r=0}^{i} a_r c_{i-r} \ .$$

Potete constatare da soli che queste sono le operazioni sui polinomi che vi sono già familiari dalle scuole superiori. Inoltre si verifica che con tali operazioni l'insieme $R[x]$ è un anello in cui zero e identità sono, rispettivamente, 0_R e 1_R. $R[x]$ si chiama **l'anello dei polinomi** nell'indeterminata x a coefficienti in R, e chiaramente contiene R come sottoanello (in particolare, *la caratteristica di $R[x]$ coincide con la caratteristica di R*).

Se f è un polinomio (a coefficienti in un anello commutativo) e $f \neq 0$, conveniamo di scrivere

$$f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

con $a_n \neq 0$. Il numero naturale n è detto allora **grado** del polinomio f e si denota con $\deg f$; osserviamo in particolare che $\deg f = 0$ se e solo se $f \in R \setminus \{0\}$.. Il termine a_n è detto **coefficiente direttivo** di $f \neq 0$ (mentre a_0 e detto "termine noto"); conveniamo che il coefficiente direttivo del polinomio nullo è 0). Ancora, $0 \neq f \in R[x]$. si dice **monico** se il suo coefficiente direttivo è 1_R.
Le seguenti proprietà sono di immediata verifica, che lasciamo per esercizio.

Proposizione 9.1. *Siano $f, g \in R[x] \setminus \{0_R\}$. Allora*

(1) $\deg(f + g) \leq \max\{\deg f, \deg g\}$

(2) $\deg(fg) \leq \deg f + \deg g$, *con uguaglianza se R è un dominio d'integrità.*

Osserviamo che l'uguaglianza al punto (2) può non sussistere se R non è un dominio d'integrità; ad esempio, in $(\mathbb{Z}/6\mathbb{Z})[x]$: $(\overline{2}x + \overline{1})(\overline{3}x + \overline{1}) = \overline{6}x^2 + \overline{5}x + \overline{1} = \overline{5}x + \overline{1}$.

Esercizio 9.1. Siano $f, g \in R[x] \setminus \{0_R\}$. Si provi che se il coefficiente direttivo di almeno uno tra f e g è invertibile in R, allora $\deg(fg) = \deg f + \deg g$.

Dalla proposizione 9.1 seguono facilmente le prime importanti constatazioni a proposito delle proprietà generali degli anelli di polinomi.

Proposizione 9.2. *Sia R un dominio d'integrità. Allora*

(1) *$R[x]$ è un dominio d'integrità.*

(2) *Gli elementi invertibili di $R[x]$ sono tutti e soli gli elementi invertibili di R; in particolare, se F è un campo l'insieme degli elementi invertibili di $F[x]$ è $F \setminus \{0\}$.*

Dimostrazione. (1) Sia R un dominio d'integrità, e siano $f, g \in R[x]$ polinomi non nulli. Allora $\deg f \geq 0$ e $\deg g \geq 0$; quindi per il punto (2) della Proposizione precedente, $\deg(fg) = \deg f + \deg g \geq 0$, e dunque $fg \neq 0$. Quindi $R[x]$ è un dominio d'integrità.

(2) Sia R un dominio d'integrità, e sia f un elemento invertibile di $R[x]$. Allora esiste $g \in R[x]$ tale che $1 = fg$. Quindi, sempre per il punto (2) della Proposizione precedente

$$\deg f + \deg g = \deg(fg) = \deg(1) = 0$$

che forza $\deg f = \deg g = 0$, cioè $f, g \in R$ e di conseguenza f, g sono elementi invertibili di R. ∎

Sia R un sottoanello dell'anello S e sia $b \in S$. Sia $f = a_0 + a_1 x + a_2 x^2 + \ \ldots \ + a_n x^n$ un polinomio in $R[x]$. Poichè i coefficienti a_i sono in particolare elementi di S, ha senso considerare la sostituzione di x con b in f:

$$f(b) = a_0 + a_1 b + a_2 b^2 + \ \ldots \ + a_n b^n$$

che è un elemento di S.
Ora, si verifica facilmente che, fissato $b \in S$, l'applicazione

$$\begin{array}{rccc} \sigma_b : & R[x] & \longrightarrow & S \\ & f & \mapsto & f(b) \end{array}$$

è un omomorfismo di anelli, che si chiama *omomorfismo di sostituzione* per b.
L'immagine di σ_b si denota con $R[b]$; quindi

$$R[b] = \{\ f(b) \mid f \in R[x]\ \} = \{a_0 + a_1 b + \ldots + a_n b^n \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in R\}.$$

Il nucleo di σ_b è

$$I_b = \ker(\sigma_b) = \{\ f \in R[x] \mid f(b) = 0\ \}\ .$$

Osservazione. Sia R un sottoanello dell'anello commutativo S, e sia b in S. Allora, $R[b]$ è il più piccolo sottoanello di S che contiene $R \cup \{b\}$ (ovvero ogni sottoanello di S che contiene R e b, contiene $R[b]$). Infatti $R[b]$ è un sottoanello di S poiché è immagine di un omomorfismo. Inoltre, è chiaro che ogni sottoanello di S che contiene b contiene anche tutte le potenze b^n con $n \in \mathbb{N}$. Dunque ogni sottoanello T di S che contiene $R \cup \{b\}$ contiene ogni elemento ab^n con $a \in R,\ n \in \mathbb{N}$, e quindi contiene anche ogni elemento del tipo

$$a_0 + a_1 b + a_2 b^2 + \ \ldots \ + a_n b^n$$

con $a_0, a_1, \ldots, a_n \in R$ e $n \in \mathbb{N}$. Dunque T contiene $R[b]$.

Gli omomorfismi di sostituzione sono un'applicazione particolare di quella che è chiamata la proprietà fondamentale degli anelli di polinomi, e che è descritta dal risultato che segue.

Teorema 9.3. (Principio di sostituzione). *Sia $\phi : R \to S$ un omomorfismo di anelli, sia $b \in S$, e sia $R[x]$ l'anello dei polinomi a coefficienti in R. Allora esiste uno ed un solo omomorfismo $\phi_b : R[x] \to S$ tale che*

$$\begin{cases} \phi_b(a) = \phi(a) \ \ \textit{per ogni} \ \ a \in R \\ \phi_b(x) = b. \end{cases}$$

Dimostrazione. Sia $\phi_b : R[x] \to S$ un omomorfismo che soddisfi le proprietà richieste nell'enunciato. Allora se $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$, deve essere

$$\phi_b(f) = \phi_b(a_0) + \phi_b(a_1)\phi_b(x) + \ldots + \phi_b(a_n)\phi_b(x^n) = \phi(a_0) + \phi(a_1)b + \ldots + \phi(a_n)b^n.$$

Quindi, se esiste, ϕ_b è univocamente determinato. Vediamo ora che, effettivamente, ponendo per ogni $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$

$$\phi_b(f) = \phi(a_0) + \phi(a_1)b + \ldots + \phi(a_n)b^n$$

si ottiene un omomorfismo. E' chiaro che $\phi_b(1) = \phi(1) = 1_S$. Sia ora $g = c_0 + \ldots + c_mx^m \in R[x]$. La verifica che $\phi_b(f + g) = \phi_b(f) + \phi_b(g)$ è facile. Consideriamo quindi il prodotto: $fg = \sum_{i=0}^{n+m} d_ix^i$, dove, per ogni $i = 1, 2, \ldots, n + m \ : \ d_i = \sum_{r=0}^{i} a_rc_{i-r}$; allora,

$$\phi_b(fg) = \phi_b\left(\sum_{i=0}^{n+m} d_ix^i\right) = \sum_{i=0}^{n+m} \phi(d_i)b^i$$

ora, per ogni $i = 1, 2, \ldots, n + m$:

$$\phi(d_i) = \phi\left(\sum_{r=0}^{i} a_rc_{i-r}\right) = \sum_{r=0}^{i} \phi(a_r)\phi(c_{i-r})$$

è proprio il coefficiente i-esimo (rispetto alle potenze di b) del prodotto in S

$$(\phi(a_0) + \phi(a_1)b + \ldots + \phi(a_n)b^n)(\phi(c_0) + \phi(c_1)b + \ldots + \phi(c_m)b^m)$$

dunque

$$\phi_b(fg) = \sum_{i=0}^{n+m} \phi(d_i)b^i = \phi_b(f)\phi_b(g) \ .$$

Quindi ϕ_b è un omomorfismo e la dimostrazione è completata. ∎

La situazione da cui siamo partiti (quella di un elemento b contenuto in un anello S che contiene R come sottoanello) è quindi un caso particolare di applicazione del principio di sostituzione. L'omomorfismo (di sotituzione) σ_b definito in quel caso è l'unica estensione a $R[x]$ dell'omomorfismo identico da R in S che manda x in b,

Vediamo un'altra applicazione. Sia $n \geq 2$, e consideriamo l'omomorfismo

$$\begin{array}{rccc} \phi : & \mathbb{Z} & \to & (\mathbb{Z}/n\mathbb{Z})[x] \\ & a & \mapsto & \overline{a} \end{array}$$

dove, come consuetudine, $\overline{a} = a + n\mathbb{Z}$. Scegliendo $b = x \in (\mathbb{Z}/n\mathbb{Z})[x]$, per il principio di sostituzione possiamo concludere che esiste un unico omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}[x]$ che manda ogni $a \in \mathbb{Z}$ in $\overline{a}$ e x in x. Chiaramente tale omomorfismo è definito da, per ogni $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$,

$$f \mapsto \overline{f} = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n \ .$$

Il polinomio $\overline{f} \in (\mathbb{Z}/n\mathbb{Z})[x]$ definito in questa maniera si chiama la *riduzione modulo n* del polinomio intero f e, come vedremo più avanti, risulta utile in molte circostanze. Ad esempio, la riduzione modulo 3 del polinomio $5 + 12x - 5x^2 + 7x^3 + 6x^4$ è

$$\overline{5} + \overline{12}x + \overline{-5}x^2 + \overline{7}x^3 + \overline{6}x^4 = \overline{2} + x^2 + x^3 \in \mathbb{Z}/3\mathbb{Z}[x] \ .$$

Costruzione formale dell'anello dei polinomi. Sia R un anello commutativo e consideriamo l'insieme di tutte le sequenze infinite

$$(a_0,\ a_1,\ a_2,\ a_3,\ \ldots\ldots) \qquad\qquad (*)$$

ad elementi $a_0, a_1, a_2, \ldots$ in R. Osserviamo che tale insieme può essere identificato con l'insieme $R^{\mathbb{N}}$ di tutte le applicazioni da $\mathbb{N}$ in R, facendo corrispondere alla sequenza $(a_0, a_1, a_2, a_3,\ \ldots)$ l'applicazione che ad ogni $n \in \mathbb{N}$ associa l'elemento a_n della sequenza.

Denotiamo con B il sottoinsieme costituito da tutte le sequenze quasi ovunque nulle, cioè le sequenze che hanno un numero finito di termini a_i diversi da zero (che corrispondono alle applicazioni f da $\mathbb{N}$ in R per le quali esiste un k tale che $f(i) = 0$ per ogni $i \geq k$). Su B definiamo una somma ponendo

$$(a_0, a_1, a_2, a_3, \ldots) + (b_0, b_1, b_2, b_3,\ \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3,\ \ldots) \ .$$

Si verifica facilmente che rispetto a tale operazione B soddisfa gli assiomi (S1), (S2) e (S3) per gli anelli, con elemento neutro $0_B = (0, 0, 0, \ldots)$.
Introduciamo quindi una moltiplicazione ponendo

$$(a_0, a_1, a_2, a_3, \ldots)(b_0, b_1, b_2, b_3,\ \ldots) = (c_0, c_1, c_2, c_3,\ \ldots)$$

dove, per ogni $i \in \mathbb{N}$: $c_i = \sum_{r=0}^{i} a_r b_{i-r}$. (osserviamo che se $a_r = 0$ per $r \geq n$ e $b_s = 0$ per $s \geq m$ allora $c_i = 0$ per $i \geq n + m$ e quindi $(c_0, c_1, c_2, c_3,\ \ldots) \in B$). Con un po' di lavoro, ma senza difficoltà, anche in questo caso si dimostra che rispetto a tale prodotto B soddisfa gli assiomi (P1) e (P2) di anello, con identità $1_B = (1, 0, 0, 0, \ldots)$, e che è soddisfatta la proprietà distributiva del prodotto rispetto alla somma.
Quindi, con tali operazioni, B è un anello commutativo.
Consideriamo ora la applicazione $R \to B$ che ad ogni $a \in R$ associa $(a, 0, 0, \ldots)$. Essa è un omomorfismo iniettivo di anelli; possiamo quindi identificare $(a, 0, 0, \ldots)$ con l'elemento $a \in R$ e considerare R come sottoanello di B.
Poniamo ora $x = (0, 1, 0, 0, \ldots)$. Allora, applicando la definizione di prodotto in B, e ragionando per induzione, si prova che per ogni $n \in \mathbb{N}$

$$x^n = (0, 0, \ldots, 0, 1, 0, \ldots)$$

con 1 al posto n. Da ciò segue che per ogni $a \in \mathbb{R}$

$$ax^n = (a, 0, 0, \ldots)(0, 0, \ldots, 0, 1, 0 \ldots) = (0, 0, \ldots, 0, a, 0 \ldots)$$

con a al posto n. Quindi, ogni $f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \in B$ si scrive

$$f = (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + (0, 0, a_2, \ldots) + (0, 0, \ldots, 0, a_n, 0, \ldots) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n \ .$$

Quindi, ragionando nell'estensione $R \subseteq B$, si ha $B = R[x]$. Questo si dice l'anello dei polinomi a coefficienti in R nell'indeterminata x.

La costruzione dell'anello dei polinomi si estende in modo naturale a più indeterminate. Si tratta di 'aggiungere' successivamente le indeterminate: così, se R è una anello commutativo, e x, y sono due distinte indeterminate si pone $R[x,y] = (R[x])[y]$. Il caso generale è definito induttivamente: se $n \geq 2$ e $x_1, \ldots, x_n$ sono distinte indeterminate, si pone

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

Si ha chiaramente una catena di inclusioni tra sottoanelli;

$$R \subseteq R[x_1] \subseteq R[x_1, x_2] \subseteq \ldots \subseteq R[x_1, \ldots, x_n].$$

La Proposizione 9.2 assicura che gli elementi invertibili di $R[x_1, \ldots, x_n]$ sono gli invertibili di R, e che se R è un dominio d'integrità allora anche $R[x_1, \ldots, x_n]$ è tale.
Limitiamoci, per semplicità di notazioni, al caso di due indeterminate, x e y. Usando le proprietà distributive (e la commutatività) si riconosce allora, con un po' di lavoro, che ogni elemento $f \in R[x,y]$ si scrive in modo unico nella forma

$$f = \sum_{i,j \in \mathbb{N}} a_{ij} x^i y^j \tag{9.1}$$

con a_{ij} elementi di R che sono nulli tranne che per un numero finito di coppie (i,j). Per cui si può pensare all'anello $R[x,y]$ come a quello ottenuto considerando tutte le espressioni del tipo (9.1), ovvero 'aggiungendo' ad R assieme le due indeterminate x e y, che sono assunte commutare tra loro. Che l'ordine con cui si considerano le indeterminate sia ininfluente (cosa piuttosto naturale) si può provare in modo più concettuale utilizzando il Principio di sostituzione. Infatti, l'isomorfismo naturale tra $R[x]$ e $R[y]$ (che è l'identità su R e manda $x \mapsto y$) per il principio di sostituzione si estende ad un unico omomorfismo

$$\Sigma : R[x,y] = R[x][y] \longrightarrow R[y,x]$$

che manda y in x. Ìpoiché Σ è in modo piuttosto ovvio invertibile, se ne conclude che è un isomorfismo, ovvero che $R[x,y] \simeq R[y,x]$.

Esercizio 9.2. Sia A una anello commutativo. Sia R un sottoanello di A; si provi che $R[x]$ è un sottoanello di $A[x]$. Sia I un ideale di A; si provi che l'insieme dei polinomi di $A[x]$ i cui coefficienti appartengono a I è un ideale di $A[x]$.

Esercizio 9.3. Si provi che, per ogni $n \in \mathbb{N}$, il polinomio $\overline{2}x^n + 1$ è un elemento invertibile dell'anello $(\mathbb{Z}/4\mathbb{Z})[x]$. Si concluda che $(\mathbb{Z}/4\mathbb{Z})[x]$ contiene infiniti elementi invertibili (la ragione di questa anomalia va ricercata nel fatto che $(\mathbb{Z}/4\mathbb{Z})[x]$ non è un dominio d'integrità).

Esercizio 9.4. Sia σ l'omomorfismo di sostituzione: $\sigma : \mathbb{Z}[x] \to \mathbb{Q}$ definito da, per ogni $f \in \mathbb{Z}[x]$, $\sigma(f) = f(1/3)$, e sia $\mathbb{Z}[1/3] = Im(\sigma)$.

(a) Si provi che

$$\mathbb{Z}[1/3] = \{ \frac{m}{3^i} \mid m \in \mathbb{Z}\ , i \geq 0 \}.$$

(b) Si dica, motivando la risposta, se $\mathbb{Z}[1/3]$ è un campo.

Esercizio 9.5. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi. Si provi che il sottoinsieme $\{a_0 + a_1x + \ldots + a_nx^n \mid n \in \mathbb{N},\, a_o, a_1, \ldots, a_n \in \mathbb{Z}, \sum_{i=o}^{n} a_i = 0\}$ è un ideale di $\mathbb{Z}[x]$.

9.2 Divisione tra polinomi.

In questa sezione mostriamo, in particolare, il fatto fondamentale che se F è un campo, allora l'anello dei polinomi $F[x]$ è euclideo (pertanto è un dominio a ideali principali e a fattorizzazione unica).

Attenendoci alle definizioni introdotte nel capitolo precedente, se f, g sono polinomi a coefficienti nell'anello commutativo A, allora f *divide* g (e scriviamo $f|g$) se esiste $h \in A[x]$ tale che $g = fh$.

Esempio, Sia A un anello commutativo e siano $1 \leq m, n \in \mathbb{N}$ con $m|n$; allora il polinomio $x^m - 1 \in A[x]$ è un divisore di $x^n - 1$. Infatti, se $d \in \mathbb{N}$ è tale che $n = md$, come si verifica facendo i calcoli,

$$x^n - 1 = (x^m - 1)(x^{(d-1)m} + \ldots + x^{2m} + x^m + 1).$$

Essendo l'anello dei polinomi ben lontano dall'essere un campo, fissati casualmente due polinomi in $A[x]$ è assai improbabile che uno dei due divida l'altro. Tuttavia, se A è un campo è possibile definire una divisione con resto. Più in generale, è possibile dividere con resto (nel senso che preciseremo subito) se il coefficiente direttivo del polinomio divisore è un elemento invertibile di A

Teorema 9.4. *Sia A un anello commutativo, e sia $f = a_0 + a_1x + \ldots + a_nx^n \in A[x]$ con a_n un elemento* invertibile *di A. Allora per ogni $g \in A[x]$ esistono due polinomi $h, r \in A[x]$ tali che*

$$\begin{array}{ll} (i) & g = hf + r \\ (ii) & r = 0 \quad \textit{oppure} \quad \deg(r) \leq \deg(f) - 1 \end{array}$$

inoltre, h, r sono univocamente determinati da tali condizioni.

Dimostrazione. 1) (esistenza) Sia f cme nell'enunciato e e $g = b_0 + b_1x + \ldots + b_mx^m$. Se $g = 0$ allora $g = 0f + 0$. Sia quindi $g \neq 0$ e procediamo per induzione su $m = \deg(g)$.

Sia $m = 0$, allora $g \in A$. Se $n = \deg f \geq 1$ allora possiamo scrivere $g = 0f + g$ e siamo a posto perchè $\deg g = 0 < \deg f$. Se invece $\deg f = 0$, allora $f = a_0$ è invertibile in A e quindi $g = a_0(a_0^{-1}g) = fh + 0$ con $h = a_0^{-1}g$.

Sia ora $m \geq 1$ e supponiamo l'enunciato vero per ogni polinomio dividendo di grado $\leq m - 1$.
Se $m \leq n - 1$ allora $g = 0f + g$ soddisfa le condizioni.
Sia quindi $m \geq n$, e poniamo

$$g_1 = a_ng - b_mx^{m-n}f = a_n(b_0 + b_1x + \ldots + b_mx^m) - b_mx^{m-n}(a_0 + a_1x + \ldots + a_nx^n) =$$

$$= a_n b_0 + \ldots + a_n b_m x^m - a_0 b_m x^{m-n} - \ldots - a_{n-1} b_m x^{m-1} - a_n b_m x^m \ .$$

Allora $\deg g_1 \leq m-1$; quindi, per ipotesi induttiva esistono $h_1, r_1 \in A[x]$ tali che $g_1 = h_1 f + r_1$ e $r_1 = 0$ o $\deg r_1 \leq n-1$. Segue che

$$g = a_n^{-1}(g_1 + b_m x^{m-n} f) = a_n^{-1}(h_1 f + r_1 + b_m x^{m-n} f) = a_n^{-1}(h_1 + b_m x^{m-n}) f + a_n^{-1} r_1$$

e le condizioni dell'enunciato sono soddisfatte con $h = a_n^{-1}(h_1 + b_m x^{m-n})$ ed $r = a_n^{-1} r_1$.

2) (unicità) Supponiamo di poter scivere $g = hf + r = h'f + r'$ con la condizione (ii) soddisfatta. Allora $(h-h')f = r' - r$, se fosse $h \neq h'$ avremmo l'assurdo $\deg(f) \leq \deg((h-h')f) = \deg(r-r') \leq \deg(f) - 1$ (vedi esercizio 9.1). Quindi $h = h'$ da cui discende immediatamente anche $r = r'$. ∎

La dimostrazione del Teorema fornisce anche il metodo per eseguire una divisione tra polinomi (quando consentito); si tratta di ripetere il passo in cui si dividono i monomi di grado massimo, ottenendo un monomio che va moltiplicato per il divisore e quindi sottratto dal polinomio su cui si sta operando, ottenendo così un polinomio di grado inferiore, ed andando avanti. È il solito metodo che si impara nelle scuole.

Esercizio 9.6. Nell'anello $\mathbb{Q}[x]$ dividere $g = 2x^4 - x^2 + 5x$ per $f = x^2 - x + 1$.

Soluzione. La familiare tabella:

$2x^4$		$-x^2$	$+5x$		$x^2 - x + 1$
$2x^4$	$-2x^3$	$+2x^2$			$2x^2 + 2x - 1$
	$2x^3$	$-3x^2$	$+5x$		
	$2x^3$	$-2x^2$	$+2x$		
		x^2	$+3x$		
		x^2	$+x$	-1	
			$2x$	-1	

Quindi, $g = (2x^2 + 2x - 1)f + (2x - 1)$.

Si osservi come, nella dimostrazione del Teorema 9.4, sia essenziale il fatto che il coefficiente direttivo a_n del polinomio divisore f sia invertibile. In particolare, il Teorema si applica al caso in cui f è monico.

Ma ancora più importante è notare che se F è un campo, allora il Teorema sussiste per qualsiasi $f \in F[x]$ purché sia $f \neq 0$. Questo ci conferma che, assumendo come valutazione euclidea il grado $deg : F[x] \to \mathbb{N}$, l'anello dei polinomi $F[x]$ è un dominio euclideo. Di conseguenza (Teorema 8.12), $F[x]$ è un Dominio a Ideali Principali. Questo ultimo fatto è così importante che lo rienunciamo esplicitamente, e ne forniamo anche una dimostrazione diretta (che non è altro che l'adattamento al caso di quella del Teorema 8.12).

Teorema 9.5. *Sia F un campo. Allora*

(1) $F[x]$ è un dominio euclideo;

(2) $F[x]$ è un dominio a ideali principali. Più precisamente: se $I \neq \{0\}$ è un ideale non-nullo di $F[x]$, e $0 \neq f \in I$ è un polinomio di grado minimo *tra quelli non-nulli appartenenti a I, allora $I = (f)$.*

Dimostrazione. (1) Il Teorema 9.4, applicato al caso in cui $A = F$ è un campo, afferma in particolare che $F[x]$, dotato della valutazione data dal grado, è un dominio euclideo.
(2) Questo discende immediatamente dal punto (1) e dal Teorema 8.12; ma vediamo la dimostrazione diretta. Sia I un ideale di $F[x]$. Se $I = \{0\}$ allora $I = (0)$. Sia quindi $I \neq \{0\}$; allora I contiene almeno un elemento non nullo, sia $n = \min\{\deg f \mid f \in I\ , f \neq 0\}$; e sia $f \in I$ tale che $\deg f = n$. Proviamo che $I = (f)$
In un verso, poichè (f) è il minimo ideale che contiene f, e $f \in I$, si ha $(f) \subseteq I$.
Viceversa, sia $g \in I$. Dividiamo g per f:

$$g = fq + r \qquad \text{con} \quad r = 0 \ \text{ o } \ \deg r < \deg f = n\ .$$

Ora $fq \in I$ e quindi $r = g - fq \in I$. Se fosse $r \neq 0$ allora r sarebbe un elemento non nullo di I di grado strettamente minore del grado di f, e questo contraddice la scelta di f in I. Quindi $r = 0$ e di conseguenza $g = fq \in (f)$. Dunque $I \subseteq (f)$; pertanto $I = (f)$, completando la dimostrazione. ∎

Osservazione. Il Teorema precedente non vale in generale per anelli di polinomi a coefficienti in un dominio d'integrità. Ad esempio, nell'anello $\mathbb{Z}[x]$ consideriamo l'insieme

$$I = \{a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x] \mid 2 \ \text{ divide } \ a_0\}\ .$$

Si verifichi per esercizio che I è un ideale di $\mathbb{Z}[x]$ (ad esempio provando che è il nucleo di un opportuno omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$). Di fatto I è l'ideale di $\mathbb{Z}[x]$ generato da x e da 2, ovvero $I = (2, x)$. Supponiamo per assurdo che I sia principale, cioè che esista $a \in \mathbb{Z}[x]$ tale che $I = (a)$. Allora, poichè $2 \in I$, esiste $g \in \mathbb{Z}[x]$ tale che $2 = ag$, ciò implica $\deg a = 0$, cioè $a \in \mathbb{Z}$. Ma è anche $x \in I$ e quindi esiste $h \in \mathbb{Z}[x]$ tale che $x = ah$; per la formula dei gradi, deve essere $h = c + dx$, con $c, d \in \mathbb{Z}$; quindi $x = a(c + dx) = ac + adx$, da cui segue $c = 0$ e $ad = 1$. Dunque $a = \pm 1$, ma allora $I = (a) = \mathbb{Z}[x]$ il che è assurdo perchè $I \neq \mathbb{Z}[x]$.

Sia F un campo. Richiamando le definizioni fissate nella sezione 8.1, e ricordando che gli invertibili di $F[x]$ sono tutti e soli gli elementi non-nulli di F, si conclude che $f, g \in F[x]$ sono *associati* (e quindi, $(f) = (g)$) se e soltanto se $g = af$, per qualche $0 \neq a \in F$. Detto in modo apparentemente più preciso, si ha il seguente Lemma, che non dovrebbe risultare difficile dimostrare.

Lemma 9.6. *Sia F un campo; e siano $0 \neq f, g \in F[x]$ con g un divisore di f. Allora*

(i) g è un divisore proprio se e solo se $0 < \deg g < \deg f$;

(ii) $f|g$ se e solo se esiste $0 \neq c \in F$ tale che $g = cf$.

(Si rifletta a come e perché tali affermazioni non valgano se l'anello dei coefficienti non è un campo - ad esempio nel caso di $\mathbb{Z}[x]$).

In particolare, i polinomi generatori di un ideale $\{0\} \neq I$ di $F[x]$ differiscono tra loro per il prodotto di un elemento non nullo di F (in particolare, hanno lo stesso grado, che è il minimo tra i gradi degli elementi non-nulli di I).
Se $f = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ è un polinomio non nullo a coefficenti in F, con $a_n \neq 0_F$, allora a_n è invertibile in F, e si può scrivere

$$f = a_n(x^n + a_n^{-1}a_{n-1}x^{n-1} + \ldots + a_n^{-1}a_1x + a_n^{-1}a_0.)$$

Ovvero $f = a_n f_0$ è il prodotto del suo coefficiente direttivo a_n per un polinomio monico f_0 (che, è chiaro, sono univocamante individuati da f). Quindi, ogni ideale non nullo di $F[x]$ ha uno ed un solo generatore *monico*.

Queste osservazioni conducono al fatto che i divisori propri di un $f \in F[x] \setminus F$ hanno grado strettamente minore di quello di f. In particolare si ricava una descrizione degli elementi irriducibili di $F[x]$ (F è sempre un campo) che è molto conveniente: *un polinomio $f \in F[x]$ è* **irriducibile** *in $F[x]$ se e solo se* $\deg f \geq 1$ *e f non ha divisori di grado strettamente minore di $\deg f$.*
In altri termini $f \in F[x] \setminus F$ è irriducibile se non è possibile scrivere $f = gh$ con g e h polinomi tali che $\deg g < \deg f$ e $\deg h < \deg f$. In particolare, ogni polinomio di grado 1 in $F[x]$ è irriducibile. Si noti che questo non è più vero se i coefficienti non sono su un campo; ad esempio il polinomio $2x - 6$ è riducibile in $\mathbb{Z}[x]$ come prodotto dei divisori propri $2(x - 3)$ (infatti, 2 non è invertibile in $\mathbb{Z}[x]$).

Esempio. Il polinomio $x^3 + 2x^2 + 2x + 1 \in \mathbb{Q}[x]$ è riducibile in $\mathbb{Q}[x]$; infatti si trova facilmente che $x^3 + 2x^2 + 2x + 1 = (x + 1)(x^2 + x + 1)$. Mentre $x^2 + x + 1$ è un polinomio irriducibile di $\mathbb{Q}[x]$ (lo si dimostri).

Un'ovvia avvertenza è che un polinomio va sempre considerato come un elemento dell'anello dei polinomi a coefficienti in un esplicito anello commutativo, ed è in tale anello dei polinomi che ha senso chiedersi se sia o meno irriducibile (si vedano esempi nella prossima sezione).

Massimo comun divisore tra polinomi. Sia ancora F un campo. La proprietà di fattorizzazione unica di $F[x]$ assicura che ogni coppia di polinomi f e g in $F[x]$ ammette un massimo comun divisore d (come abbiamo visto in generale per gli UFD nella sezione 8.1).
Poiché $F[x]$ è anche un PID, le osservazioni poste alla fine della sezione 8.3 comportano che se $d \in F[x]$ è un massimo comun divisore di f e g, allora d può essere scritto nella forma

$$d = \alpha \cdot f + \beta \cdot g$$

con $\alpha, \beta \in F[x]$; anzi, d è, tra i polinomi che si scrivono in questa forma, uno di grado minimo (diverso da zero). Inoltre, dal Lemma 9.6, segue che, se d e d_1 sono due massimi comun divisori di f e g, esiste un $0 \neq a \in F$ tale che $d_1 = ad$. Ne segue, sempre per il Lemma 9.6, che f e g hanno un *unico* massimo comun divisore *monico*, che si denota quindi con (f, g). Come nel caso degli interi, diremo che due polinomi a coefficienti su un campo f e g sono *coprimi* se $(f, g) = 1$.
Infine, anche con l'anello $F[x]$, per calcolare il massimo comun divisore di due polinomi non nulli, è possibile applicare l'algoritmo di Euclide. La procedura è la stessa del caso dei numeri interi (ed è fondata sulla divisione euclidea, Teorema 9.4), per cui, invece che descriverla nuovamente in generale, ci limitiamo a fornire un esempio della sua applicazione.

Esercizio 9.7. Calcolare un MCD in $\mathbb{Q}[x]$ dei polinomi:

$$f = 12x^7 + 5x^5 + 10x^4 - 7x^3 + 10x^2 \qquad g = 2x^5 - x^4 + 2x^3 + 1.$$

Soluzione. L'algoritmo di Euclide opera mediante divisioni successive. In questo caso si ha:

$$\begin{array}{ll} f = (6x^2+3x-2)g + r_1 & r_1 = 2x^4 - 3x^3 + 4x^2 - 3x + 2 \\ g = (x+1)r_1 + r_2 & r_2 = x^3 - x^2 + x - 1 \\ r_1 = (2x-1)r_2 + r_3 & r_3 = x^2 + 1 \\ r_2 = (x-1)r_3 + 0 & \end{array}$$

quindi $r_3 = x^2 + 1$ è un MCD di f e g.

Esercizio 9.8. Si dica per quali valori di $a \in \mathbb{Q}$, x^2+1 divide $x^4 + 3x^3 + x - a^2$ nell'anello $\mathbb{Q}[x]$.

Esercizio 9.9. In $\mathbb{Q}[x]$ si considerino i polinomi

$$f = x^5 - 2x^4 + x^3 - 9x^2 + 18x - 9 \qquad g = x^5 - x^3 - 9x^2 + 9 \ .$$

Determinare un massimo comun divisore di f e g.

Esercizio 9.10. Si dica per quali $a \in \mathbb{Z}$ i seguenti polinomi sono coprimi in $\mathbb{Q}[x]$,

$$3x^4 + 4x^3 + ax^2 + ax + a \qquad\qquad x^2 + 2x + 1 \ .$$

Esercizio 9.11. Sia $g = \overline{2}x + \overline{2} \in \mathbb{Z}_4[x]$. Si provi che se $f \in \mathbb{Z}_4[x]$ è un polinomio monico, allora non esiste alcuna coppia $q, r \in \mathbb{Z}_4[x]$ tale che $f = qg + r$ e $\deg r < \deg f$.

Esercizio 9.12. Sia R un dominio di integrità. Provare che se R non è un campo, $R[x]$ non è un dominio a ideali principali.

9.3 Radici e fattorizzazioni.

Un'immediata conseguenza del Teorema 9.5 e del Teorema 8.11 è la seguente.

Corollario 9.7. *Sia F un campo. Allora $F[x]$ è un dominio a fattorizzazione unica.*

Quindi, ogni polinomio non nullo di grado diverso da zero a coefficienti su un campo F (ciò vale a dire: ogni elemento non zero e non invertibile di $F[x]$) si fattorizza in modo essenzialmente unico come prodotto di polinomi irriducibili. Poiché ogni classe di polinomi irriducibili associati contiene uno ed un solo polinomio monico, possiamo concludere che, se F è un campo, allora *ogni polinomio $f \in F[x] \setminus F$ si scrive in modo unico (a meno dell'ordine dei fattori) come $f = a_n f_1 f_2 \dots f_k$ dove a_n è il coefficiente direttivo di f e $f_1, f_2, \dots, f_k$ sono polinomi monici irriducibili in $F[x]$.*

Esempio. Vediamo le fattorizzazioni in irriducibili del polinomio $x^4 + 1$ rispettivamente in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.

$x^4 + 1$ è irriducibile in $\mathbb{Q}[x]$ (lo si provi per esercizio).

$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ in $\mathbb{R}[x]$.

$x^4 + 1 = (x - \omega_1)(x - \omega_2)(x - \omega_3)(x - \omega_4)$ in $\mathbb{C}[x]$,

dove $\omega_1 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ \omega_2 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ \omega_3 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},\ \omega_4 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.

(osserviamo che dalla fattorizzazione in $R[x]$ si deduce che x^4+1 è irriducibile in $\mathbb{Q}[x]$; infatti x^4+1 non ha radici in $\mathbb{Q}$ e quindi non ha fattori di grado 1, se si decomponesse in $\mathbb{Q}[x]$ come prodotto di due fattori (monici) di grado 2, allora tali fattori sarebbero anche i fattori nella decomposizione in $R[x]$ e quindi, per l 'unicità della fattorizzazione, dovrebbero coincidere con i fattori scritti sopra che tuttavia non sono a coefficienti razionali).

Osservazione importante. Ribadisco ancora una volta che se R è un dominio d'integrità ma non è un campo, allora $R[x]$ non è un PID. Lo abbiamo già verificato nel caso $R = \mathbb{Z}$ nell'esempio che segue il Teorema 9.5: un ideale non principale di $\mathbb{Z}[x]$ è, per esempio l'ideale $(p, x) = \{pf + xg \mid f, g \in \mathbb{Z}[x]\}$. Si cerchi di adattare questo argomento a qualsiasi dominio R che possiede elementi non-nulli e non–invertibili.
Nella prossima sezione proveremo tuttavia che anche $\mathbb{Z}[x]$ è un UFD, provando così in particolare che esistono domini a fattorizzazione unica che non sono a ideali principali.

Definizione. Sia R un anello e $0 \neq f \in R[x]$. Un elemento $a \in R$ si dice **radice** (o, anche, "zero") di f se $f(a) = 0$.

Un primo criterio di riducibilità (cioè di esistenza di divisori propri) di un polinomio è il noto Teorema di Ruffini. Si tratta, in fin dei conti, di una conseguenza del Teorema 9.4, e dunque, ancora una volta, è una proprietà dei polinomi per la quale è richiesto che l'anello dei coefficienti sia un campo.

Teorema 9.8. (di Ruffini) *Sia A un anello commutativo, $0 \neq f \in A[x]$ ed $a \in A$. Allora a è una radice di f se e solo se $(x-a)$ divide f.*

Dimostrazione. Supponiamo $f(a) = 0$, e dividiamo f per $x - a$. Esistono $h, r \in A[x]$ tali che $f = (x-a)h + r$, con $r = 0$ o $\deg r = 0$. Quindi, in ogni caso, $r \in A$ e dunque $r(a) = r$. Ora

$$0 = f(a) = (a-a)h(a) + r(a) = 0h(a) + r = r$$

quindi $f = (x-a)h$ cioè $(x-a)$ divide f.
Viceversa, supponiamo che $(x-a)$ divida f. Allora $f = (x-a)h$ per qualche $h \in A[x]$ e pertanto

$$f(a) = (a-a)h(a) = 0h(a) = 0$$

quindi a è una radice di f. ∎

Osserviamo che una conseguenza banale del Teorema di Ruffini è che un polinomio $0 \neq f$ a coefficienti in un campo F ha divisori di primo grado se e soltanto se ha radici in F. Infatti se $g = ax + b$ (con $a, b \in F$) è un divisore di f, allora $g = a(x - (-ba^{-1}))$, e quindi anche $x - (-ba^{-1})$ è un divisore di f; pertanto $-ba^{-1}$ è una radice di f.

Esempio. Il polinomio $x^2 + x - 1$ è irriducibile in $\mathbb{Q}[x]$ dato che ha grado 2 e non ha radici in $\mathbb{Q}$ (e quindi non ha divisori di grado 1 in $\mathbb{Q}[x]$); d'altra parte $x^2 + x - 1$ è riducibile in $\mathbb{R}[x]$, dato che, in $\mathbb{R}[x]$,

$$x^2 + x - 1 = \left(x - \frac{-1+\sqrt{5}}{2}\right)\left(x - \frac{-1-\sqrt{5}}{2}\right).$$

L'esempio che abbiamo dato tratta un polinomio di secondo grado a coefficienti reali, per i quali esiste una ben nota formula esplicita per il calcolo delle radici. Per polinomi di grado superiore, applicare il teorema di Ruffini ai fini di studiare l'irriducibilità è meno agevole (il famoso teorema di Galois asserisce, in particolare, che non esistono formule risolutive generali per calcolare le radici di un polinomio razionale di grado maggiore o uguale a 5); tuttavia, almeno per polinomi monici in $\mathbb{Q}[x]$ i cui coefficienti sono tutti degli interi, c'è un facile trucco. Sia $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ un polinomio monico in $\mathbb{Q}[x]$, tale che i coefficienti $a_0, a_1, \ldots, a_{n-1}$ sono numeri interi e $a_0 \neq 0$. Supponiamo che $q \in \mathbb{Q}$ sia una radice di f. Sia $q = a/b$, con $a, b \in \mathbb{Z}$, $(a, b) = 1$ e $b \geq 1$. Allora

$$0 = f(\alpha) = q^n + a_{n-1}q^{n-1} + \ldots + a_1 q + a_0 = \frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \ldots + a_1\frac{a}{b} + a_0.$$

Moltiplicando per b^n si ha

$$-a^n = a_{n-1}a^{n-1}b + \ldots + a_1 a b^{n-1} + a_0 b^n.$$

Questa è una relazione tra numeri interi, e siccome a e b sono coprimi, da essa segue che $b = 1$. Dunque $q = a \in \mathbb{Z}$; inoltre $-a_0 = a^n + a_{n-1}a^{n-1} + \ldots + a_1 a = (a^{n-1} + a_{n-1}a^{n-2} + \ldots + a_1)a$, e dunque a divide a_0 in $\mathbb{Z}$. Abbiamo cioè provato che le eventuali radici in $\mathbb{Q}$ di un polinomio monico i cui coefficienti sono numeri interi, sono numeri interi che dividono (come numeri interi) il termino noto a_0 del polinomio (questa osservazione è generalizzata nell'esercizio 9.13). Ad esempio, il polinomio $f = x^4 + 2x^3 - 7x + 1$ non ha radici in $\mathbb{Q}$ (e dunque non ha divisori di primo grado in $\mathbb{Q}[x]$), dato che 1 e -1 non sono radici di f.

Torniamo ad occuparci di polinomi su un campo generico. Sia $0 \neq f$ un polinomio a coefficienti sul campo F e sia $a \in F$ una radice di f. Allora $(x - a)$ divide f, e quindi si può scrivere $f = (x - a)g$ con $g \in F[x]$. A sua volta, a potrebbe essere una radice di g; in tal caso $(x - a)$ divide g, e quindi $(x - a)^2$ divide f. Dunque, se a è una radice di f, esiste un massimo intero positivo $m(a)$ tale che $(x - a)^m$ divide f. Tale intero si chiama *molteplicità (algebrica)* della radice a, e chiaramente soddisfa $1 \leq m(a) \leq \deg f$. Possiamo fattorizzare f come $f = (x - a)^{m(a)}h$, dove $h \in F[x]$, e $h(a) \neq 0$. Se $m(a) = 1$, la radice a si dice *semplice*, altrimenti si dice multipla. Un criterio per il calcolo delle eventuali radici multiple di un polinomio $f \in F[x]$ è fornito dall'esercizio 9.34.

Considerazioni di simile natura sono applicate per dimostrare la seguente e importantissima conseguenza del Teorema di Ruffini.

Teorema 9.9. *Sia F un campo e $0 \neq f \in F[x]$, con $n = \deg f$. Allora il numero di radici distinte di f in F è al più n.*

Dimostrazione. Siano $\alpha_1, \alpha_2, \ldots, \alpha_k$ radici distinte di f in F. Procedendo per induzione su k proviamo che $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ divide f. Per $k = 1$ è il teorema di Ruffini. Sia quindi $k \geq 2$ e assumiamo per ipotesi induttiva che $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})$ divida f. Sia $g \in F[x]$ tale che $f = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_{k-1}) \cdot g$. Allora

$$0 = f(\alpha_k) = (\alpha_k - \alpha_1)(\alpha_k - \alpha_2)\cdots(\alpha_k - \alpha_{k-1})g(\alpha_k)$$

in cui il termine di destra è un prodotto di elementi del campo F; quindi, poichè $\alpha_k \neq \alpha_i$ per $i = 1, 2, \ldots, k-1$, deve essere $g(\alpha_k) = 0$. Per il Teorema di Ruffini

$(x-\alpha_k)$ divide g, quindi $g=(x-\alpha_k)h$ per un $h\in F[x]$ e dunque

$$f=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})(x-\alpha_k)h$$

Quindi, per il principio di induzione, l'affermazione è provata. Ora se $\alpha_1,\alpha_2,\ldots,\alpha_t$ sono *tutte* le radici distinte di f, per quanto appena visto $d=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)$ divide f e quindi $n=\deg f\geq \deg d=t$. ∎

In effetti, il Teorema precedente può essere reso ulteriormente preciso nel modo seguente (la verifica consiste nel ripercorrere con attenzione la dimostrazione del Teorem 9.9 tenendo conto delle osservazioni che lo precedono, ed è lasciata per esercizio).

Teorema 9.10. *Sia F un campo, e sia $0\neq f\in F[x]$, un polinomio non nullo di grado n. Siano $a_1, a_2,\ldots,a_k$ le radici distinte di f in F, e per ogni $i=1,2,\ldots,k$, sia $m_i=m(a_i)$ la molteplicità della radice a_i. Allora $m_1+m_2+\cdots+m_k\leq n$.*

Vediamo un'interessante applicazione alla teoria dei numeri.

Teorema 9.11. (**Teorema di Wilson**) *Sia p un numero primo positivo. Allora*

$$(p-1)!\equiv -1 \pmod p.$$

Dimostrazione. Sia p un primo positivo (che chiaramente possiamo supporre dispari), e consideriamo il campo $\mathbb{Z}/p\mathbb{Z}$. Sappiamo, dal teorema di Fermat, che

$$0\neq \overline{a}\in\mathbb{Z}/p\mathbb{Z} \quad\Rightarrow\quad \overline{a}^{p-1}=\overline{1}.$$

Quindi $\overline{1}$, $\overline{2}$, $\overline{3},\ldots,\overline{p-1}$ sono le radici distinte del polinomio $x^{p-1}-\overline{1}\in\mathbb{Z}/p\mathbb{Z}[x]$. Allora, per la dimostrazione di 7.4,

$$x^{p-1}-\overline{1}=(x-\overline{1})(x-\overline{2})(x-\overline{3})\cdots(x-\overline{p-1}).$$

Confrontando i termini noti si trova che

$$-\overline{1}=(-\overline{1})\cdot(-\overline{2})\cdot(-\overline{3})\cdot\ldots\cdot(-\overline{p-1})=(-1)^{p-1}\overline{1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)}=\overline{(p-1)!}$$

e quindi $(p-1)!\equiv -1 \pmod p$. ∎

Esercizio 9.13. Sia $f=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$, con $a_0, a_1,\ldots, a_n\in\mathbb{Z}$, e sia $u=a/b\in\mathbb{Q}$ (con $a,b\in\mathbb{Z}$, $b\geq 1$ e $(a,b)=1$). Si provi che se u è una radice di f, allora $b|a_n$ e $a|a_0$.

Esercizio 9.14. Si provi che i polinomi a coefficienti razionali

$$x^3+x^2+x+2 \qquad \text{e} \qquad x^4+1$$

sono irriducibili in $\mathbb{Q}[x]$.

Esercizio 9.15. Si provi che il polinomio x^3-x ha sei radici distinte in $\mathbb{Z}_6$.

Esercizio 9.16. ia F un campo. Provare che in $F[x]$ esistono infiniti polinomi monici irriducibili. [imitare la dim. dell'infinità di numeri primi]

Esercizio 9.17. Si provi che il polinomio $x^2 + x + \overline{1}$ è irriducibile in $(\mathbb{Z}/5\mathbb{Z})[x]$. Si provi che il polinomio $x^2 + x + \overline{1}$ è riducibile in $(\mathbb{Z}/7\mathbb{Z})[x]$. Si studi la riducibilità del polinomio $x^3 + \overline{1}$ in $(\mathbb{Z}/11\mathbb{Z})[x]$.

Serie formali. Questa breve appendice, in cui descriviamo un'estensione dell'idea di anello dei polinomi, è complementare al materiale specifico del corso e può ragionevolmente essere presa come una lettura, come materiale per esercizi, o carta da riciclare. L'abbiamo inserita perché ci consente di accennare ad altri esempi interessanti (anche se concettualmente un po' alieni) di domini a ideali principali, e può suggerire un inquadramento anche algebrico della teoria dello sviluppo in serie (ci vuole però sempre cautela).

Dato un campo F l'insieme delle espressioni (dette *serie formali*)

$$\sum_{i\in\mathbb{N}} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

con $a_i \in F$ per ogni $i \in \mathbb{N}$, costituisce un dominio di integrità (esercizio 9.18) rispetto alle operazioni di somma e prodotto che estendono quelle definite per i polinomi:

$$\sum_{i\in\mathbb{N}} a_i x^i + \sum_{i\in\mathbb{N}} b_i x^i = \sum_{i\in\mathbb{N}} (a_i + b_i) x^i$$

$$\left(\sum_{i\in\mathbb{N}} a_i x^i\right)\left(\sum_{i\in\mathbb{N}} b_i x^i\right) = \sum_{i\in\mathbb{N}} c_i x^i$$

dove, per ogni $i \in \mathbb{N}$,

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

L'anello così definito si dice *anello delle serie formali (a coefficienti in F)* e si denota con il simbolo $F[[x]]$.
Le serie formali con solo un numero finito di coefficienti non nulli, (ovvero le serie $\sum a_i x^i$ per cui esista un $n \in \mathbb{N}$ tale che $a_i = 0$ per ogni $i \geq n$), cioè i *polinomi* a cofficienti in F, costituiscono un sottoanello di $F[[x]]$. In particolare, identifichiamo gli elementi di F con le serie formali $\sum a_i x^i$ tali che $a_i = 0$ per ogni $i \geq 1$.

Proviamo ora che gli elementi invertibili dell'anello $F[[x]]$ sono tutti e soli quelli del tipo $\sum a_i x^i$ con $a_0 \neq 0$. La serie $\alpha = \sum a_i x^i$ è infatti invertibile in $F[[x]]$ se e solo se esiste $\beta = \sum b_i x^i$ tale che

$$1_{F[[x]]} = 1 + 0x + 0x^2 + \ldots = \alpha\beta = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$

ovvero se e solo se esistono $b_0, b_1, b_2 \ldots \in F$ tali che

$$a_0 b_0 = 1 \qquad a_0 b_1 + a_1 b_0 = 0 \qquad a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \qquad \ldots \ .$$

Si osserva subito, quindi, che la condizione $a_0 \neq 0$ è necessaria per l'invertibilità di $\sum a_i x^i$. D'altra parte, se $a_0 \neq 0$ definiamo $b_0 = a_0^{-1}$ e per induzione, definiti $b_0, b_1, \ldots, b_{i-1}$, poniamo

$$b_i = -a_0^{-1}(\sum_{j=1}^{i} a_j b_{i-j}).$$

La serie $\sum b_i x^i$ è quindi l'inversa della serie $\sum a_i x^i$, ed abbiamo provato che la condizione $a_0 \neq 0$ è anche sufficiente.

Ad esempio, l'inversa della serie geometrica $\sum_{i\in\mathbb{N}} x^i = 1 + x + x^2 + x^3 + \dots$ è il polinomio $1 - x$ (fare i calcoli).

Osserviamo in particolare che l'insieme degli elementi non invertibili di $F[[x]]$ è pertanto

$$J = \left\{ \sum a_n \in F[[x]] \mid a_0 = 0 \right\}$$

che non è altro che l'ideale principale generato dall'elemento x: cioè $J = (x)$. Questo comporta, in particolare, che ogni ideale proprio di $F[[x]]$ è contenuto in J. Infatti, sia I un ideale di $F[[x]]$ e supponiamo che $I \not\subseteq J$; allora esiste $f \in I \setminus J$; poiché $f \notin J$, f è invertibile per quanto provato in precedenza, dunque $F[[x]] = (f) \subseteq I$, e questo prova che $I = F[[x]]$ non è proprio.
Un anello commutativo A che ammette un ideale proprio J che contiene ogni altro ideale proprio, si dice *anello locale*. La condizione è equivalente (vedi Esercizio 6.48) all'essere $A \setminus J$ l'insieme degli elementi invertibili di A (ogni campo è, in modo banale, un anello locale).

Vediamo ora come $F[[x]]$ sia un dominio a ideali principali.
Cominciamo con l'osservare che, a differenza dell'anello dei polinomi $F[x]$, che possiede (per ogni campo F) un numero infinito di polinomi monici irriducibili (esercizio 8.1), l'anello delle serie formali $F[[x]]$ ha, a meno di associati, *un solo* elemento irriducibile. Il polinomio x è infatti un elemento irriducibile di $F[[x]]$ (verificare) e se $\pi = \sum_{i=0}^{\infty} a_i x^i$ non è invertibile, esiste $n \geq 1$ tale che $a_i = 0$ per ogni $0 \leq i < n$ e $a_n \neq 0$, per cui

$$\pi = x^n \sum_{i=0}^{\infty} a_{n+i} x^i \quad \sim \quad x^n \tag{9.2}$$

dato che $\sum a_{n+i} x^i$ è invertibile, e quindi π è irriducibile se e solo se $n = 1$ e $\pi \sim x$. La (9.2) dice come sono le fattorizzazioni in irriducibili in $F[[x]]$: ogni $f \in F[[x]]$ si scrive in modo unico nella forma $f = x^n g$ con $n \geq 0$ e g invertibile. Infine, gli ideali di $F[[x]]$ sono $\{0\}$ e tutti e soli quelli del tipo (x^n) con $n \geq 0$.

Esercizio 9.18. Si provi che $F[[x]]$ è un dominio d'integrità.

Esercizio 9.19. In $\mathbb{R}[[x]]$ si calcoli l'inversa della serie formale

$$f = \sum_{n\in\mathbb{N}} \frac{x^n}{n!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

Esercizio 9.20. Sia I un ideale proprio di $F[[x]]$. Si provi che esiste $n \in \mathbb{N}$ tale che $I = (x^n)$. Si deduca che $F[[x]]$ è un dominio a ideali principali. Si dica se $F[[x]]$ è un dominio euclideo.

9.4 Fattorizzazioni in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$

In questa sezione dimostreremo, in particolare, che $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica (quindi $\mathbb{Z}[x]$ è un esempio di UFD che non è un PID), e vedremo come il problema della fattorizzazione in $\mathbb{Q}[x]$ si riconduca a quello della fattorizzazione in $\mathbb{Z}[x]$. Le

idee, anche se espresse in modo formale, sono del tutto elementari, a partire dal - raccoglimento del fattor comune per i polinomi interi. Per comodità, denoteremo con $\mathbb{Z}_p$ l'anello delle classi resto $\mathbb{Z}/p\mathbb{Z}$.

Definizione. Sia $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ un polinomio non nullo in $\mathbb{Z}[x]$. f si dice **primitivo** se $\mathrm{MCD}(a_0, a_1, a_2, \ldots, a_n) = 1$.

Sia $0 \neq f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ e sia $d = \mathrm{MCD}(a_0, a_1, \ldots, a_n)$. Allora, chiaramente, $f_0 = \frac{a_0}{d} + \frac{a_1}{d}x + \ldots + \frac{a_n}{d}x^n$ è un polinomio primitivo in $\mathbb{Z}[x]$ e $f = df_0$. Inoltre se $f = cf_1$ con $c \in \mathbb{Z}$ e $f_1 \in \mathbb{Z}[x]$ primitivo, allora c divide tutti i coefficienti di f e quindi $c|d$; similmente $\frac{d}{c}$ divide tutti i coefficienti di f_1 che è primitivo, quindi $c = \pm d$ e $f_1 = \pm f_0$. Pertanto abbbiamo il seguente

Lemma 9.12. *Sia $0 \neq f \in \mathbb{Z}[x]$. Allora $f = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo, e tale fattorizzazione è unica a meno del segno.*

Osservazione che ciò si estende facilmente al caso razionale.

Lemma 9.13. *Sia $0 \neq f \in \mathbb{Q}[x]$. Allora $f = \gamma f_0$ con $\gamma \in \mathbb{Q}$ e f_0 un polinomio primitivo in $\mathbb{Z}[x]$. Tale fattorizzazione è unica a meno del segno.*

Dimostrazione. Sia $0 \neq f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Q}[x]$. Per ogni $i = 0, \ldots, n$ sia $a_i = \frac{r_i}{s_i}$ con $r_i, s_i \in \mathbb{Z}$. Allora, posto $s = s_1s_2 \ldots s_n$, si ha $sf \in \mathbb{Z}[x]$ dunque, per il Lemma 9.12, $sf = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo, e quindi $f = \frac{d}{s}f_0$ con $\frac{d}{s} \in \mathbb{Q}$. Supponiamo ora che $f = \frac{a}{b}f_1$ con $\frac{a}{b} \in \mathbb{Q}$ $(a, b \in \mathbb{Z})$ e f_1 primitivo in $\mathbb{Z}[x]$; allora $bdf_0 = asf_1$ e, ancora per il Lemma 9.12, $f_1 = \pm f_0$ e $bd = \pm as$ da cui $\frac{a}{b} = \pm\frac{d}{s}$. ∎

Veniamo ora al Lemma fondamentale per quanto riguarda i polinomi primitivi. Per la sua dimostrazione è conveniente utilizzare la riduzione modulo un primo p dei polinomi interi, cioè l'omomorfismo

$$\begin{array}{ccc} \mathbb{Z}[x] & \to & \mathbb{Z}_p[x] \\ f & \mapsto & \overline{f} \end{array}$$

dove se $f = a_0 + a_1x + \ldots + a_nx^n$, $\overline{f} = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n$ (vedi sezione 7.1). Osserviamo che $\overline{f} = 0$ se e soltanto se il primo p divide tutti i coefficienti di f; in particolare, se f è primitivo allora $\overline{f} \neq 0$ nella riduzione per qualsiasi primo p.

Lemma 9.14 (Lemma di Gauss)**.** *Il prodotto di polinomi interi primitivi è primitivo.*

Dimostrazione. Siano $f, g \in \mathbb{Z}[x]$ e supponiamo che il prodotto fg **non** sia primitivo. Allora esiste un primo p che divide tutti i coefficienti di fg. Considerando la riduzione modulo p si ha dunque (ricordando che la riduzione è un omomorfismo):

$$0 = \overline{fg} = \overline{f} \cdot \overline{g}$$

che è una uguaglianza nel dominio d'integrità $\mathbb{Z}_p[x]$. Dunque deve essere $\overline{f} = 0$ oppure $\overline{g} = 0$ e quindi, per quanto osservato, f e g non possono essere entrambi primitivi, dimostrando così il Lemma. ∎

Proposizione 9.15. *Sia $0 \neq f \in \mathbb{Q}[x]$ e scriviamo $f = \gamma f_0$ con $\gamma \in \mathbb{Q}$ e $f_0 \in \mathbb{Z}[x]$ primitivo. Allora f è irriducibile in $\mathbb{Q}[x]$ se e solo se f_0 è irriducibile in $\mathbb{Z}[x]$.*

Dimostrazione. Supponiamo che il polinomio f sia riducibile in $\mathbb{Q}[x]$, cioè che $f = gh$ con $g, h \in \mathbb{Q}[x]$ e $\deg g, \deg h < \deg f$. Scriviamo $g = \alpha g_0$, $h = \beta h_0$ con $\alpha, \beta \in \mathbb{Q}$ e g_0, h_0 polinomi primitivi in $\mathbb{Z}[x]$. Allora $f = \gamma f_0 = \alpha\beta g_0 h_0$. Per il Lemma di Gauss, $g_0 h_0$ è primitivo, e quindi, per il Lemma 9.13, $f_0 = \pm g_0 h_0$ provando che f_0 si riduce in $\mathbb{Z}[x]$.

Viceversa, supponiamo che f_0 si riduca in $\mathbb{Z}[x]$: $f_0 = gh$ con $g, h \in Z[x]$ e $g \neq \pm 1 \neq h$. Poiché f_0 è primitivo, né g né h appartengono a $\mathbb{Z}$; quindi $\deg g < \deg f_0 = \deg f$ e $\deg h < \deg f$, e dunque $f = (\gamma h)g$ è una decomposizione in fattori propri di f in $\mathbb{Q}[x]$, provando così che f è riducibile in $\mathbb{Q}[x]$. ∎

Questa proposizione mostra, in particolare, che il problema della determinazione della irriducibilità o meno di un polinomio razionale si riconduce al caso di un polinomio intero primitivo. Riterneremo più avanti su questa questione. Prima proviamo il risultato principale di questa sezione.

Teorema 9.16. *$\mathbb{Z}[x]$ è un dominio a fattorizzazione unica;*

Dimostrazione. Sia $f \in \mathbb{Z}[x] \setminus \{0, 1, -1\}$. Proviamo che f ammette un fattorizzazione essenzialmente unica in irriducibili (osserviamo che in questo caso essenzialmente unica significa a meno dell'ordine e del segno dei fattori).
Cominciamo con lo scrivere $f = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo, e fattorizziamo f in $\mathbb{Q}[x]$, $f = g_1 g_2 \dots g_k$, con g_i polinomi irriducibili in $\mathbb{Q}[x]$ individuati a meno di moltiplicazione per elementi non nulli di $\mathbb{Q}$. Quindi scriviamo ciascun g_i come $g_i = \gamma_i g_i'$ con $\gamma_i \in \mathbb{Q}$, g_i' polinomio primitivo in $\mathbb{Z}[x]$ individuati a meno del segno. Allora, posto $\gamma = \gamma_1 \gamma_2 \dots \gamma_k$,

$$df_0 = f = \gamma g_1' g_2' g_3' \ \dots \ g_k' \ .$$

Per il Lemma di Gauss $g = g_1' g_2' \dots g_k'$ è primitivo e quindi, per il Lemma 9.13, $\gamma = \pm d$ e $g = \pm f_0$. Inoltre, per la Proposizione 9.15, ogni g_i' è irriducibile in $\mathbb{Z}[x]$.
Quindi, se $d = \pm 1$, allora (a meno del segno)

$$f = g_1' g_2' g_3' \ \dots \ g_k'$$

è una fattorizzazione di f in irriducibili di $\mathbb{Z}[x]$.
Se $d \neq \pm 1$, si fattorizza $d = p_1 p_2 \dots p_s$ come prodotto di primi di $\mathbb{Z}$ (che sono elementi irriducibili in $\mathbb{Z}[x]$) e quindi

$$f = p_1 p_2 \dots p_s g_1' g_2' g_3' \ \dots \ g_k' \qquad (*)$$

è una fattorizzazione di f in irriducibili di $\mathbb{Z}[x]$.
Infine la (essenziale) unicità delle fattorizzazioni $f = df_0$, $d = p_1 p_2 \dots p_s$ e di f come polinomio in $\mathbb{Q}[x]$, assicurano che la fattorizzazione $(*)$ è essenzialmente unica. ∎

Abbiamo dimostrato il Teorema 9.16 per l'anello $\mathbb{Z}$, ma, con un po' di attenzione, non è difficile generalizzare gli argomenti usati ad un qualunque dominio a fattorizzazione unica R. In questo caso, il ruolo svolto da $\mathbb{Q}$ è affidato al campo dell frazioni (sezione

7.3) di R, e la locuzione "a meno del segno" rimpiazzata con "a meno di moltiplicazione per elementi invertibili di R". Si può cosi dimostrare la seguente versione più generale.

Teorema 9.17. *Sia R un dominio a fattorizzazione unica. Allora $R[x]$ è un dominio a fattorizzazione unica.*

Vediamo ora alcuni strumenti pratici che possono essere usati per studiare la riducibilità di un polinomio intero (o razionale). Cominciamo con il richiamare un'osservazione elementare ma utile, la cui dimostrazione si trova nella sezione precedente.

Sia $f = a_0 + a_1 x + \ldots + x^n$ un polinomio monico a coefficienti interi. Allora ogni radice razionale di f è un numero intero e divide a_0.

Esempio 1. Proviamo che il polinomio $x^3 + 2x^2 - x + 2$ è irriducibile in $\mathbb{Q}[x]$. Se f fosse riducibile dovrebbe avere un fattore di grado 1 (attenzione! questa affermazione vale perchè $\deg f \leq 3$) e quindi, per il Teorema di Ruffini, una radice in $\mathbb{Q}$. Ora, per l'osservazione precedente, le eventuali radici razionali di f sono divisori interi di 2. Ma $f(1) = 4,\ f(-1) = 4,\ f(2) = 16$ e $f(-2) = 4$; quindi f non ha radici razionali e pertanto è irriducibile in $\mathbb{Q}[x]$.

Vediamo ora una applicazione della riduzione modulo un primo. Sia p un numero primo. Allora come abbiamo visto, la riduzione modulo p è un omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$; seguendo le notazioni adottate precedentemente, denotiamo con $\overline{f}$ la riduzione modulo p del polinomio $f \in \mathbb{Z}[x]$. Sia f un polinomio primitivo in $\mathbb{Z}[x]$ tale che p non divida il coefficiente direttivo a_n di f. Supponiamo che f sia riducibile in $\mathbb{Z}[x]$; allora $f = gh$ con g, h polinomi in $\mathbb{Z}[x]$ il cui grado (essendo f primitivo) è strettamente minore del grado di f ed il cui coefficiente direttivo non è diviso da p. Applicando la riduzione modulo p si ha $\overline{f} = \overline{g}\overline{h}$ in $\mathbb{Z}_p[x]$, e per la condizione sul coefficiento direttivo, $\deg \overline{g} < \deg \overline{f}$ e $\deg \overline{h} < \deg \overline{f}$. Quindi $\overline{f}$ è riducibile in $\mathbb{Z}_p[x]$. Possiamo enunciare quanto abbiamo così stabilito nel modo seguente:

Criterio 1. *Sia f un polinomio primitivo in $\mathbb{Z}[x]$, sia p un primo che non divide il coefficiente direttivo di f e sia $\overline{f} \in \mathbb{Z}_p[x]$ la riduzione di f modulo p. Se $\overline{f}$ è irriducibile in $\mathbb{Z}_p[x]$ allora f è irriducibile in $\mathbb{Z}[x]$ (e quindi anche in $\mathbb{Q}[x]$).*

Esempio 2. Proviamo che il polinomio

$$\frac{2}{3}x^4 + x^3 + \frac{1}{6}x^2 - \frac{1}{2}x - \frac{2}{3}$$

è irriducibile in $\mathbb{Q}[x]$. Innanzi tutto riportiamoci ad un polinomio intero primitivo: si ha $f = \frac{1}{6}g$ con $g = 4x^4 + 6x^3 + x^2 - 3x - 4$. Ora, 3 non divide il coefficiente direttivo di g e, riducendo modulo 3 si considera

$$\overline{g} = \overline{4}x^4 + \overline{6}x^3 + \overline{1}x^2 - \overline{3}x - \overline{4} = x^4 + x^2 - \overline{1}\ .$$

Proviamo che $\overline{g}$ è irriducibile on $\mathbb{Z}_3[x]$. Innanzi tutto, $\overline{g}(\overline{0}) = -\overline{1},\ \overline{g}(\overline{1}) = \overline{1}$ e $\overline{g}(\overline{2}) = \overline{1}$, quindi $\overline{g}$ non ha radici in $\mathbb{Z}_3[x]$ e dunque (essendo $\mathbb{Z}_3$ un campo) non ha fattori di grado 1 in $\mathbb{Z}_3[x]$. Supponiamo che $\overline{g}$ sia il prodotto di due fattori (monici) di grado 2:

$$x^4 + x^2 - \overline{1} = \overline{g} = (x^2 + ax + b)(x^2 + cx + d)$$

con $a, b, c, d \in \mathbb{Z}_3$. Dal confronto tra i coefficienti di grado 0 risulta $bd = -\overline{1} = \overline{2}$, quindi (a meno di scambiare i due polinomi) possiamo supporre $b = \overline{1}$ e $d = \overline{2}$ ottenendo

$$\overline{g} = (x^2 + ax + \overline{1})(x^2 + cx + \overline{2})$$

il cui confronto dei coefficienti di grado 1,2 e 3 dà: $2a + c = \overline{0},\ ac = \overline{1}\ a + c = \overline{0},$ condizioni che non sono soddisfatte da alcuna coppia $a, c \in \mathbb{Z}_3$.
Quindi $\overline{g}$ è irriducibile in $\mathbb{Z}_3[x]$ e dunque per il Criterio 1, g è irriducibile in $\mathbb{Z}[x]$. Per la Proposizione 9.15, f è irriducibile in $\mathbb{Q}[x]$.

Osserviamo che l'implicazione del Criterio 1 non si inverte; ad esempio $x^2 + 1$ è irriducibile in $\mathbb{Z}[x]$ mentre la sua riduzione modulo 5 è riducibile in $\mathbb{Z}_5[x]$: $x^2 + \overline{1} = (x + \overline{2})(x + \overline{3})$. Anzi esistono polinomi monici irriducibili in $\mathbb{Z}[x]$ la cui riduzione modulo qualunque primo è riducibile.

Un famoso e utile criterio di irriducibilità, sul quale ci soffermeremo un po' più a lungo è il criterio di Eisenstein.

Criterio di Eisenstein. *Sia $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ e supponiamo che esista un primo p tale che*

(i) p non divide a_n
(ii) p divide $a_0,\ a_1,\ \ldots,\ a_{n-1}$
(iii) p^2 non divide a_0

allora f è irriducibile in $\mathbb{Q}[x]$ e, se è primitivo, f è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Supponiamo che f sia primitivo. Supponiamo per assurdo che $f = gh$ con $g = b_mx^m + \ldots + b_0$ e $h = c_{n-m}x^{n-m} + \ldots + c_0$ polinomi interi di grado positivo. Consideriamo quindi la riduzione modulo p di f; per le condizioni (i) e (ii) si ha

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n}x^n. \tag{9.3}$$

Poiché $\mathbb{Z}_p[x]$ è un dominio a fattorizzazione unica, e x è un suo elemento irriducibile, i divisori propri di $\overline{a_n}x^n$ sono tutti del tipo $\overline{c}x^k$ con $0 \neq \overline{c} \in \mathbb{Z}_p$ e $0 \leq k \leq n$; si deduce quindi da (9.3) che , $\overline{g} = \overline{b_m}x^m$ e $\overline{h} = \overline{c_{n-m}}x^{n-m}$. In particolare si trova $\overline{b_0} = \overline{c_0} = \overline{0}$, il che implica $p|b_0$ e $p|c_0$. Ma allora $p^2|b_0c_0 = a_0$ contro la condizione (iii).
Se f non è primitivo si considera $f = df_0$ con $d \in \mathbb{Z}$ e f_0 primitivo e si osserva che, per la condizione (i), p non divide d e dunque si può applicare il criterio al polinomio primitivo f_0. ∎

Prima di vederne delle applicazioni, facciamo un'utile osservazione generale, riguardante quello che è volgarmente chiamato "cambiamento di variabile". Sia R un anello commutativo, e $a, b \in R$ con $a \neq 0$. Il principio di sostituzione assicura che esiste un unico omomorfismo $\nu : R[x] \to R[x]$ che fissa gli elementi di R e manda x in $ax + b$; quello che di solito si intende rappresentare con $f(x) \mapsto f(ax+b)$. Se assumiamo che a sia invertibile in R, l'omomorfismo ν di prima ha un inverso, dato dall'unico omomorfismo di $R[x]$ in sè tale che $x \mapsto a^{-1}x - a^{-1}b$. Dunque, se a è invertibile, l'applicazione ν (che, dal punto di vista pratico, è la sostituzione di x con $ax + b$) è un isomorfismo, e quindi *un automorfismo* di $R[x]$. In particolare ne segue l'utile constatazione che: *se F è un campo, e $a, b \in F$ con $a \neq 0$, allora $f(x) \in F[x]$ è irriducibile se e soltanto se $f(ax + b)$ è irriducibile.*

L'esempio che diamo ora di applicazione del Criterio di Eisenstein è sufficientemente importante da essere enunciato come una Proposizione.

Proposizione 9.18. *Sia p un numero primo. Allora il polinomio*

$$x^{p-1} + x^{p-2} + \ \dots \ + x^2 + x + 1$$

è irriducibile in $\mathbb{Q}[x]$.

Dimostrazione. Sia $f = x^{p-1} + \ \dots \ + x + 1$. Poniamo $y = x + 1$ e scriviamo $f(y) = (x+1)^{p-1} + \ \dots \ + (x+1) + 1$. Per quanto osservato prima, f è irriducibile se e solo se $f(y)$ è irriducibile. Si ha

$$\begin{array}{rl} xf(y) & = (y-1)(y^{p-1} + \ldots + y + 1) = y^p - 1 = (x+1)^p - 1 = \\ & = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \ldots \ + \binom{p}{p-1}x + 1 - 1 \\ & = x(x^{p-1} + \binom{p}{1}x^{p-2} + \ldots \ + \binom{p}{p-2}x + p) \end{array} .$$

Ora, sappiamo che, per ogni $1 \leq i \leq p-1$, p divide $\binom{p}{i}$. Quindi, per il Criterio di Eisenstein,

$$f(y) = x^{p-1} + \binom{p}{1}x^{p-2} + \ \dots \ + \binom{p}{p-2}x + p$$

è irriducibile, e dunque f è irriduciblile. ∎

Se p è un primo il polinomio $\Phi_p = x^{p-1} + x^{p-2} + \ \dots \ + x + 1$ si chiama *polinomio ciclotomico p-esimo*, e poichè $(x-1)\Phi_p = x^p - 1$, le sue radici complesse sono le radici p-esime dell'unità diverse da 1.

Fattorizzazioni in $\mathbb{R}[x]$ e $\mathbb{C}[x]$. Completiamo questa sezione illustrando rapidamente la situazione per quanto riguarda i polinomi irriducibili in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$. Una delle proprietà fondamentali dell'anello dei numeri complessi è che esso contiene radici di ogni polinomio non costante. L'enunciato di questo fatto viene tradizionalmente chiamato **Teorema fondamentale dell'Algebra** (anche se tale denominazione appare oggi non del tutto giustificata). La sua dimostrazione è in genere fatta usando strumenti del corso di Analisi, e quindi la omettiamo.

Definizione. Un campo F si dice **algebricamente chiuso** se ogni polinomio di grado maggiore o uguale a 1 in $F[x]$ ammette almeno una radice in F.

Teorema 9.19. *Il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso.*

Dalla definizione seguono immediatamente le seguenti proprietà, che valgono in particolare per il campo $\mathbb{C}$. La dimostrazione è lasciata per esercizio.

Proposizione 9.20. *Sia F un campo algebricamente chiuso. Allora*

- **(1)** *I polinomi irriducibili di $F[x]$ sono tutti e soli i polinomi di grado 1.*
- **(2)** *Ogni polinomio $f \in F[x]$ con $\deg f = n \geq 1$ si decompone in $F[x]$ come $f = a(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ con $a, \alpha_1, \alpha_2, \ldots, \alpha_n$ elementi di F.*

Vediamo ora cosa si può dire per il campo dei numeri reali $\mathbb{R}$.
Sia $f = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio a coefficienti in $\mathbb{R}$ e grado $n \geq 1$. Sia $\alpha \in \mathbb{C}$ una radice (complessa) di f. Ricordando che il coniugio in $\mathbb{C}$ è un isomorfismo che manda ogni numero reale in se stesso, si ha

$$0 = \overline{a_0 + a_1\alpha + \ldots + a_n\alpha^n} = \overline{a_0} + \overline{a_1\alpha} + \ldots + \overline{a_n\alpha}^n == a_0 + a_1\overline{\alpha} + \ldots + a_n\overline{\alpha}^n = f(\overline{\alpha}).$$

Quindi, abbiamo provato il seguente fatto:

Lemma 9.21. *Se α è una radice complessa del polinomio $f \in \mathbb{R}[x]$ allora anche il suo coniugato $\overline{\alpha}$ è una radice di f.*

Proposizione 9.22. *Gli elementi irriducibili di $\mathbb{R}[x]$ sono*

(i) *I polinomi di grado 1.*

(ii) *I polinomi $ax^2 + bx + c$ con $a \neq 0$ e $b^2 - 4ac < 0$.*

Dimostrazione. Chiaramente ogni polinomio di grado 1 è irriducibile (questo vale per coefficienti in qualsiasi campo). Sia quindi $f \in \mathbb{R}[x]$ un polinomio irriducibile di grado almeno 2. Allora f non ha radici in $\mathbb{R}$ (altrimenti, per il Teorema di Ruffini, avrebbe un fattore di grado 1). Sia α una radice in $\mathbb{C}$ di f, allora $\alpha \in \mathbb{C} \setminus \mathbb{R}$ e quindi $\alpha \neq \overline{\alpha}$. Per il Lemma 9.21, $\overline{\alpha}$ è una radice di f e quindi, per il Teorema di Ruffini, $g = (x - \alpha)(x - \overline{\alpha})$ divide f in $\mathbb{C}[x]$, cioè $f = gh$ con $h \in \mathbb{C}[x]$. Ora, se $\alpha = u + iv$ con $u, v \in R$:

$$g = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2ux + (u^2 + v^2) \in \mathbb{R}[x] \ .$$

Allora, se $f = gq + r$ è la divisione di f per g in $\mathbb{R}[x]$, essa è anche la divisione di f per g in $\mathbb{C}[x]$. Ma, in $\mathbb{C}[x]$, $f = gh$. Per l'unicità della divisione, deve essere $r = 0$ e $h = q \in \mathbb{R}[x]$. Quindi $g|f$ in $\mathbb{R}[x]$. Poichè f è irriducibile, deve essere $f = ag$ per $a \in \mathbb{R}$ (a non è altro che il coefficiente direttivo di f), in particolare $\deg f = 2$.

Infine, sia $f = ax^2 + bx + c$ un polinomio di grado 2 in $\mathbb{R}[x]$. Allora, f è irriducibile se e soltanto se non ha fattori di grado 1, ovvero se e soltanto se non ha radici in $\mathbb{R}$, ed è ben noto che questa condizione equivale all'essere $b^2 - 4ac < 0$. ∎

Da questa proposizione segue che ogni polinomio in $\mathbb{R}[x] \setminus \mathbb{R}$ si fattorizza in $\mathbb{R}[x]$ come il prodotto di polinomi di grado 1 o 2. In particolare, ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha almeno un fattore di grado 1, quindi ha almeno una radice reale. Questo fatto si può dimostrare senza ricorrere alla chiusura algebrica di $\mathbb{C}$. Infatti sia $f \in \mathbb{R}[x]$; denotiamo con $f(x)$ la funzione reale associata ad f, cioè

$$\begin{array}{rccc} f(x): & \mathbb{R} & \to & \mathbb{R} \\ & a & \mapsto & f(a) \end{array}$$

$f(x)$ è una funzione continua. Se f ha grado dispari allora

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

quindi il grafico di $f(x)$ interseca l'asse delle x, e dunque esiste $a \in \mathbb{R}$ tale che $f(a) = 0$.

Esercizio 9.21. Senza usare il Teorema 9.16 si provi che ogni irriducibile di $\mathbb{Z}[x]$ è primo.

Esercizio 9.22. Si fattorizzi il polinomio $2x^4 - x^3 + 6x^2 + 7x - 5$ in $\mathbb{Z}[x]$.

Esercizio 9.23. 1) Si fattorizzi $x^4 + 3x + 2$ in $\mathbb{Q}[x]$.

2) Siano p, q primi positivi. Si provi che, escluso il caso $p = 2$, $q = 3$, il polinomio $x^4 + qx + p$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 9.24. Si provi che per ogni primo p dispari il polinomio $x^p + px + 1$ è irriducibile in $\mathbb{Q}[x]$. [sugg.: si faccia la sostituzione $x = y - 1$.]

9.5 Esercizi.

Esercizio 9.25. Sia A una anello commutativo. Sia I_* un ideale di $A[x]$.

(1) Si provi che l'insieme dei termini noti dei polinomi in I_* costituisce un ideale di A. Viceversa, sia I è un ideale di A; si provi che l'insieme dei polinomi in $A[x]$ il cui termine noto appartiene ad I è un ideale di $A[x]$.

(2) Si provi che l'insieme dei coefficienti direttori dei polinomi in I_* costituisce un ideale di A. Si dice se è vero che, se I è un ideale di A, allora l'insieme dei polinomi in $A[x]$ il cui coefficiente direttore appartiene ad I è un ideale di $A[x]$.

Esercizio 9.26. Sia $Y = \{a_0 + a_1x^2 + a_2x^4 ... + a_nx^{2n} \mid n \in \mathbb{N}, a_i \in \mathbb{Q}\}$. Si provi che Y è un sottoanello ma non è un ideale di $\mathbb{Q}[x]$.

Esercizio 9.27. Sia R un anello commutativo e sia $f \in R[x]$. Si provi che se f è un divisore dello zero in $R[x]$ allora esiste $b \in R$ tale che $bf = 0$. [sugg.: fare induzione su $\deg f$]

Esercizio 9.28. Siano $f = x^4 - x^3 - 4x^2 + 4x$ e $h = x^2 - a$ polinomi a coefficienti in $\mathbb{Q}$. Si determini per quali valori $a \in \mathbb{Q}$ si ha $(h, f) = 1$.

Esercizio 9.29. Si provi che il polinomio $x^3 - 4$ è irriducibile in $\mathbb{Q}[x]$, mentre ammette radici in ciascuno dei campi $\mathbb{Z}_p$ con $p = 3, 5, 7, 11$.

Esercizio 9.30. In $\mathbb{Q}[x]$ si considerino i polinomi

$$f = x^4 + 3x^3 + 2x^2 + x + 6 \qquad g = x^3 + x^2 + 2x + 3 \ .$$

Si determini un massimo comun divisore di f e g in $\mathbb{Q}[x]$.
Sia considerino poi le riduzioni modulo 7, $\overline{f}$, $\overline{g}$, di f e di g; se ne determini un massimo comun divisore in $\mathbb{Z}_7[x]$ (si confronti il risultato con il caso dei razionali).

Esercizio 9.31. Sia A un dominio d'integrità e sia $0 \neq f \in A[x]$. Si provi che il numero di radici distinte di f in A è al più $\deg f$.

Esercizio 9.32. Siano $c = \sqrt{5}$, $d = (\sqrt{5})^{-1}$. Denotiamo con σ_c, σ_d rispettivamente gli automorfismi di sostituzione da $\mathbb{Q}[x]$ in $\mathbb{R}$, definiti da, per ogni $f \in \mathbb{Q}[x]$:

$$\sigma_c(f) = f(c) \qquad\qquad \sigma_d(f) = f(d) \ .$$

(a) σ_c è iniettivo ?

(b) $d \in Im(\sigma_c)$?

(c) $Im(\sigma_c) \cap Im(\sigma_d)$ è finito o infinito ?

Esercizio 9.33. Sia p un numero primo, con $p \not\equiv 1 \pmod 3$. Si provi che il polinomio $x^2 + x + 1$ è irriducibile in $\mathbb{Z}_p[x]$.

Esercizio 9.34. Sia $f = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Q}[x]$. Definiamo il *polinomio derivato* di f, come

$$f' = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1$$

(a) Si dimostri che per ogni $f, g \in \mathbb{Q}[x]$ si ha $(fg)' = f'g + fg'$.

(b) Sia $b \in \mathbb{Q}$; si provi che b è radice comune di f e di f' se e solo se $(x-b)^2$ divide f (in questo caso si dice che b è una radice multipla di f).

Esercizio 9.35. Provare che se f è un polinomio irriducibile in $\mathbb{Q}[x]$ allora f non ha radici multiple in $\mathbb{C}$.

Esercizio 9.36. Sia R un anello commutativo, e x, y due distinte indeterminate. Si enunci e dimostri un principio di sostituzione "in due variabili" per $R[x, y]$, analogo al Teorema 9.3. [Nella dimostrazione potete applicare 9.3]

Esercizio 9.37. Sia R un anello commutativo. Si provi che

$$\{f \in R[x, y] \mid f(a, b) = f(b, a) \text{ per ogni } a, b \in R\}$$

è un sottoanello ma non un ideale di $R[x, y]$.

Esercizio 9.38. Sia F un campo. Nell'anello $F[x, y]$ si consideri l'ideale (x, y). Si provi che $(x, y) = \{f \in F[x, y] \mid f(0, 0) = 0\}$, e che (x, y) non è principale. Si provi quindi che $S = \{f \in F[x, y] \mid f(a, a) = 0 \text{ per ogni } a \in F\}$ è un ideale è principale di $F[x, y]$.

Esercizio 9.39. In $\mathbb{Q}[x]$ si trovi un generatore del seguente ideale

$$(x^7 + 2x^4 + x^3 + x + 3,\ x^4 + 1)\ .$$

Esercizio 9.40. Siano $f, g \in \mathbb{Q}[x]$ polinomi non nulli. Sia d un MCD di f, g in $\mathbb{Q}[x]$. Si provi che d è un MCD di f, g in $\mathbb{R}[x]$.

Esercizio 9.41. Si fattorizzino i polinomi $x^9 - x$ e $x^5 - 2x^3 - x^2 + 2$ in irriducibili in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$.

Esercizio 9.42. Siano $a, b \in \mathbb{Q}$ (fissati), e si consideri l'applicazione $\Phi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}$ definita da $\Phi(f) = (f(a), f(b))$ per ogni $f \in \mathbb{Q}[x]$.

(a) Si provi che Φ è un omomorfismo d'anelli.

(b) Si determini $Ker(\Phi)$ (trovandone un generatore).

(c) Si provi che $\{a_0 + a_1x + a_2x^2 + \ldots \in \mathbb{Q}[x] \mid a_0 + a_2 + \ldots = 0 = a_1 + a_3 + \ldots\}$ è un ideale di $\mathbb{Q}[x]$ e si trovi un suo generatore.

Esercizio 9.43. Si dica quali fra i seguenti polinomi sono irriducibili in $\mathbb{Q}[\sqrt{2}][x]$:

$$x^2 - 2,\quad x^2 + 2,\quad x^2 - 4x + 2,\quad x^3 - 2,\quad x^4 + 1.$$

Esercizio 9.44. Siano $f, g \in \mathbb{Z}[x]$ polinomi monici. Si provi che il massimo comun divisore di f e g in $\mathbb{Q}[x]$ ha coefficienti interi.

Esercizio 9.45. Si provi che le condizioni su un campo F descritte dai punti (1) e (2) della Proposizione 9.20 sono entrambe equivalenti ad affermare che F è algebricamente chiuso.

Esercizio 9.46. Si fattorizzi in prodotto di irriducibili i seguenti polinomi:

1) $x^4 - x^2 - 2 \in K[x]$, con $K = \mathbb{Z}/2\mathbb{Z}$, e $K = \mathbb{Q}$.

2) $x^4 + 1 \in K[x]$, con $K = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}$ e $\mathbb{Z}/2\mathbb{Z}$.

3) $f = x^5 - 2x^4 + x^3 - 9x^2 + 18x - 9$ in $\mathbb{Q}[x]$.

4) $x^5 - 1$ in $\mathbb{Z}_p[x]$, con $p = 3,\ 5,\ 11$.

Esercizio 9.47. Si determini per quali valori $h \in \mathbb{Z}$ il polinomio $f_h = x^4 - x^2 + hx + 1$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 9.48. (Funzioni polinomiali, I) Sia F un campo. L'anello F^F di tutte le funzioni da F in F è definito analogamente a quanto abbiamo visto per $\mathbb{R}^\mathbb{R}$ nella sezione 6.1 (vedi anche l'Esercizio 6.27). Ad ogni polinomio $f \in F[x]$ è associata una *funzione polinomiale* $f^* \in F^F$, definita mediante sostituzione, ovvero si pone $f^*(a) = f(a)$ per ogni $a \in F$ (si osservi che, se $f = a_0 + a_1 x + \ldots + a_n$ allora, denotando con ι l'applicazione identica su F, si ha, nell'anello F^F, $f^* = a_0 + a_1\iota + \ldots + a_n\iota^n$). Definiamo quindi l'applicazione $\Phi : F[x] \to F^F$, ponendo $\Phi(f) = f^*$, per ogni $f \in F$. L'immagine di Φ si chiama insieme delle *funzioni polinomiali* di F.
Si provi che Φ è un omomorfismo d'anelli. Si provi quindi che se F *è infinito*, allora Φ è iniettiva. [applicare la conseguenza del teorema di Ruffini]
Sia quindi p un numero primo e $F = \mathbb{Z}_p$. In questo caso, $\Phi : F[x] \to F^F$ non può essere iniettiva (dato che F^F è finito mentre $F[x]$ è comunque infinito); si provi che

$$\ker \Phi = (x^p - x).$$

[applicare il Teorema di Fermat per una inclusione, Ruffini e il Teorema 9.5 per l'altra]

Esercizio 9.49. (Funzioni polinomiali, II) Siano $F = \mathbb{Z}_p$ e Φ come nell'esercizio precedente, e sia $X = \{f \in F[x] \mid f = 0 \text{ o } \deg f \leq p - 1\}$.

(1) Si provi che la restrizione di Φ a X è iniettiva. [Ruffini]

(2) Si provi che ogni funzione di F in sé è polinomiale. [contare].

(Quanto negli ultimi due esercizi vale in generale per un campo F di ordine finito)

Esercizio 9.50. (Funzioni polinomiali, III) Sia F un campo. Il concetto di funzione polinomiale si estende nel modo naturale a polinomi in più indeterminate. Si consideri, ad esempio, il caso di due indeterminate x, y; si definisca una applicazione $\Phi_2 : F[x, y] \to F^{F \times F}$, analoga alla Φ degli esercizi precedenti; si provi che è un omomorfismo d'anelli e che è iniettiva se e solo se F è infinito.

Capitolo 10

Quozienti

10.1 Anelli quoziente.

In questa sezione, la costruzione degli anelli del tipo $\mathbb{Z}/n\mathbb{Z}$ verrà estesa ad un anello generico R (non necessariamente commutativo) e qualunque suo ideale proprio I.

Sia dunque I un ideale proprio dell'anello R (cioè I è un ideale e $I \neq R$). Per ogni $a \in R$ si definisce la **classe laterale** (modulo l'ideale I) di rappresentante a,

$$a + I = \{\ a + x \mid x \in I\ \}.$$

Si tratta quindi di un sottoinsieme non vuoto di R (dato che $a = a + 0_r \in a + I$). Si pone quindi

$$R/I = \{\ a + I \mid a \in R\ \}$$

l'insieme di tutte la classi laterali distinte modulo I.

Ora, fissato l'ideale I, è sempre possibile definire una equivalenza $\sim_I$ su R, in modo tale che le classi laterali modulo I coincidono con le classi di equivalenza modulo $\sim_I$. Precisamente, per ogni $x, y \in R$, si pone

$$x \sim_I y \quad \Leftrightarrow \quad x - y \in I.$$

Innanzi tutto, verifichiamo che $\sim_I$ è una equivalenza su R. Come si vedrà, quasto fatto dipende essenzialmente dalle proprietà additive degli ideali. Per ogni $a \in R$, $a - a = 0_R \in I$, quindi $a \sim_I a$, e pertanto $\sim_I$ è riflessiva. Siano $a, a \in R$ con $a \sim_I b$; allora $a - b \in I$, dunque $b - a = -(a - b) \in I$, cioè $b \sim_I a$, provando che $\sim_I$ è simmetrica. Infine, se $a, b, c \in R$ sono tali che $a \sim_I b$ e $b \sim_I c$, allora $a - b \in$ e $b - c \in I$, da cui segue $a - c = (a - b) + (b - c) \in I$, e quindi $a \sim_I c$. Pertanto $\sim_I$ è anche transitiva, e dunque è una relazione di equivalenza.
Ora, dato $a \in R$, la classe di equivalenza di a modulo $\sim_I$ è costituita da *tutti gli elementi $b \in R$ tali che la differenza $x = b - a$ appartiene all'ideale I*; si tratta cioè di tutti i $b \in R$ che si possono scrivere nella forma $b = a + x$ con $x \in I$. Dunque, la

classe di equivalenza di a modulo $\sim_I$ coincide con la classe laterale $a+I$, come definita all'inizio della sezione.

Dalla teoria generale delle relazioni d'equivalenza, segue che le classi laterali modulo l'ideale I costituiscono una partizione di R, in particolare esse sono a due a due disgiunte, ed il loro insieme R/I è l'insieme quoziente $R/\sim_I$. Ancora, evidenziamo il seguente elementare ma importante fatto.

Lemma 10.1. *Sia I un ideale proprio dell'anello R, e siano $a, b \in R$. Allora*

$$a + I = b + I \quad \Leftrightarrow \quad a - b \in I.$$

Ora, nell'insieme quoziente R/I definiamo un'operazione di somma, ed un'operazione di prodotto, ponendo, per ogni $a+I, b+I \in R/I$,

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

dove le operazioni tra i rappresentanti a e b delle due classi sono quelle nell'anello R.

Prima di fare ogni ulteriore osservazione, è indispensabile stabilire che quelle date sopra sono **buone** definizioni, che effettivamente determinano operazioni sull'insieme quoziente. Occorre cioè provare che il risultato (come classe laterale) non dipende dalla scelta dei due particolari rappresentanti a e b ma solo dalle loro classi $a + I$ e $b + I$. Siano dunque a' e b' elementi di R tali che

$$\begin{cases} a + I = a' + I \\ b + I = b' + I \end{cases}$$

Allora $a - a' \in I$ e $b - b' \in I$. Poiché I è un ideale, si ha allora

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

e dunque $(a + b) + I = (a' + b') + I$, mostrando che la somma è ben definita.
Tenendo anche conto delle proprietà di assorbimento di I, si ha inoltre

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$$

(dato che $(a - a')b \in I$ e $a'(b - b') \in I$). Dunque $ab + I = a'b' + I$, provando che il prodotto su R/I è ben definito.

A questo punto, si verifica facilmente che, rispetto a tali operazioni di somma e prodotto R/I è un anello che si chiama **anello quoziente** di R modulo I. In tale anello

- $0_{R/I} = 0_R + I = I$;
- per ogni $a + I \in R/I$, $-(a + I) = (-a) + I$;
- $1_{R/I} = 1_R + I$ (la condizione che I sia un ideale proprio serve ad evitare che R/I sia degenere);

Ad esempio, per $n \geq 2$, l'anello delle classi resto $\mathbb{Z}/n\mathbb{Z}$ è proprio l'anello quoziente di $\mathbb{Z}$ modulo l'ideale $n\mathbb{Z}$.

Osservazione. Avremmo anche potuto, come abbiamo fatto per gli anelli $\mathbb{Z}/n\mathbb{Z}$, definire le operazioni di somma e prodotto di due classi laterali intendendo, rispettivamente, le loro somma e prodotto come sottoinsiemi di R. Questo avrebbe condotto al medesimo risultato. Tuttavia, l'approccio mediante la relazione d'equivalenza associata all'ideale, è più astratto ma anche più generale, e trova corrispettivi in diverse altre categorie di strutture algebriche.

Esempio. Consideriamo l'anello $\mathbb{R}^{\mathbb{R}}$ di tutte le applicazioni $f : \mathbb{R} \to \mathbb{R}$. Si verifica facilmente che l'insieme

$$I = \{ f \in \mathbb{R}^{\mathbb{R}} \mid f(0) = 0 \}$$

è un ideale di $\mathbb{R}^{\mathbb{R}}$ (vedi sezione 6.3). È quindi possibile costruire l'anello quoziente $\mathbb{R}^{\mathbb{R}}/I$, i cui elementi sono le classi laterali $f + I$, al variare di $f \in \mathbb{R}^{\mathbb{R}}$. Osserviamo che $f + I = g + I$ se e soltanto se $f - g \in I$, ovvero $0 = (f - g)(0) = f(0) - g(0)$, cioè se e solo se $f(0) = g(0)$. Per ogni $r \in \mathbb{R}$, denotiamo con C_r la funzione costante definita da $C_r(x) = r$ per ogni $x \in \mathbb{R}$. Da quanto osservato sopra, segue in particolare che, dati $r, s \in \mathbb{R}$

$$C_r + I = C_s + I \quad \Leftrightarrow \quad r = s,$$

e quindi che, al variare di $r \in \mathbb{R}$, le classi laterali $C_r + I$ sono tutte distinte. Ancora, se $f \in \mathbb{R}^{\mathbb{R}}$, allora $C_{f(0)}(0) = f(0)$, e dunque $C_{f(0)} + I = f + I$. In conclusione,

$$\frac{\mathbb{R}^{\mathbb{R}}}{I} = \{ C_r + I \mid r \in \mathbb{R} \},$$

e le classi $C_r + I$ sono tutte distinte (questo si esprime dicendo che l'insieme $\{C_r \mid r \in \mathbb{R}\}$ è un sistema completo di rappresentanti delle classi laterali di $\mathbb{R}^{\mathbb{R}}$ modulo I).
Inoltre, proprio per come sono definite le operazioni nel quoziente $\mathbb{R}^{\mathbb{R}}/I$, si può facilmente verificare che l'applicazione $\Psi : \mathbb{R} \longrightarrow \mathbb{R}^{\mathbb{R}}/I$, definita da $\Psi(r) = C_r + I$ per ogni $r \in \mathbb{R}$, è un isomorfismo d'anelli. Quest'ultimo fatto non è un caso, ed il motivo verrà chiarito nella sezione che segue.

Come c'è da aspettarsi, e come vedremo anche nelle prossime sezioni, vi sono forti legami tra le proprietà di un ideale e quelle del suo corrispondente anello quoziente. Il seguente è un primo rilevante esempio di ciò.

Teorema 10.2. *Sia R un anello commutativo, ed I un ideale di R. Allora I è un ideale primo se e solo se l'anello quoziente R/I è un dominio d'integrità.*

Dimostrazione. ($\Rightarrow$) Sia I un ideale primo dell'anello commutativo R (quindi R/I è non degenere, dato che $I \neq R$). Siano $a + I$ e $b + I$ elementi di R/I tali che

$$ab + I = (a + I)(b + I) = 0_{r/I} = I.$$

Allora $ab \in I$ e, poiché I è un ideale primo, si ha $a \in I$ oppure $b \in I$. Nel primo caso $a + I = I = 0_{R/I}$; altrimenti $b + I = I = 0_{R/I}$. Dunque R/I è un dominio d'integrità.

($\Leftarrow$) Sia R/I un dominio d'integrità, e siano $a, b \in R$ tali che $ab \in I$. Allora,

$$0_{R/I} = I = ab + I = (a + I)(b + I).$$

Poiché R/I è un dominio d'integrità, si ha allora $a + I = 0_{R/I}$, oppure $b + I = 0_{R/I}$. Nel primo caso $a \in I$, e nel secondo, $b \in I$. Dunque I è un ideale primo di R. ■

Esercizio 10.1. Sia R un anello commutativo, sia a un elemento nilpotente di R e sia $J = (a)$ l'ideale generato da a. Sia $b \in R$ tale che $b + J$ è un elemento nilpotente dell'anello quoziente R/J. Si provi che b è un elemento nilpotente di R.

Esercizio 10.2. Sia A un dominio di integrità e sia I un ideale di A tale che A/I è isomorfo a $\mathbb{Z}/p\mathbb{Z}$, con p un numero primo. Si dimostri che $char(A) \in \{0, p\}$.

Esercizio 10.3. Si provi che l'anello quoziente $\mathbb{Q}[x]/(x^2)$ non è un dominio d'integrità. Si provi che l'anello $\mathbb{Q}[x]/(x + 1)$ è isomorfo a $\mathbb{Q}$.

Esercizio 10.4. Sia F un campo e sia $0 \neq f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in F[x]$. Si provi che la classe laterale $x + (f)$ è un elemento invertibile di $F[x]/(f)$ se e solo se $a_0 \neq 0$.

10.2 Quozienti e omomorfismi.

Sia $\phi : R \to S$ un omomorfismo d'anelli. Abbiamo dimostrato in precedenza (Teorema 6.16) che il nucleo $\ker(\phi) = \{a \in R \mid \phi(a) = 0_S\}$ è un ideale di R.

Viceversa, sia I un ideale dell'anello R. Si verifica facilmente che la *proiezione canonica*

$$\begin{array}{rccc} \pi : & R & \to & R/I \\ & a & \mapsto & a + I \end{array}$$

è un omomorfismo suriettivo di anelli. Inoltre, $\ker(\pi) = I$; infatti, tenendo conto del Lemma 10.1,

$$\ker(\pi) = \{a \in R \mid \pi(a) = 0_{R/I}\} = \{a \in R \mid a + I = I\} = \{a \in R \mid a \in I\} = I.$$

Quindi abbiamo provato la seguente fondamentale fatto.

Proposizione 10.3. *Un sottoinsieme di un anello è un ideale se e solo se è il nucleo di qualche omomorfismo dell'anello.*

Proviamo ora un teorema fondamentale riguardante omomorfismi e quozienti, che ha un corrispettivo in diverse altre strutture algebriche.

Teorema 10.4 (di omomorfismo)**.** *Sia $\phi : R \to S$ un omomorfismo di anelli. Siano $I = \ker(\phi)$ il suo nucleo, e π la proiezione canonica di R su R/I. Allora esiste un unico omomorfismo $\overline{\phi} : R/I \to S$ tale che $\overline{\phi} \circ \pi = \phi$; inoltre $\overline{\phi}$ è iniettivo e $Im(\overline{\phi}) = Im(\phi)$.*

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo di anelli, e $I = \ker(\phi)$. Definiamo un'applicazione $\overline{\phi} : R/I \to S$ ponendo, per ogni $a + I \in R/I$,

$$\overline{\phi}(a + I) = \phi(a).$$

Verifichiamo, innanzi tutto, che questa è una buona definizione. Siano $a, a' \in R$ tali che $a + I = a' + I$; allora $a - a' \in I = \ker(\phi)$, e quindi

$$0_S = \phi(a - a') = \phi(a) - \phi(a'),$$

da cui segue $\phi(a) = \phi(a')$, ovvero (come deve essere) $\overline{\phi}(a + I) = \overline{\phi}(a' + I)$.

Proviamo ora che $\overline{\phi}$ è un omomorfismo di anelli; ciò dipende dal fatto che tale è ϕ. Siano $a + I, b + I \in R/I$; allora

$$\begin{aligned} \overline{\phi}((a + I) + (b + I)) &= \overline{\phi}(a + b + I) = \phi(a + b) = \phi(a) + \phi(b) = \overline{\phi}(a + I) + \overline{\phi}(b + I) \\ \overline{\phi}((a + I)(b + I)) &= \overline{\phi}(ab + I) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(a + I)\overline{\phi}(b + I) \end{aligned}$$

ed inoltre

$$\overline{\phi}(1_{R/I}) = \overline{\phi}(1_R + I) = \phi(1_R) = 1_S.$$

Dunque $\overline{\phi}$ è un omomorfismo. Per dimostrarne l'iniettività è ora sufficiente provare che il suo nucleo è banale.

$$\begin{aligned} \ker(\overline{\phi}) &= \{a + I \in R/I \mid \overline{\phi}(a + I) = 0_S\} = \{a + I \in R/I \mid \phi(a) = 0_S\} \\ &= \{a + I \in R/I \mid a \in I\} = \{I\} = \{0_{R/I}\} \end{aligned}$$

dunque $\overline{\phi}$ è iniettivo. Il fatto che $Im(\overline{\phi}) = Im(\phi)$ è chiaro dalla definizione di $\overline{\phi}$. Infine, per ogni $a \in R$,

$$\overline{\phi} \circ \pi(a) = \overline{\phi}(\pi(a)) = \overline{\phi}(a + I) = \phi(a)$$

e dunque $\overline{\phi} \circ \pi = \phi$, completando così la dimostrazione. ∎

Una conseguenza immediata ma molto importante è il seguente

Corollario 10.5. *Sia $\phi : R \to S$ un omomorfismo di anelli. Allora*

$$R/\ker(\phi) \simeq Im(\phi);$$

in particolare, se ϕ è suriettivo allora $R/\ker(\phi) \simeq S$.

Esempio. Rivediamo alla luce di questo corollario l'ultima osservazione dell'esempio alla fine della sezione precedente. Definiamo $\phi : \mathbb{R}^{\mathbb{R}} \longrightarrow \mathbb{R}$, ponendo, per ogni $f \in \mathbb{R}^{\mathbb{R}}$, $\phi(f) = f(0)$. Allora, come si verifica facilmente, ϕ è un omomorfismo suriettivo di anelli, ed il nucleo di ϕ è proprio l'ideale $I = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(0) = 0\}$ definito nell'esempio. Per il Corollario 10.5, si ha quindi che esiste un isomorfismo $\overline{\phi} : \mathbb{R}^{\mathbb{R}}/I \to \mathbb{R}$ (che è l'inverso dell'isomorfismo Ψ descritto nell'esempio).

Il prossimo Teorema prosegue nell'analisi degli anelli quoziente modulo il nucleo di un omomorfismo. Premettiamo un facile Lemma (vedi Esercizio 6.22).

Lemma 10.6. *Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli. Allora*

i) Se I è un ideale di R, $\phi(I)$ è un ideale di S.

ii) Se T è un ideale di S, la sua immagine inversa $\phi^{-1}(T)$ è un ideale di R che contiene $\ker(\phi)$.

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli.

i) Sia I un ideale di R Allora, $\phi(I) \neq \emptyset$ perchè $0_S = \phi(0_R) \in \phi(I)$; inoltre, se $x, y \in \phi(I)$, esistono $a, b \in I$ tali che $x = \phi(a)$, $y = \phi(b)$ e, poiché I è un ideale, $x - y = \phi(a) - \phi(b) = \phi(a - b) \in \phi(I)$. Infine sia $x = \phi(a) \in \phi(I)$ (con $a \in I$) e $s \in S$; poiché ϕ è suriettivo, esiste $r \in R$ tale che $s = \phi(r)$, quindi $xs = \phi(a)\phi(r) = \phi(ar) \in \phi(I)$ e similmente $sx \in \phi(I)$. Dunque $\phi(I)$ è un ideale di S.

ii) Sia T un ideale di S, e sia $M = \phi^{-1}(T)$ la sua immagine inversa rispetto a ϕ; proviamo che M è un ideale di R che contiene $\ker(\phi)$. Innanzi tutto, per ogni $a \in \ker(\phi)$ si ha $\phi(a) = 0_S \in T$, quindi $a \in \phi^{-1}(T) = M$, e dunque $\ker(\phi) \subseteq M$. Resta da provare che M è un ideale; siano $a, b \in M$ allora $\phi(a), \phi(b) \in T$ ed essendo T un ideale, $\phi(a - b) = \phi(a) - \phi(b) \in T$, e quindi $a - b \in \phi^{-1}(T) = M$; infine, se $a \in M$ e $r \in R$ allora $\phi(ar) = \phi(a)\phi(r) \in T$ perché $\phi(a) \in T$ e T è un ideale di S; quindi $ar \in M$ e similmente si prova che $ra \in M$. Dunque M è un ideale di R che contiene $\ker(\phi)$. ∎

Teorema 10.7 (di Corrispondenza)**.** *Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli e sia $I = \ker(\phi)$. Allora ϕ definisce una biezione tra l'insieme degli ideali di R che contengono I e l'insieme di tutti gli ideali di S.*

Dimostrazione. Sia $\phi : R \to S$ un omomorfismo suriettivo di anelli, e denotando con $\mathcal{A}$, $\mathcal{B}$ rispettivamente l'insieme degli ideali di R che contengono $I = \ker(\phi)$ e l'insieme di tutti gli ideali di S. Per il lemma precedente, possiamo dunque definire le seguenti applicazioni:

$$\begin{array}{rccc} \Phi: & \mathcal{A} & \to & \mathcal{B} \\ & K & \mapsto & \phi(K) \end{array}$$

$$\begin{array}{rccc} \Psi: & \mathcal{B} & \to & \mathcal{A} \\ & T & \mapsto & \phi^{-1}(T) \end{array}$$

Dimostriamo che Φ e Ψ sono una l'inversa dell'altra.
Sia pertanto $K \in \mathcal{A}$. Allora

$$(\Psi \circ \Phi)(K) = \Psi(\Phi(K)) = \Psi(\phi(K)) = \phi^{-1}(\phi(K)).$$

Ora, $K \subseteq \phi^{-1}(\phi(K))$ per definizione di immagine inversa. Viceversa, sia $a \in \phi^{-1}(\phi(K))$; allora $\phi(a) \in \phi(K)$, e dunque esiste $b \in K$ tale che $\phi(a) = \phi(b)$; da ciò segue che $\phi(a - b) = 0_S$, ovvero che $a - b \in \ker(\phi) \subseteq K$. Dunque $a - b = c \in K$, e pertanto $a = b + c \in K$, provando che $\phi^{-1}(\phi(K)) \subseteq K$. Quindi

$$K = \phi^{-1}(\phi(K)) = (\Psi \circ \Phi)(K).$$

Sia ora $T \in \mathcal{B}$. Allora, ancora per definizione di immagine inversa,

$$\phi(\phi^{-1}(T)) \subseteq T.$$

Viceversa, siccome ϕ è suriettivo, per ogni $t \in T$ esiste $a \in R$ tale che $\phi(a) = t$ (dunque $a \in \phi^{-1}(T)$); quindi $T \subseteq \phi(\phi^{-1}(T))$. Pertanto

$$(\Phi \circ \Psi)(T) = \phi(\phi^{-1}(T)) = T.$$

Dunque Φ e Ψ sono una l'inversa dell'altra. In particolare, esse sono biezioni, ed il teorema è dunque provato. ∎

Osserviamo che l'ipotesi che l'omomorfismo ϕ è suriettivo non è limitante; infatti l'immagine $Im(\phi)$ di un omomorfismo di anelli $\phi : A \to B$ è un anello, possiamo quindi applicare il teorema di corrispondenza, rimpiazzando B con $Im(\phi)$ (tenendo conto che, quindi, vanno considerati fli ideali di quest ultimo).

La prima fondamentale applicazione del Teorema di corrispondenza è la descrizione degli ideali di un anello quoziente. Siano I, K ideali dell'anello R tali che $I \subseteq K$. Denotiamo con K/I l'immagine di K tramite la proiezione canonica π di R su R/I, cioè $K/I = \{\ a + I \mid a \in K\ \}$. Per il Teorema di Corrispondenza applicato a π, K/I è un ideale di R/I. Si dimostra quindi il seguente

Teorema 10.8. *Sia I un ideale dell'anello R. Gli ideali dell'anello quoziente R/I sono tutti e soli quelli del tipo T/I al variare di T nell'insieme degli ideali di R che contengono I.*

Dimostrazione. Sia I un ideale dell'anello R; la proiezione canonica $\pi : I \to R/I$ è un omomorfismo suriettivo il cui nucleo è I. Per il teorema di Corrispondenza, gli ideali di R/I sono quindi le immagini tramite la proiezione degli ideali K di R tali che $I \subseteq K$, ovvero sono tutti e soli quelli del tipo K/I definiti prima dell'enunciato. ∎

Caso importante. Dato $n \geq 1$, consideriamo l'anello quoziente $\mathbb{Z}/n\mathbb{Z}$. I suoi ideali sono in corrispondenza con gli ideali $m\mathbb{Z}$ di $\mathbb{Z}$ tali che $n\mathbb{Z} \subseteq m\mathbb{Z}$ (con $n, m \geq 0$). Per la Proposizione 8.1 quest'ultima condizione si verifica se e solo se $m|n$. Quindi, gli ideali di $\mathbb{Z}/n\mathbb{Z}$ sono tutti e soli quelli del tipo

$$m\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} \mid x \in m\mathbb{Z}\} = \{mz + n\mathbb{Z} \mid z \in \mathbb{Z}\} = \{mz + n\mathbb{Z} \mid 0 \leq mz \leq n-1\}$$

con $m|n$.
Ad esempio, gli ideali di $\mathbb{Z}/12\mathbb{Z}$ sono (utilizzando la convenzione di indicare con una barra le classi resto: $a + 12\mathbb{Z} = \overline{a}$):

$$\begin{aligned}
\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{1},\ \overline{2},\ \ldots, \overline{11}\ \}\ ,\\
2\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{2},\ \overline{4},\ \overline{6},\ \overline{8},\ \overline{10}\ \}\ ,\\
3\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{3},\ \overline{6},\ \overline{9}\ \}\ ,\\
4\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{4},\ \overline{8}\ \}\ ,\\
6\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0},\ \overline{6}\ \}\ ,\\
12\mathbb{Z}/12\mathbb{Z} &= \{\ \overline{0}\ \}\ .
\end{aligned}$$

Esempio . Sia $R = \mathbb{Z}[\sqrt{2}] = \{\ x + y\sqrt{2} \mid x, y \in \mathbb{Z}\ \}$. Si provi che R è un anello (dimostrando che è un sottoanello di $\mathbb{R}$). Consideriamo il seguente ideale di R:

$$I = \{\ x + y\sqrt{2} \mid x, y \in 2\mathbb{Z}\ \}$$

(I è - lo si verifichi - l'ideale generato da 2 in R). Vogliamo determinare gli ideali dell'anello quoziente R/I. Per il Teorema precedente, ciò si realizza determinando gli ideali J di R che contengono I. Cominciamo con

$$K = (\sqrt{2}) = \{\ \sqrt{2}(y + x\sqrt{2}) \mid x, y \in \mathbb{Z}\ \} = \{\ 2x + y\sqrt{2} \mid x, y \in \mathbb{Z}\ \}$$

chiaramente $I \subseteq K$ (e $I \neq K$).
Sia ora J ideale di R con $I \subseteq J$. Supponiamo che J contenga un elemento $x + y\sqrt{2}$ con $2 \not| x$; allora $x - 1 \in 2\mathbb{Z}$, quindi $x - 1 \in I \subseteq J$, dunque $x + y\sqrt{2} - (x - 1) = 1 + y\sqrt{2} \in J$. Poichè J è ideale si ha $2y + \sqrt{2} = (1 + y\sqrt{2})\sqrt{2} \in J$ e dunque $\sqrt{2} \in J$ (dato che $2y \in I \subseteq J$); quindi $1 = (1 + y\sqrt{2}) - y\sqrt{2} \in J$, che implica $J = R$.
Sia dunque $J \neq R$ allora, per quanto dimostrato sopra, $J \subseteq K$. Supponiamo $I \neq J$. Allora esiste un elemento $x+y\sqrt{2} \in J$ con y dispari (e x pari dato che $J \subseteq K$). Poichè $x, (y-1)\sqrt{2} \in J$ si ha $\sqrt{2} = (x + y\sqrt{2}) - x - (y - 1)\sqrt{2} \in J$; ma allora $K = (\sqrt{2}) \subseteq J$ e quindi $J = K$.
In conclusione, gli ideali di R che contengono I sono I, K ed R; di conseguenza, gli ideali di R/I sono $I/I = \{0_{R/I}\},\ K/I$ e R/I.

Esercizio 10.5. Sia $f : R \to S$ un omomorfismo suriettivo di anelli commutativi, e sia K il nucleo di f. Sia I un ideale massimale di R. Si dimostri che si ha una delle seguenti possibilità:

- $f(I)$ un ideale massimale di S;
- $K + I = R$.

Esercizio 10.6. Sia J un ideale diverso dall'ideale nullo dell'anello degli interi di Gauss $Z[i]$. Si provi che l'anello quoziente $Z[i]/J$ è finito.

Esercizio 10.7. (Teorema cinese del Resto generalizzato) Sia R un anello commutativo, e siano I_1, I_2 ideali propri di R tali che $R = I_1 + I_2$. Si provi che

$$\frac{R}{I_1 \cap I_2} \simeq \frac{R}{I_1} \times \frac{R}{I_2}$$

[sugg.: provare che la applicazione $R \to R/I_1 \times R/I_2$ definita da $a \mapsto (a + I_1, a + I_2)$ è un omomorfismo suriettivo il cui nucleo è $I_1 \cap I_2$.]
Dedurre, applicando il punto precedente all'anello $\mathbb{Z}$, il Teorema Cinese dei resti (Teorema 4.13).

Esercizio 10.8. Sia R l'anello $\mathbb{Z}/24\mathbb{Z}$.

(1) Quali sono gli ideali massimali di R? E quelli primi?

(2) Descrivere i campi F tali che esiste un omomorfismo suriettivo $R \to F$.

Esercizio 10.9. Sia p un numero primo fissato e sia $R = \{\ \frac{m}{p^i} \mid m \in \mathbb{Z}\ , i \in \mathbb{N}\ \}$. Sia q un numero primo con $q \neq p$, e sia

$$J = \Big\{\ \frac{m}{p^i} \in R \mid q \text{ divide } m \Big\}.$$

Si provi che J è un ideale primo di R.

10.3 Quozienti di un PID e di $F[x]$.

In questa sezione applicheremo quanto visto nelle precedenti al caso di Domini a Ideali Principali. Cominciamo però con un'importante caratterizzazione degli ideali massimali, che vale in qualunque anello commutativo, e che ricorda il Teorema 10.2.

Teorema 10.9. *Sia R un anello commutativo, ed I un ideale di R. Allora I è un ideale massimale se e solo se l'anello quoziente R/I è un campo.*

Dimostrazione. ($\Rightarrow$) Sia I un ideale massimale e consideriamo l'anello quoziente R/I (è non degenere, perchè $I \neq R$). Per il Teorema di corrispondenza, gli ideali di R/I sono tutti e soli del tipo J/I con J ideale di R contenente I; per la massimalità di I, un tale J coincide con R o con I. Quindi, gli ideali di R/I sono : R/I e $I/I = \{0_{R/I}\}$. Per il Teorema 4.3 del capitolo III, si ha che R/I è un campo.
($\Leftarrow$) Sia R/I un campo. Allora, Per il Teorema III.4.3 , gli ideali di R/I sono R/I e $\{0_{R/I}\}$. Per il Teorema di corrispondenza, essi sono in corrispondenza biunivoca con tutti gli ideali di R che contengono I. Dunque tali ideali sono R (che corrisponde a R/I) e I stesso (che corrisponde a $\{0_{R/I}\} = I/I$). Quindi I è un ideale massimale. ∎

Mediante questo Teorema, e la Proposizione 8.8, si ottiene una nuova dimostrazione che $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se n è un numero primo. In modo simile il Teorema è utilizzato nell'esempio seguente. Più avanti, lo utilizzeremo in senso inverso.

Esempio. Consideriamo l'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ definito in precedenza. Fissato $a \in \mathbb{R}$, proviamo che l'insieme

$$I_a = \{\ f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\ \}$$

è un ideale massimale di $\mathbb{R}^{\mathbb{R}}$. Si consideri la applicazione $\Phi : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$ definita da $\Phi(f) = f(a)$. Provate che Φ è un omomorfismo suriettivo di anelli e che I_a è il suo nucleo; dal teorema di omomorfismo segue allora che $\mathbb{R}^{\mathbb{R}}/I_a$ è isomorfo a $\mathbb{R}$ che è un campo. Per il Teorema 10.9, I_a è un ideale massimale.

Veniamo ora a descrivere i quozienti dei domini a ideali principali. Come vedremo si tratta di mettere assieme diversi risultati provati finora.

Teorema 10.10. *Sia A un PID, e sia $0_A \neq a \in A$. Le seguenti condizioni sono equivalenti:*

(1) *(a) è primo;*

(2) *a è irriducibile;*

(3) *(a) è massimale;*

(4) *$A/(a)$ è un campo;*

Dimostrazione. (1) $\Rightarrow$ (2). Segue dal lemma 8.3.
(2) $\Rightarrow$ (3). Segue dalla Proposizione 8.10.
(3) $\Rightarrow$ (4). Segue dal Teorema 10.9

(4) $\Rightarrow$ (1). Se $A/(a)$ è un campo, allora $A/(a)$ è un dominio d'integità, dunque (a) è primo per il Teorema 10.2, e quindi a è un elemento primo per la Proposizione 8.7. ∎

Osservazione. Sia A un PID, sia a un suo elemento irriducibile, e sia $I = (a)$. Allora, A/I è un campo. In particolare, ogni elemento $b + I \neq I = 0_{A/I}$ di A/I ha un inverso. Vediamo come questo fatto possa essere dimostrato anche senza l'ausilio del Teorema di Corrispondenza. Ora $b + I \neq I$ se e solo se $b \notin I$, ovvero se e solo se a non divide b, e dato che a è irriducibile, ciò equivale a dire che $MCD(a, b) = 1$. Poiché A è un PID, per l'osservazione alla fine della sezione 8.3, se $b \notin I$, esistono allora $\alpha, \beta \in A$ tali che $a\alpha + b\beta = 1$. Ma allora, nel quoziente A/I, $(\beta + I)(b + I) = 1 + I = 1_{A/I}$, quindi $b + I$ è invertibile.
Un caso importante è quando A è un dominio euclideo (ad esempio un anello di polinomi a coefficienti su un campo), poiché in tal caso i coefficienti α e β di sopra (e dunque in particolare $\beta + I = (b + I)^{-1}$) possono essere trovati mediante l'algoritmo di Euclide.

Quozienti di $F[x]$. Applicando il Teorema 10.10 agli anelli di polinomi a coefficienti su un campo (che è un dominio a ideali principali), si ha il seguente e fondamentale risultato.

Teorema 10.11. *Sia F un campo, e sia $0 \neq f \in F[x]$. Allora sono equivalenti*

(1) f è irriducibile;

(2) (f) è un ideale massimale di $F[x]$;

(3) $F[x]/(f)$ è un campo.

Questo Teorema verrà usato appieno nella prossima sezione. Concludiamo questa con un risultato di notevole importanza pratica, in quanto descrive in modo conveniente gli elementi di un quoziente di un anello di polinomi (si osservi che qui non si richiede che il generatore dell'ideale sia irriducibile)

Proposizione 10.12. *Sia F un campo, sia $I = (f)$ un ideale non nullo e proprio di $F[x]$ e sia $n = \deg f$. Allora ogni elemento di $F[x]/I$ si scrive in modo unico nella forma*

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + I$$

con $a_0, a_1, \ldots, a_{n-1} \in F$.

Dimostrazione. Poichè $I = (f)$ è proprio e non nullo, si ha $n = \deg f \geq 1$. Sia $g + I$ un generico elemento di $F[x]/I$. Dividendo g per f, otteniamo $g = fq + r$, con $q, r \in F[x]$ e $r = 0$ o $\deg r \leq n - 1$; quindi $r = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$ per $a_0, a_1, \ldots, a_{n-1} \in F$. Ora $g - r = fq \in (f) = I$, quindi $g + I = r + I$, cioè

$$g + I = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + I \ .$$

Proviamo ora l'unicità. Siano $b_0, b_1, \ldots, b_{n-1} \in F$ tali che

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + I = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} + I$$

allora

$$h = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1} \in I = (f)$$

quindi $h = ft$ per qualche $t \in F[x]$. Poichè $\deg h \leq n-1 < n = \deg f$, ciò forza $h = 0$ e quindi $a_i = b_i$ per ogni $i = 0, 1, \ldots, n-1$. ∎

Esempio. Sia $f = x^2 + x + 1$. In $\mathbb{Q}[x]/(f)$ troviamo le eventuali radici del polinomio $t^3 - 2$. Per la proposizione 10.12, gli elementi di $\mathbb{Q}[x]/(f)$ si scrivono nella forma $u = ax + b + (f)$, con $a, b \in \mathbb{Q}$. Dunque se u è una radice di $t^3 - 8$ si ha

$$\begin{aligned} 8 + (f) = u^3 &= (ax+b)^3 + (f) = a^3x^3 + 3a^2bx^2 + 3ab^2x + b^3 + (f) \\ &= (3ab^2 - 3a^2b)x + (a^3 + b^3 - 3a^2b) + (f) \end{aligned}$$

(dove $(3ab^2 - 3a^2b)x + (a^3 + b^3 - 3a^2b)$ è il resto della divisone di $a^3x^3 + 3a^2bx^2 + 3ab^2x + b^3$ per f). Per l'unicità della scrittura in $\mathbb{Q}[x]/(f)$ dev'essere:

$$\begin{cases} 3ab^2 - 3a^2b = 0 \\ a^3 + b^3 - 3a^2b = 8 \end{cases}$$

Le soluzioni razionali di questo sistema sono $(a, b) = (2, 0), (0, 2), (-2, -2)$. Quindi se $u \in \mathbb{Q}[x]/(f)$, allora $u^3 = 8 + (f)$ se e solo se $u \in \{2x + (f), 2 + (f), -2x - 2 + (f)\}$.

Oltre che per lo studio delle estensioni, che vedremo nella prossima sezione, il Teorema 10.11 è uno strumento molto efficace per la costruzione di campi con particolari proprietà. Questo aspetto verrà approfondito nel corso di Algebra II; per il momento vediamo come si possano costruire campi finiti diversi dai quozienti $\mathbb{Z}/p\mathbb{Z}$.
Ad esempio, consideriamo il campo $\mathbb{Z}_2$, ed il polinomio $f = x^2 + x + \overline{1} \in \mathbb{Z}_2[x]$. Poichè $f(\overline{1}) = \overline{3} = \overline{1}$ e $f(\overline{0}) = \overline{1}$, f non ha radici in $\mathbb{Z}_2$ e dunque, essendo $\mathbb{Z}_2$ un campo, non ha fattori di grado 1. Quindi f è irriducibile in $\mathbb{Z}_2[x]$ e pertanto

$$E = \frac{\mathbb{Z}_2[x]}{(x^2 + x + \overline{1})}$$

è un campo. Inoltre sappiamo dalla Porposizione 10.12 che $E = \{a + bx + (f) \mid a, b \in \mathbb{Z}_2\}$. Per ciascuno degli elementi a, b sono possibili due scelte ($\overline{0}$ o $\overline{1}$), dunque E contiene esattamente 4 elementi. Abbiamo quindi costruito un campo di ordine 4, che fino a questo punto ci era sconosciuto.
Con un procedimento simile si può costruire per ogni primo p e ogni $n \geq 1$ un campo di ordine p^n. Anzi, ogni campo finito è isomorfo ad un campo costruito in questo modo. Questo risultato, insieme con la teoria di base dei campi finiti, verrà studiato nel corso di Algebra II.

Esercizio 10.10. Si provi che in un PID ogni quoziente modulo un ideale *non nullo* è un campo oppure possiede divisore dello zero.

Esercizio 10.11. Sia $f = x^4 - 6x^2 + 4$. Si provi che $\mathbb{Q}[x]/(f)$ è un campo.

Esercizio 10.12. Si dica se il seguente anello è un campo

$$R = \frac{\mathbb{Z}_5[x]}{(x^3 + \overline{2}x + \overline{1})}$$

e si dica quanti elementi contiene.

Esercizio 10.13. 1) Sia dica se il seguente anello R è un campo e, in caso di risposta negativa, si determinino i suoi ideali massimali

$$R = \frac{\mathbb{Q}[x]}{(x^3 - 3x + 2)} \ .$$

2) Si dica se esistono elementi $0 \neq a \in R$ tali che $a^2 = 0$.

Esercizio 10.14. Si costruisca un campo con 9 elementi.

10.4 Estensioni semplici

Sia R un sottoanello dell'anello *commutativo* S (il modello principale a cui fare riferimento è $\mathbb{Q} \subseteq \mathbb{C}$). Fissato un elemento $b \in S$ ci proponiamo di studiare il più piccolo sottoanello di S che contiene $R \cup \{b\}$; tale (sotto)anello, che certamente esiste, lo denoteremo con $R[b]$, e diremo che $R[b]$ è ottenuto da R mediande *l'aggiunzione* dell'elemento b. Un'estensione di R ottenibile mediante l'aggiunzione di un singolo elemento si dice *estensione semplice* di R. Osserviamo che dalla definizione segue immediatamente che $R[b] = R$ se e solo se $b \in R$.

Esempi. Abbiamo già incontrato esempi di questo tipo. Come abbiamo visto, l'insieme

$$\{\ a + b\sqrt{2} \mid a, b \in \mathbb{Q}\ \}$$

è un sottoanello dei numeri reali. Esso contiene $\mathbb{Q} \cup \{\sqrt{2}\}$, ed è chiaramente incluso in ogni sottoanello di $\mathbb{R}$ che contiene $\mathbb{Q} \cup \{\sqrt{2}\}$; si tratta quindi proprio del minimo sottoanello di $\mathbb{R}$ che contiene $\mathbb{Q} \cup \{\sqrt{2}\}$, cioè $\mathbb{Q}[\sqrt{2}]$ (come del resto lo avevamo denotato).

Similmente, l'anello $\mathbb{Z}[i]$ degli interi di Gauss è il minimo sottoanello di $\mathbb{C}$ che contiene $\mathbb{Z} \cup \{i\}$.

Un altro esempio è $\mathbb{C} = \{\ a + ib \mid a, b \in \mathbb{R}\ \} = \mathbb{R}[i]$.

Sia R sottoanello di S e $b \in S$. Chiaramente, ogni sottoanello di S che contiene b contiene anche tutte le potenze b^n con $n \in \mathbb{N}$. Dunque ogni sottoanello di S che contiene $R \cup \{b\}$ contiene ogni ab^n con $a \in R,\ n \in \mathbb{N}$ e quindi contiene anche ogni elemento del tipo

$$a_0 + a_1 b + a_2 b^2 + \ \ldots\ + a_n b^n \qquad (*)$$

con $a_0, a_1, \ldots, a_n \in R$ e $n \in \mathbb{N}$ (osserviamo che possiamo intendere $a_0 = a_0 b^0$).

Ora, l'insieme degli elementi di S del tipo $(*)$ costituisce un sottoanello di S. Innanzi tutto possiamo convenientemente scrivere in forma contratta tali elementi:

$$a_0 + a_1 b + a_2 b^2 + \ \ldots \ + a_n b^n = \sum_{i=0}^{n} a_i b^i \ .$$

Siano quindi $u = \sum_{i=0}^{n} a_i b^i$, $v = \sum_{i=0}^{m} c_i b^i$ con a_i $(i = 0, \ldots, n)$, c_j $(j = 0, \ldots, m)$ elementi di R, $n, m \in \mathbb{N}$; se $n \geq m$ (cosa che possiamo senz'altro assumere), riscriviamo: $v = \sum_{i=0}^{n} c_i b^i$ ponendo $c_i = 0$ per ogni $m + 1 \leq i \leq n$. Allora:

$$u - v = \sum_{i=0}^{n} a_i b^i - \sum_{i=0}^{n} c_i b^i = (a_0 - c_0) + (a_1 - c_1)b + \ldots + (a_n - c_n)b^n = \sum_{i=0}^{n} (a_i - c_i) b^i$$

che è del tipo $(*)$. Inoltre, usando le proprietà distributiva e commutativa, si prova che

$$uv = \left(\sum_{i=0}^{n} a_i b^i \right) \left(\sum_{i=0}^{m} c_i b^i \right) = \sum_{i=0}^{n+m} d_i b^i$$

dove $d_0 = a_0 c_0$, $d_1 = a_0 c_1 + a_1 c_0$, $d_2 = a_0 c_2 + a_1 c_1 + a_2 c_0$, $\ldots$, e in generale, per $0 \leq i \leq n + m$:

$$d_i = a_0 c_i + a_1 c_{i-1} + \ldots + a_{i-1} c_1 + a_i c_0 = \sum_{r=0}^{i} a_r c_{i-r}$$

infine $1_S = 1_R$ è del tipo $(*)$.

Dunque l'insieme degli elementi di S del tipo $(*)$ è un sottoanello che, per quanto osservato all'inizio, deve essere contenuto in ogni sottoanello di S che contiene $R \cup \{b\}$. Abbiamo quindi provato

Teorema 10.13. *Sia R sottoanello di S e sia $b \in S$. Allora*

$$R[b] = \left\{ \ \sum_{i=0}^{n} a_i b^i \ \mid \ n \in \mathbb{N}, \ a_0, a_1, \ldots, a_n \in R \ \right\} \ .$$

Come risulta dagli esempi visti in precedenza, per ottenere gli elementi di $R[b]$ non è sempre necessario dover considerare tutte le potenze b^n. Ad esempio, poichè $(\sqrt{2})^2 = 2$, $(\sqrt{2})^3 = 2(\sqrt{2})$, etc., ogni potenza di $\sqrt{2}$ con esponente ≥ 2 può essere riscritta nella forma 2^i oppure $2^i\sqrt{2}$ e quindi $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. La ragione generale di questo fenomeno, che si verifica solo per particolari elementi $b \in S$, sarà chiara tra poco.

Esercizio 10.15. Provare che $\mathbb{Q}[\sqrt{2}] \cap \mathbb{Q}[\sqrt{3}] = \mathbb{Q}$.

Soluzione. Si vede facilmente che $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Sia $u = x + y\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$ (con $x, y \in \mathbb{Q}$) e supponiamo per assurdo $y \neq 0$. Poichè $x, y^{-1} \in \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}]$ si ha in particolare $\sqrt{2} = y^{-1}(u - x) \in \mathbb{Q}[\sqrt{3}]$. Quindi esistono $a, b \in \mathbb{Q}$ tali che $\sqrt{2} = a + b\sqrt{3}$, da cui, elevendo al quadrato si ottiene $2ab\sqrt{3} = 2 - (a^2 + 3b^2) \in \mathbb{Q}$. Poichè $\sqrt{3} \notin \mathbb{Q}$, deve essere $ab = 0$. Se

$b = 0$ allora $\sqrt{2} = a \in \mathbb{Q}$ che è assurdo. Dunque $a = 0$ e quindi si ha $\sqrt{2} = b\sqrt{3}$. Sia $b = \frac{m}{n}$ con $m, n \in \mathbb{N}$; allora, elevando al quadrato, $2n^2 = 3m^2$ il che è impossibile perchè il primo 2 compare con esponente dispari nella fattorizzazione di $2n^2$ e con esponente pari in quella di $3m^2$. Quindi, se $u = x + y\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$, allora $y = 0$ cioè $u \in \mathbb{Q}$. Dunque $\mathbb{Q}[\sqrt{2}] \cap \mathbb{Q}[\sqrt{3}] = \mathbb{Q}$.

La notazione si estende naturalmente al caso di aggiunzione di 2 o più elementi. Se R è un sottoanello dell'anello commutativo S, e $b_1, b_2 \in S$, si denota con $R[b_1, b_2]$ il più piccolo sottoanello di S che contiene $R \cup \{b_1, b_2\}$. Chiaramente, $R[b_1, b_2] = R[b_1][b_2] = R[b_2][, b_1]$. Similmente, se $b_1, b_2, \ldots, b_n \in S$ allora $R[b_1, b_2, \ldots, b_n]$ è il più piccolo sottoanello di S che contiene $R \cup \{b_1, b_2, \ldots, b_n\}$, e $R[b_1, b_2, \ldots, b_n] = R[b_1, b_2, \ldots, b_{n-1}][b_n]$ etc.

Veniamo ora ad un punto importante. Sia R un sottoanello dell'anello S e sia $b \in S$. Sia $f = a_0 + a_1x + a_2x^2 + \ \ldots \ + a_nx^n$ un polinomio in $R[x]$. Poichè i coefficienti a_i sono in particolare elementi di S, ha senso considerare la sostituzione di x con b in f:

$$f(b) = a_0 + a_1b + a_2b^2 + \ \ldots \ + a_nb^n$$

che è un elemento di S. Dalla discussione precedente, risulta immediatamente

$$R[b] = \{f(b) \mid f \in R[x]\},$$

che è l'immagine dell'omomorfismo di sostituzione

$$\begin{array}{rccc} \sigma_b : & R[x] & \to & S \\ & f & \mapsto & f(b) \end{array}$$

Ora, il nucleo di tale omomorfismo è $I_b = \ker(\sigma_b) = \{f \in R[x] \mid f(b) = 0\}$.
Dal Teorema di omomorfismo 10.4 discende allora che

$$R[b] \simeq \frac{R[x]}{I_b}.$$

Questo è un fatto molto importante, perché ci dice che *ogni estensione semplice di un anello R si può realizzare come un opportuno quoziente dell'anello dei polinomi $R[x]$* e merita di essere enunciato come un Teorema.

Teorema 10.14. *Sia R sottoanello dell'anello S e sia $b \in S$. Allora*

$$\{f \in R[x] \mid f(b) = 0\} = I_b$$

è un ideale di $R[x]$ e $R[b] \simeq R[x]/I_b$.

Prima di continuare in questa analisi, passando a vedere cosa succede quando R è un campo, diamo una importante definizione

Elementi algebrici e trascendenti. Sia R un sottoanello dell'anello S e sia $b \in S$.

(1) b si dice **algebrico** su R se esiste un polinomio $f \neq 0$ in $R[x]$ tale che $f(b) = 0$.

(2) b si dice **trascendente** su R se per ogni polinomio $f \neq 0$ in $R[x]$ si ha $f(b) \neq 0$.

Esempio 1. Per ogni $n, m \in \mathbb{N}$ con $m \geq 1$, $\sqrt[m]{n}$ è un numero reale algebrico su $\mathbb{Q}$ (ed anche su $\mathbb{Z}$), essendo radice del polinomio $x^m - n \in \mathbb{Z}[x]$.

Esempio 2. Similmente, $i \in \mathbb{C}$ è algebrico su $\mathbb{Q}$ essendo radice del polinomio $x^2 + 1$.

Esempio 3. Proviamo che $u = \sqrt{2} - \sqrt{3}$ è algebrico su $\mathbb{Q}$. Occorre trovare un polinomio non nullo in $\mathbb{Q}[x]$ che ammette u come radice. Cominciamo con elevare u al quadrato

$$u^2 = 2 - 2\sqrt{2}\sqrt{3} + 3 = 5 - 2\sqrt{6}$$

da cui $2\sqrt{6} = 5 - u^2$ ed elevando ancora al quadrato

$$24 = u^4 - 10u^2 + 25$$

quindi u è radice del polinomio $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ e dunque è algebrico su $\mathbb{Q}$.

Osserviamo che se R è sottoanello in S e $b \in S$ è trascendente su R, allora l'ideale $I_b = \{f \in R[x] \mid f(b) = 0\}$ del Teorema 10.14 coincide con $\{0\}$; dunque, in questo caso, l'omomorfismo di sostituzione σ_b è iniettivo. Si ha quindi la

Teorema 10.15. *Sia R un sottoanello dell'anello S e sia $b \in S$ trascendente su R. Allora $R[b] \simeq R[x]$.*

Esistono numeri reali che sono trascendenti su $\mathbb{Q}$. Esempi sono i numeri π ed e (e quindi, per il Teorema 10.15, $\mathbb{Q}[\pi]$ è, ad esempio, isomorfo all'anello dei polinomi $\mathbb{Q}[x]$). La dimostrazione di questo fatto è stata ottenuta da F. Lindemann nel 1882, ed è piuttosto complicata. Tuttavia, non è difficile provare che l'insieme dei numeri reali che sono algebrici su $\mathbb{Q}$ è un insieme numerabile; poichè l'insieme dei reali non è numerabile, da ciò segue che devono esistere numeri reali trascendenti su $\mathbb{Q}$.

Estensioni semplici di campi. Supponiamo ora che F sia un campo contenuto come sottoanello di S, e che b sia un elemento di S algebrico su F. Allora, per definizione, esiste almeno un polinomio non nullo a coefficienti in F che ammette b come radice. Essendo F un campo, l'ideale

$$I_b = \{\ g \in F[x] \mid g(b) = 0\ \}$$

è principale e non è l'ideale nullo. Dunque, dalla dimostrazione del Teorema 9.5, sappiamo che un generatore f di I_b è un polinomio di grado *minimo* tra i polinomi non nulli di I_b; quindi

se b è un elemento algebrico sul campo F, allora l'ideale $I_b = \{g \in F[x] \mid g(b) = 0\}$ di $F[x]$ è un ideale principale, generato da un polinomio di grado minimo tra i polinomi non nulli a coefficienti in F che ammettono b come radice.

Supponiamo ora che f e f_1 siano due generatori del medesimo ideale $I \neq \{0\}$ di $F[x]$; dalla Proposizione 8.1 sappiamo che f ed f_1 sono associati in $F[x]$, e quindi che esiste un elemento $0_F \neq c \in F$ (si ricordi che gli elementi invertibili di $F[x]$ sono tutti e soli gli elementi non nulli di F) tale che $f_1 = cf$. Ora, se $f = a_0 + a_1x + \ldots + a_nx^n$ con $a_n \neq 0$ allora $a_n^{-1}f$ è il solo polinomio associato ad f che abbia coefficiente direttivo

uguale a 1. (Ricordo che un polinomio con coefficiente direttivo uguale ad 1 si dice *monico*).
Assemblando le osservazioni fatte sopra, otteniamo che ogni ideale non nullo di $F[x]$ (F è sempre un campo) ha un solo generatore monico. In particolare se b è un elemento algebrico sul campo F, allora l'ideale $I_b = \{g \in F[x] \mid g(b) = 0\}$ ha un unico generatore monico, che si chiama **il polinomio minimo** di b su F.

Poniamoci ora nella situazione che ci interessa di più, che è quella in cui F è sottocampo di un altro campo K (il caso principale è quello di $\mathbb{Q}$ come sottocampo di $\mathbb{C}$).
Sia $b \in K$ un elemento algebrico su F, e sia $f \in F[x]$ il suo polinomio minimo. Supponiamo che f si fattorizzi in $F[x]$ come il prodotto di due polinomi, cioè che $f = gh$ con $g, h \in F[x]$ (ed, essendo $f \neq 0$, è anche $g \neq 0 \neq h$). Allora, applicando l'omomorfismo di sostituzione:

$$0 = f(b) = g(b)h(b) \ ;$$

poichè K è un campo, si deve avere $g(b) = 0$ oppure $h(b) = 0$. Sia $g(b) = 0$, allora, poichè $g \neq 0$, deve essere $\deg g = \deg f$, quindi $\deg h = 0$, che significa $h \in F^*$; similmente, se $h(b) = 0$ si ha $\deg h = \deg f$ e $g \in F^*$. Abbiamo quindi concluso che il polinomio f è irriducibile; un fatto fondamentale che riportiamo nel seguente enunciato.

Proposizione 10.16. *Sia F un sottocampo del campo K, e sia $b \in K$ un elemento algebrico su F. Allora il polinomio minimo di b su F è irriducibile.*

Osserviamo che, viceversa, se $f \in F[x]$ è un polinomio monico irriducibile che ammette b come radice nel campo K, allora f è il polinomio minimo di b su F; infatti il polinomio minimo g di b divide f e quindi $\deg g = \deg f$ da cui $g = f$ (essendo entrambi monici).

Esempio. Consideriamo il numero reale $u = \sqrt{2} - \sqrt{3}$ dell'esmpio 3 a pagina precedente, e proviamo che $f = x^4 - 10x^2 + 1$ è proprio il polinomio minimo di u su $\mathbb{Q}$. Per quanto osservato sopra, è sufficiente provare che f non è il prodotto di due polinomi razionali di grado minore o uguale a 3. Cominciamo con l'osservare che f non ha divisori di grado 1. Infatti se g fosse un divisore di grado 1 di f, moltiplicando per un invertibile, possiamo assumere $g = x - a$ per qualche $a \in \mathbb{Q}$. Allora, per il Teorema di Ruffini, $f(a) = 0$. Ma ogni radice α di f soddisfa

$$\alpha^2 = 5 \pm \sqrt{24}$$

e quindi non è un numero razionale. Dunque f non ha divisori di grado 1.
Supponiamo per assurdo che f sia il prodotto di due polinomi razionali di grado 2. Allora

$$f = (x^2 + ax + b)(x^2 + cx + d)$$

con $a, b, c, d \in \mathbb{Q}$. Eseguendo il prodotto e confrontando i coefficienti con quelli di f si ottengono le condizioni

$$\begin{cases} a + c = 0 \\ d + ac + b = -10 \\ ad + bc = 0 \\ bd = 1 \end{cases}$$

da cui, con elementari passaggi algebrici, si ricava $a = 0$ oppure $b = b^{-1}$. Nel primo caso segue che $c = 0$ e b, d sono radici del polinomio $x^2 + 10x + 1$ che non sono razionali. Nel secondo caso, $b = \pm 1$ ed $a^2 = 10 \pm 2$ che ancora non è soddisfatta per valori razionali di a. Dunque il sistema non ha soluzioni razionali, e di conseguenza f non è il prodotto di due polinomi razionali di grado 2. In conclusione, f è il polinomio minimo di $\sqrt{2} - \sqrt{3}$ su $\mathbb{Q}$.

Unendo la Proposizione 10.16 con i Teoremi 10.11 e 10.14 si ottiene un'immediata ed importante conseguenza:

Teorema 10.17. *Sia F un sottocampo del campo K, sia $b \in K$ un elemento algebrico su F. Allora $F[b]$ è un campo.*

Dimostrazione. Sia f il polinomio minimo di b su F. Allora, per la Proposizione 10.16, f è un polinomio irriducibile, quindi, per il Teorema 10.11, (f) è un ideale massimale e dunque, per il Teorema 10.14

$$F[b] \simeq \frac{F[x]}{(f)}$$

è un campo. ∎

Esempio. $x^2 + 1$ è il polinomio minimo su $\mathbb{R}$ dell'elemento $i \in \mathbb{C}$, ed inoltre $\mathbb{C} = \mathbb{R}[i]$. Quindi

$$\mathbb{C} \simeq \frac{\mathbb{R}[x]}{(x^2 + 1)}$$

che si può anche vedere come una costruzione del campo $\mathbb{C}$ a partire da $\mathbb{R}$; si potrebbe cioè *definire* il campo dei numeri complessi come l'anello $\mathbb{R}[x]/(x^2 + 1)$.

Infine, se $b \in K$ è un elemento algebrico su F e $f \in F[x]$ è il suo polinomio minimo, utilizzando la Proposizione 10.12, e mediante l'isomorfismo $F[x]/(f) \to F[b]$, otteniamo una descrizione conveniente degli elementi di $F[b]$.

Proposizione 10.18. *Sia F un campo, b un elemento algebrico su F appartenente ad campo K e $f \in F[x]$ il suo polinomio minimo. Allora ogni elemento di $F[b]$ si scrive in modo unico nella forma*

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

dove $n = \deg f$ e $a_0, a_1, \ldots, a_{n-1} \in F$.

Esempio 1. Sia $\zeta = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$ una radice primitiva terza dell'unità. $\zeta^3 = 1$, quindi ζ è radice del polinomio razionale $x^3 - 1$. Si ha $x^3 - 1 = (x - 1)(x^2 + x + 1)$ e poichè ζ non è radice di $x - 1$ deve essere radice di $f = x^2 + x + 1$. Ora, f è irriducibile in $\mathbb{Q}[x]$ (dato che non ha radici in $\mathbb{Q}$, non ha divisori di grado 1 in $\mathbb{Q}[x]$), e dunque è il polinomio minimo di ζ su $\mathbb{Q}$. Quindi $\mathbb{Q}[\zeta] \simeq \mathbb{Q}[x]/(x^2 + x + 1)$ è un campo; inoltre per la Proposizione 10.18

$$\mathbb{Q}[\zeta] = \{\ a + b\zeta \mid a, b \in \mathbb{Q}\ \}\ .$$

Il polinomio minimo fornisce la relazione fondamentale per eseguire i calcoli in $\mathbb{Q}[\zeta]$: $\zeta^2 = -\zeta - 1$. Proviamo, ad esempio che $i \notin \mathbb{Q}[x]$. Supponiamo per assurdo che esistano $a, b \in \mathbb{Q}$ tali che $a + b\zeta = i$; allora

$$-1 = i^2 = a^2 + 2ab\zeta + b^2\zeta^2 = a^2 + 2ab\zeta - b^2\zeta - b^2 = (a^2 - b^2) + (2a - b)b\zeta$$

per l'unicità della scrittura degli elementi di $\mathbb{Q}[\zeta]$ nella forma $x + y\zeta$ si ha

$$\begin{cases} a^2 - b^2 = -1 \\ (2a - b)b = 0 \end{cases}$$

da cui $b = 0$ oppure $b = 2a$; nel primo caso si ha allora $a^2 = -1$ che è assurdo (a è razionale); nel secondo caso si ha $3a^2 = 1$ che anche non è possibile per $a \in \mathbb{Q}$. Quindi $i \notin \mathbb{Q}[\zeta]$.

Esempio 2. Sia $u = \sqrt{2} - \sqrt{3}$. Come abbiamo visto il u è algebrico su $\mathbb{Q}$; quindi $\mathbb{Q}[u]$ è un campo. In particolare $v = \sqrt{2} + \sqrt{3} = -u^{-1} \in \mathbb{Q}[u]$ e conseguentemente

$$\sqrt{2} = \frac{v + u}{2} \in \mathbb{Q}[u] \qquad \text{e} \qquad \sqrt{3} = \frac{v - u}{2} \in \mathbb{Q}[u]$$

Quindi $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2} - \sqrt{3}]$; d'altra parte è chiaro che $\mathbb{Q}[\sqrt{2} - \sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ e dunque $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} - \sqrt{3}]$.
Si provi per esercizio che $\mathbb{Q}[\sqrt{2} - \sqrt{3}] = \{\ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\ \}$.

Grado di una estensione. Concludiamo questo capitolo con una utile considerazione, che sarà ripresa ed approfondita in un corso successivo.

Sia F un sottocampo del campo K. Allora è possibile vedere K come spazio vettoriale su F: i vettori sono gli elementi di K, gli scalari quelli di F e il prodotto di un vettore per uno scalare è effettuato mediante la moltiplicazione dei due elementi nel campo K. In questa situazione, la dimensione di K come spazio vettoriale su F si chiama **grado** di K su F, e si denota con $[K : F]$.
Ad esempio, ogni numero complesso si scrive in modo unico nella forma $a+ib = a1+bi$ con $a, b \in \mathbb{R}$, cioè come combinazione lineare (a coefficienti nel campo degli scalari $\mathbb{R}$) di 1 e i (visti come vettori). Quindi $\{1, i\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$ e quindi $[\mathbb{C} : \mathbb{R}] = 2$.
Più in generale, se $b \in K$ è algebrico su F e il polinomio minimo di b su F ha grado n, la Proposizione 10.18 asserisce che l'insieme $\{1,\ b,\ b^2,\ \ldots\ ,\ b^{n-1}\}$ è una base di $F[b]$ come spazio vettoriale su F, la cui dimensione è quindi n. Con le notazioni introdotte sopra, abbiamo provato

Proposizione 10.19. *Sia F sottocampo del campo K, sia $b \in K$ un elemento algebrico su F, e sia $f \in F[x]$ il suo polinomio minimo. Allora* $[F[b] : F] = \deg f$.

Il concetto di grado svolgerà un ruolo essenziale nello studio delle estensioni di campi nel corso di Algebra II.

Esercizio 10.16. Descrivere gli elementi di $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Esercizio 10.17. Si provi che l'elemento $u = 1 - \sqrt[3]{2}$ è algebrico su $\mathbb{Q}$. Si determini il suo polinomio minimo e, in $\mathbb{Q}(u)$, si calcoli u^{-1}.

Esercizio 10.18. Sia F un campo e b un elemento algebrico su F. Provare che, per ogni $a \in F$, $b + a$ è algebrico su F.

Esercizio 10.19. Provare che $\mathbb{Z}[\frac{1}{3}] \simeq \mathbb{Z}[x]/(3x-1)$.

Esercizio 10.20. Sia $S = \mathbb{R} \times \mathbb{R}$ l'anello prodotto diretto. Sia $\overline{\mathbb{R}} = \{ (a,a) \mid a \in \mathbb{R} \}$. Si provi che $\overline{\mathbb{R}}$ è un sottoanello di S e che $\overline{\mathbb{R}} \simeq \mathbb{R}$. Si consideri quindi l'elemento $b = (0,1) \in S$, si provi che è algebrico su $\overline{\mathbb{R}}$ e che il suo polinomio minimo è $x^2 - x$, che **non** è irriducibile in $\mathbb{R}[x]$. Quindi la Proposizione 10.16 non vale se l'elemento algebrico b non viene preso in un campo. Si provi infine che $\overline{\mathbb{R}}[(0,1)] = S$, concludendo che $\mathbb{R} \times \mathbb{R} \simeq \mathbb{R}[x]/(x^2 - x)$.

Esercizio 10.21. Si determini il grado $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}]$.

10.5 Esercizi.

Esercizio 10.22. Sia $\phi : \mathbb{Z}[x] \to \mathbb{Q}$ un omomorfismo d'anelli.

(a) Si provi che $\mathrm{Im}(\phi) \neq \mathbb{Q}$.

(b) Si provi che se $\phi(x) = \frac{r}{s}$ con $r, s \in \mathbb{Z}$ e $(r,s) = 1$, allora $\ker(\phi) = (sx - r)$.

(c) Quanti sono gli omomorfismi distinti da $\mathbb{Z}[x]$ in $\mathbb{Q}$?

(d) Quanti sono gli omomorfismi distinti da $\mathbb{Q}$ in $\mathbb{Z}[x]$?

[suggerimento per il punto (b): osservare innanzi tutto che $\phi(z) = z$ per ogni $z \in \mathbb{Z}$. Quindi, posto $f = rx - s$, l'inclusione $(f) \subseteq \ker(\phi)$ è facile; per il viceversa, osservare che è sufficiente provare che ogni polinomio primitivo $g \in \ker(\phi)$ appartiene a (f); quindi dividere g per f in $\mathbb{Q}[x]$, come deve essere il resto ?...quindi applicare le considerazioni che riguardano le fattorizzazioni dei polinomi primitivi...]

Esercizio 10.23. Sia

$$A = \{ a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N},\, a_0 \in \mathbb{Z},\, a_i \in 12\mathbb{Z} \text{ per } i = 1, \ldots, n \} .$$

(a) Si provi che A è un sottoanello dell'anello dei polinomi $\mathbb{Z}[x]$.

(b) Si provi che $J = \{ f \in A \mid f(0) = 0 \}$ è un ideale di A, e si dica se è un ideale massimale.

(c) Determinare gli ideali dell'anello A/J.

(d) Dire se A/J è un dominio d'integrità.

Esercizio 10.24. Sia $f = x^2 - 3 \in \mathbb{Q}[x]$. Si determinino gli elementi invertibili dell'anello $\mathbb{Q}[x]/(f)$.

Esercizio 10.25. Al variare di $a \in (\mathbb{Z}/5\mathbb{Z})$ sia $f_a = x^3 + 2ax - 1 \in (\mathbb{Z}/5\mathbb{Z})[x]$. Si dica per quali valori di a l'anello $(\mathbb{Z}/5\mathbb{Z})[x]/(f_a)$ è un campo.

Esercizio 10.26. Siano $f = x^4 + x^3 - 5x^2 + x - 6$ e $g = x^5 + x^4 - 7x^3 - 3x^2 + 4x + 12$, e sia $I = (f,g)$ l'ideale generato da f e g in $\mathbb{Q}[x]$.

(a) Si provi che I non è un ideale massimale di $\mathbb{Q}[x]$.

(b) Si determinino i divisori dello zero dell'anello quoziente $\mathbb{Q}[x]/I$.

Esercizio 10.27. Sia $f = x^4 + 4x^2 - 10 \in \mathbb{Q}[x]$, e sia $\overline{f} \in (\mathbb{Z}/5\mathbb{Z})[x]$ la riduzione modulo 5 di f.

(a) Si dica se $\mathbb{Q}[x]/(f)$ è un campo.

(b) Si dica se $\overline{f}$ è irriducibile in $(\mathbb{Z}/5\mathbb{Z})[x]$.

Esercizio 10.28. Sia $Y = \{a_0 + a_1x^2 + a_2x^4 ... + a_nx^{2n} \mid n \in \mathbb{N}, a_i \in \mathbb{Q}\}$. Si provi che Y è un ideale di $Q[x]$, si trovi un generatore $f \in \mathbb{Q}[x]$ di Y e si dica se $\mathbb{Q}[x]/Y$ è un campo.

Esercizio 10.29. (a) Si trovi un generatore dell'ideale

$$I = (x^3 - x^2 - 3x + 2\ ,\ x^4 + x^3 - 3x^2 - 2x + 2)$$

nell'anello $\mathbb{Q}[x]$. Si dica se $\mathbb{Q}[x]/I$ è un campo.

(b) Stesse domande in $\mathbb{R}[x]$.

Esercizio 10.30. Sia

$$F = (\mathbb{Z}/3\mathbb{Z})[x]/(x^3 - x + \overline{1}).$$

(a) Si provi che F è un campo, e si dica quanti elementi ha F.

(b) Posto $\alpha = x + (x^3 - x + \overline{1})$, si scriva l'elemento $(\alpha^3 - 1)^{-1}$ come combinazione a coefficienti in $\mathbb{Z}/3\mathbb{Z}$ di $1\ , \alpha\ , \alpha^2$.

Esercizio 10.31. Dire, motivando le risposte, se le seguenti affermazioni sono vere.

(a) $\mathbb{Q}[i] = \mathbb{Q}[i + 2]$.

(b) $\mathbb{Q}[i] = \mathbb{Q}[2i]$.

(c) $\mathbb{Q}[i] = \mathbb{Q}[i + \sqrt{2}]$.

Esercizio 10.32. Dimostrare o confutare che $\mathbb{Q}[\sqrt{2}, \sqrt{7}] = \mathbb{Q}[\sqrt{2} + \sqrt{7}]$.

Esercizio 10.33. Per ogni $h \in \mathbb{Z}$ sia

$$E_h = \frac{\mathbb{Q}[x]}{(x^3 + hx^2 - hx + 2)}$$

(a) Si dica per quali $h \in \mathbb{Z}$, E_h è un campo.

(b) Posto $h = 2$ si dica se esiste un elemento $u \in E_h$ tale che $u^2 = -3$.

(c) Posto $h = 1$ si determini un ideale I di $\mathbb{Q}[x]$ tale che $(x^3 + hx^2 - hx + 2) \subseteq I$ e $\mathbb{Q}[x]/I$ contiene un elemento w tale che $w^2 = -3 + I$.

Esercizio 10.34. Sia $f = x^4 + 5x^2 + 6 \in \mathbb{Q}[x]$.

(a) Si dica, motivando la risposta, se l'anello $E = \mathbb{Q}[x]/(f)$ è un campo.

(b) Si dica se $x + (f)$ è un elemento invertibile di E.

(c) Si determinino tutti gli ideali di $\mathbb{Q}[x]$ che contengono l'ideale (f).

Esercizio 10.35. Determinare in $\mathbb{Q}[x]$ il polinomio minimo di $\sqrt[3]{2} - 2$ e quello di $\sqrt[3]{4} - \sqrt[3]{2}$.

Esercizio 10.36. Sia $\mathbb{R} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

(a) Si dica se R è un campo, e in R si determini $(\sqrt{2}-3)^{-1}$.

(b) Si dica quali fra i seguenti numeri reali appartengono a R: $\sqrt{2},\ \sqrt{5},\ \sqrt{6}$.

(c) Si dica se esiste un automorfismo ϕ di R tale che $\phi(\sqrt{2}) = \sqrt{3}$.

Esercizio 10.37. Sia $u = \sqrt[3]{5} - 2$.

(a) Si calcoli il polinomio minimo di u su $\mathbb{Q}$.

(b) Si provi che $\mathbb{Q}[u] = \mathbb{Q}[u^2]$.

(c) Si dica se il polinomio $x^3 - 5$ ha soluzioni diverse da 1 in $\mathbb{Q}[u]$.

Esercizio 10.38. Sia $1 \neq a \in \mathbb{C}$ un elemento algebrico su $\mathbb{Q}$, e sia $h \in \mathbb{Q}[x]$ il suo polinomio minimo su $\mathbb{Q}$.

(a) Si provi che esiste $g \in \mathbb{Q}[x]$ tale che $g(a) = \frac{1}{a-1}$.

(b) Sia $I = \{f - g \mid f, g \in \mathbb{Q}[x] \text{ e } f(a) = ag(a)\}$; si provi che I è un ideale di $\mathbb{Q}[x]$ che contiene (h).

Esercizio 10.39. Determinare $\mathbb{Q}[\sqrt[3]{2}] \cap \mathbb{Q}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt[3]{2}] \cap \mathbb{Q}$.

Esercizio 10.40. Sia b una radice complessa del polinomio $x^3 - 3x + 4$.

(a) Si calcoli il grado del polinomio minimo di b su $\mathbb{Q}$;

(b) In $\mathbb{Q}[b]$ si scriva b^{-1} come combinazione di $1, b, b^2$ a coefficienti razionali.

(c) Si dica se $i \in \mathbb{Q}[b]$.

Esercizio 10.41. Si calcoli il polinomio minimo di $\sqrt{2} + \sqrt{3}$ sul campo $\mathbb{Q}(\sqrt{6})$.

Esercizio 10.42. Sia $f = x^5 - 2x^3 - 2x^2 + 4 \in \mathbb{Q}[x]$.

(1) Si dica se $\mathbb{Q}[x]/(f)$ è un campo.

(2) Si dica se il campo $E = \mathbb{Q}(\sqrt[6]{2})$ contiene tutte le radici complesse di f.

Esercizio 10.43. Sia $f = x^4 + 4x^3 - 2 \in \mathbb{Q}[x]$.

(a) Si provi che f è irriducibile in $\mathbb{Q}[x]$, ma che le riduzioni di f rispettivamente modulo 2, 3 e 5 sono riducibili in $(\mathbb{Z}/2\mathbb{Z})[x]$, $(\mathbb{Z}/3\mathbb{Z})[x]$ e $(\mathbb{Z}/5\mathbb{Z})[x]$.

(b) Sia $\alpha \in \mathbb{C}$ una radice di f, e si consideri il suo quadrato α^2. Si provi che il polinomio minimo di α^2 su $\mathbb{Q}$ ha grado 4.

Esercizio 10.44. Sia $f = a_o + a_1 x + ... + a_n x^n \in \mathbb{Q}[x]$, con $a_o \neq 0 \neq a_n$. Si definisca quindi il polinomio $Rew(f) = a_n + a_{n-1}x + ... + a_o x^n$, e si provi che $Rew(f)$ è irriducibile in $\mathbb{Q}[x]$ se e solo se f è irriducibile in $\mathbb{Q}[x]$.

Esercizio 10.45. Sia f un polinomio monico irriducibile in $\mathbb{Q}[x]$ e sia $\beta \in \mathbb{C}$ una sua radice. Si provi che per ogni $0 \neq a \in \mathbb{Q}$, $\beta + a$ non è una radice di f. [sugg.: Poichè f è monico e irriducibile, f è il polinomio minimo di β su $\mathbb{Q}$. Supponete, per assurdo, che per un certo $0 \neq a \in \mathbb{Q}$, $\beta + a$ sia una radice di f, allora β è una radice del polinomio $g = f(x + a) \in \mathbb{Q}[x]$; per l'unicità del polinomio minimo, $g = f$. Ma allora $f(\beta + 2a) = f(\beta + a + a) = g(\beta + a) = f(\beta + a) = 0$ ...]

Esercizio 10.46. Si provi che ogni numero complesso è algebrico su $\mathbb{R}$.

Esercizio 10.47. Si dimostri che l'anello $E = \mathbb{Q}[x]/(x^4 + 15x^3 + 7)$ è un campo. Si dica quindi se il polinomio $x^2 - 2$ è irriducibile in $E[x]$.

Esercizio 10.48. Al variare di $h \in \mathbb{Q}$, sia $f_h = x^3 + hx + 1 \in \mathbb{Q}[x]$, e sia E_h il campo ottenuto aggiungendo a $\mathbb{Q}$ tutte le radici complesse di f_h.

(a) Per quali valori razionali di h si ha $[E_h : \mathbb{Q}] = 2$?

(b) Per quali valori razionali di h esistono due radici complesse distinte c_1 e c_2 di f_h tali che $c_1 c_2 \in \mathbb{Q}$?

Esercizio 10.49. Si costruisca un campo di ordine 25.

Esercizio 10.50. A partire da $\mathbb{Z}/3\mathbb{Z}$ si costruisca un campo E di ordine 27. Si dica quali sono nel campo E le radici del polinomio $x^5 - 1$.

Appendice A

Soluzioni di alcuni esercizi

6.1 Occorre provare che anche la commutatività della somma è soddisfatta. Siano $a, b \in A$. Applicando le proprietà distributive (D), le proprietà (P1) e (S1) abbiamo

$$(a+b)(1_A+1_A) = (a+b)1_A + (a+b)1_A = (a+b) + (a+b) = a + (b+a) + b$$

$$(a+b)(1_A+1_A) = a(1_A+1_A)+b(1_A+1_A) = (a1_A+a1_A)+(b1_A+b1_A) = a+(a+b)+b$$

quindi $a + (b + a) + b = a + (a + b) + b$, da cui, sommando a sinistra $(-a)$ e a destra $(-b)$ entrambi i membri dell'equaglianza, si ricava $b + a = a + b$.

6.6 Sia $0 \neq f \in \mathbb{R}^{\mathbb{R}}$ e supponiamo che f non sia invertibile; allora per quanto visto nel testo $Z_f = \{a \in \mathbb{R} \mid f(a) = 0\} \neq \emptyset$. Poiché $f \neq 0$ si ha anche $Z_f \neq \mathbb{R}$. Sia allora $g \in \mathbb{R}^{\mathbb{R}}$ definita da

$$g(a) = \begin{cases} 0 & \text{se} \quad f(a) \neq 0 \\ 1 & \text{se} \quad f(a) = 0 \end{cases}$$

Allora $g \neq 0$ e $fg = o$, provando che f è un divisore dello zero.
Se invece consideriamo l'anello $\mathcal{C}$ delle funzioni continue, l'asserto non è più vero. Consideriamo ad esempio, la finzione $f(x) = x$. Essa è non invertibile (perché $f(0) = 0$), ma non esiste alcuna funzione continua $g \neq 0$ tale che $fg = 0$: infatti, la seconda condizione comporta che g si annulli in ogni $x \neq 0$; ma allora, per continuità g è la funzione costante 0.

6.31 Poiché $I + L = A$, esistono $x \in I$ e $y \in L$ tali che $1_A = x + y$. Sia ora $a \in K$; allora $a - xa \in K$, perché K è un ideale, e $ya \in L$, perché L è un ideale. Quindi

$$a - xa = (1_A - x)a = ya \in K \cap L \subseteq I.$$

Infine, poiché I è un ideale, $ax \in I$, e dunque $a = (a - ax) + ax \in I$, provando così $K \subseteq I$.

6.35 (a) Siano $x, y \in R$, e supponiamo che x^2 e $x + y$ appartengano all'ideale I. Allora (tenendo conto che R è commutativo), I contiene

$$(y - x)(x + y) = yx + y^2 - x^2 - xy = y^2 - x^2$$

e quindi $y^2 = (y^2 - x^2) + x^2 \in I$.

(b) Sia $x \in R$ tale che $x^2 \in I$, e sia K come definito nel testo. Si osservi che la condizione che definisce gli elementi y di K, $x(x+y) \in I$, equivale a $x^2 - xy \in I$, e quindi (siccome $x^2 \in I$), equivale a $xy \in I$. A questo punto, tenendo conto che I è un ideale e che R è commutativo, è facile provare che K è un ideale di R.

6.36 (a) Osserviamo che, poiché R è sottoanello di $\mathbb{Q}$, $1 \in R$, e quindi $\mathbb{Z} \subseteq R$. Sia dunque $a/b \in R$, con a e b interi coprimi (e $b \neq 0$). Allora esistono $\alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha a + \beta b$, e quindi, per quanto osservato,

$$\frac{1}{b} = \frac{\alpha a + \beta b}{b} = \alpha \frac{a}{b} + \beta \in R.$$

(b) Sia I un ideale di R, e sia $I \neq \{0\} = (0)$. Allora esiste un numero razionale $0 \neq a/b \in I$ (con a, b interi coprimi). Quindi, poiché $b \in R$, $a = (a/b)b \in I$. Dunque $I \cap \mathbb{N} \neq \emptyset$. Sia allora $n = \min(I \cap \mathbb{N})$. Chiaramente $(n) = nR \subseteq I$. Viceversa, sia $x = u/v \in I$ (con u, v interi coprimi). Osserviamo che, per il punto (a), $1/v \in R$, e quindi $n/v = n(1/v) \in I$. Dividiamo ora l'intero u per n, $u = qn + r$, con $0 \leq r \leq n-1$. Allora

$$\frac{r}{v} = \frac{u}{v} - n\frac{q}{v} \in I$$

(dato che I è un ideale e $q/v = q(1/v) \in R$). Quindi, $r/v \in I$ e, di conseguenza, $r \in I$. Per la scelta di n deve essere pertanto $r = 0$, il che mostra che $u/v = n(q/v) \in I$, provando così che $I = (n) = nR$.

6.41 Siano I e J ideali non nulli dell'anello commutativo R, e supponiamo che $I \cap J = \{0_R\}$. Prendiamo allora $0_R \neq x \in I$ e $0_r \neq y \in J$. Per la proprietà di assorbimento degli ideali $xy \in I \cap J$, e quindi $xy = 0_R$. Dunque R non è un dominio d'integrità.

6.42 Sia H ideale di R, e siano $x \in H$, $a \in \ker(f)$. Allora

$$f(x+a) = f(x) + f(a) = f(x) + 0_S = f(x) \in f(H)$$

e dunque $x + a \in f^{-1}(f(H))$, provando così che $H + \ker(f) \subseteq f^{-1}(f(H))$. Viceversa, sia $b \in f^{-1}(f(H))$. Allora $f(b) \in f(H)$, e quindi esiste $h \in H$ tale che $f(b) = f(h)$. Sia $c = b - h$; allora

$$f(c) = f(b) - f(h) = f(h) - f(h) = 0_S$$

e pertanto $c \in \ker(f)$. Dunque, $b = h + c \in H + \ker(f)$, provando l'altra inclusione.

6.46 Sia $0_r \neq a \in I$. Allora (a) è un ideale non banale di R contenuto in I e quindi, per la minimilità di I, $(a) = I$. Siano $x, y \in R \setminus \{0_R\}$, e supponiamo per assurdo $xy = 0_R$. Poiché $x \neq 0_R$, (x) è un ideale non banale, e quindi $(a) = I \subseteq (x)$. In particolare, esiste $u \in R$ tale che $a = xu$. Allo stesso modo si prova che esiste $v \in R$ tale che $a = yv$. Ma allora, essendo R commutativo,

$$a^2 = a \cdot a = (xu)(yv) = (xy)(uv) = 0_R(uv) = 0_R$$

contro una delle ipotesi su R. Dunque R è un dominio d'integrità. Inoltre $a^2 \neq 0_R$, e pertanto, per il consueto argomento, $(a^2) = (a)$. Quindi esiste $b \in R$ tale che $a = a^2b$, e da ciò segue

$$0_R = a^2b - a = a(ab - 1_R)$$

Siccome R è un dominio d'integrità, e $a \neq 0_R$, deve essere $ab - 1_R = 0_R$, ovvero $ab = 1_R$. Dunque a è invertibile, e quindi $I = (a) = R$. Poiché I è l'ideale non banale minimo, ne consegue che R ha i soli ideali $\{0_R\}$ ed R. Essendo commutativo, R è un campo.

6.48 Siano A ed I come definiti nel testo. Supponiamo che I sia un ideale; allora, poiché $1_A \notin I$, I è un ideale proprio. Proviamo che ogni altro ideale proprio J è contenuto in I. Sia $x \in J$; allora $(x) \subseteq J$, e quindi $1_A \notin (x)$. Da ciò segue che x non è invertibile, e dunque che $x \in I$, provando che $J \subseteq I$.
Viceversa, supponiamo che esista un ideale proprio T che contiene ogni ideale proprio di A, e proviamo che $T = I$ (e quindi I è un ideale). Sia $x \in I$. Allora x non è invertibile, e quindi $(x) \neq A$. Pertanto $(x) \subseteq T$, e dunque $x \in T$, provando che $I \subseteq T$. D'altra parte, essendo T un ideale proprio, nessuno dei suoi elementi è invertibile, e quindi $T \subseteq I$.

7.27 (a) La verifica che θ è un omomorfismo di anelli è facile. Determiniamo il suo nucleo. Sia $z \in \mathbb{Z}$; allora $z \in \ker(\theta)$ se e solo se $z + p\mathbb{Z} = 0_{\mathbb{Z}/p\mathbb{Z}}$ e $z + q\mathbb{Z} = 0_{\mathbb{Z}/q\mathbb{Z}}$, e quindi se e solo se $z \in p\mathbb{Z} \cap q\mathbb{Z}$. Ne segue che $\ker(\theta) = pq\mathbb{Z}$ se $p \neq q$, e $\ker(\theta) = p\mathbb{Z}$ se $p = q$.
(b) Sia $p \neq q$, e sia $(x + p\mathbb{Z},\, y + q\mathbb{Z}) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. Per il Teorema Cinese del Resto, esiste un intero z tale che

$$\begin{cases} z \equiv x \pmod{p} \\ z \equiv y \pmod{q} \end{cases}$$

Ma allora, $\theta(z) = (z + p\mathbb{Z},\, z + q\mathbb{Z}) = (x + p\mathbb{Z},\, y + q\mathbb{Z})$, provando così che θ è suriettiva. Se invece $p = q$, allora θ non è suriettiva. Infatti, non esiste alcun $z \in \mathbb{Z}$ tale che $\theta(z) = (0 + p\mathbb{Z},\, 1 + p\mathbb{Z})$ (dato che un tale z sarebbe congruo sia a 0 che ad 1 modulo p, il ché chiaramente non è possibile).

8.29 Siano I, K, $a \in A$ e $I_{(K,a)}$ come nel testo.
(a) Poiché $0_R \in I$, e $0_r a = 0_R \in K$, si ha $0_R \in I_{(K,a)}$. Se $x, y \in I_{(K,a)}$, allora $x - y \in I$ e $(x - y)a = xa - ya \in K$, e dunque $x - y \in I_{(K,a)}$. Infine se $x \in I_{(K,a)}$ e $r \in A$, allora $xr = rx \in A$, $xa \in K$ e, essendo A commutativo e K un ideale $(xr)a = (rx)a = r(xa) \in K$; dunque $xr = rx \in I_{(K,a)}$, completando la verifica che $I_{(K,a)}$ è un ideale di A.
(b) Sia $I = 3\mathbb{Z}$. Allora

$$I_{(4\mathbb{Z},2)} = 3\mathbb{Z}_{(4\mathbb{Z},2)} = \{x \in 3\mathbb{Z} \mid 2x \in 4\mathbb{Z}\} = \{3z \mid z \in \mathbb{Z} \text{ e } 4|6z\} = 6\mathbb{Z}.$$

(c) Osservo che, in generale, $I_{(K,a)} \subseteq I$, e che è chiaro che se $I \subseteq K$, oppure se $a \in K$, allora $I = I_{(K,a)}$. Supponiamo ora che A sia PID, e $K = (c)$ un suo ideale massimale.

Osserviamo che allora c è un elemento irriducibile di A; poiché A è un PID, c è un elemento primo.
Assumiamo $a \notin K$ (e dunque c non divide a). Allora, se $x \in I_{(K,a)}$, $xa \in K = (c)$, e dunque $c|xa$. Poiché c è primo e non divide a, deve essere $c|x$ e quindi $x \in K$. Pertanto, se $I = I_{(K,a)}$ e $a \notin K$, si ha $I \subseteq K$.

8.30 La verifica che $A = \mathbb{Z}[\sqrt{10}]$ è un anello commutativo è standard. Proviamo che l'ideale $(2, \sqrt{10})$ è primo. Siano $x = a + b\sqrt{10}$, $y = c + d\sqrt{10}$ elementi di A (quindi, $a, b, c, d \in \mathbb{Z}$). Allora

$$2x + \sqrt{10}y = 2a + 2b\sqrt{10} + c\sqrt{10} + 10d = 2a + 10d + (2b + c)\sqrt{10}.$$

Dunque, per l'esercizio precedente, si ha

$$(2, \sqrt{10}) = \{2x + \sqrt{10}y \mid x, y \in A\} = \{2u + t\sqrt{10} \mid u, t \in \mathbb{Z}\}.$$

In particolare, $1 \notin (2, \sqrt{10})$, e quindi $(2, \sqrt{10})$ è un ideale proprio.
Siano ora $x = a + b\sqrt{10}$, $y = c + d\sqrt{10} \in A$ tali che $xy \in (2, \sqrt{10})$. Allora

$$xy = ac + 10bd + (ad + bc)\sqrt{10} \in (2, \sqrt{10})$$

da cui, per quanto osservato prima intorno agli elementi di $(2, \sqrt{10})$, segue che $ac+10bd$ è un numero pari. Quindi $2|ac$. Ma allora a oppure c è un numero pari. Nel primo caso $x \in (2, \sqrt{10})$; ed altrimenti $y \in (2, \sqrt{10})$. In conclusione, $(2, \sqrt{10})$ è un ideale primo di A.

8.31 Sia R un dominio a fattorizzazione unica, e sia $0_R \neq a \in R$. Allora $a = r_1 r_2 \dots r_n$ con gli r_i irriducibili di R individuati a ameno di associati.

a) Sia (b) un ideale principale di R tale che $(a) \subseteq (b)$. Allora b divide a, e ciò significa che b è associato ad un prodotto di un sottoinsieme degli r_i. Poichè tali sottoinsiemi sono in numero finito, e i generatori degli ideali principali sono individuati a meno di associati, si deduce che il numero di ideali principali contenenti (a) è finito.

b) Sia $x \in \bigcap_{n\in\mathbb{N}}(a^n)$. Allora, chiaramente x non è invertibile. Supponiamo, per assurdo $x \neq 0_R$. Allora, per ogni $n \geq 1$, $a^n|x$, ed in particolare r_1^n divide x; ma ciò contraddice il fatto che x si fattorizzi in modo unico come un prodotto finito di elementi irriducibili. (Infatti, si può provare che se $I_1 \supset I_2 \supset I_3 \supset \cdots \supset I_k \supset \cdots$ è una catena discendente infinita di ideali *principali* di un dominio d'integrità R, allora $\bigcap_{n\in\mathbb{N}} I_n = \{0_R\}$.)

8.35 Sia R come nelle ipotesi. Osservo che, poiché (0_R) è un ideale primo, R è un dominio d'integrità. Sia $0_R \neq a \in R$. Allora, $a \cdot a = a^2 \in (a^2)$, e (a^2) è un ideale primo. Dunque $a \in (a^2)$, e pertanto esiste $b \in R$ tale che $a = a^2 b = a(ab)$. Siccome $a \neq 0_R$, e R è un dominio d'integrità, per la legge di cancellazione si ottiene $1_R = ab$. Dunque a è invertibile, e ciò prova che R è un campo.

8.41 Siano R, I e $K = K(I)$ come nel testo. Poiché $0_R \in K$, K non è vuoto. Se $x, y \in K$ e $r \in R$, allora, usando il fatto che in un anello commutativo di caratteristica 2 l'elevazione al quadrato è un omomorfismo, si ha

$$(x+y)^2 = x^2 + y^2 \in I \quad \text{e} \quad (xr)^2 = (rx)^2 = r^2x^2 \in I$$

e dunque $x + y \in K$, e $rx = xr \in K$, provando che K è un ideale.
Supponiamo ora che I sia un ideale primo, e che $x \in K$. Allora $x^2 = x \cdot x \in I$. Poiché I è primo si conclude che $x \in I$. Dunque $K \subseteq I$. Siccome l'inclusione opposta è ovvia, si ha $I = K$.

9.3 Sia $1 \leq n \in \mathbb{N}$. Allora, in $(\mathbb{Z}/4\mathbb{Z})[x]$ (denotando, per ogni $a \in \mathbb{Z}$, $\overline{a} = a + 4\mathbb{Z}$)

$$(\overline{2}x^n + \overline{1})(\overline{2}x^n + \overline{1}) = \overline{4}x^{2n} + \overline{1} = \overline{1},$$

e quindi, per ogni $n \geq 1$, $\overline{2}x^n + \overline{1}$ è invertibile in $(\mathbb{Z}/4\mathbb{Z})[x]$ (e coincide con il proprio inverso). Dunque in $(\mathbb{Z}/4\mathbb{Z})[x]$ esistono infiniti elementi invertibili.

9.10 Sia $f = 3x^4 + 4x^3 + ax^2 + ax + a$. Poiché $x^2 + 2x + 1 = (x+1)^2$, e $x + 1$ è irriducibile in $\mathbb{Q}[x]$, avremo che f e $x^2 + x + 1$ sono coprimi se e soltanto se tali sono f e $x + 1$, ovvero se e soltanto se $x + 1$ non divide f. Dividendo con resto f per $x + 1$, si ottiene

$$f = (x+1)(3x^3 + x^2 + (a-1)x + 1) + (a-1).$$

Dunque, f e $x + 1$ sono coprimi se e solo se $a \neq 1$.

9.12 Sia R un dominio d'integrità che non è un campo. Allora esiste un elemento $a \in R$ non nullo e non invertibile. Proviamo che (a, x) non è un ideale principale di $R[x]$. Osserviamo, innanzi tutto che $(a, x) \neq R$. Infatti, se fosse $1_R \in (a, x)$, allora (vedi esercizio 4.7) esistono $u, v \in R[x]$ tali che $1_R = au + xv$; il confronto tra i gradi comporta $au = 1_R$ e la contraddizione che a è invertibile in $R[x]$ (e quindi in R). Supponiamo, per assurdo, che $(a, x) = (g)$ per qualche $g \in R[x]$. Allora, in particolare, g divide a; poiché R è un dominio d'integrità, da ciò segue che $\deg g \leq \deg a = 0$, e quindi $g \in R$. D'altra parte g divide x, e ciò, come si vede facilmente, implica che g è un elemento invertibile di R. Ma allora, per un fatto noto, $(a, x) = (g) = R[x]$, contro quanto avevamo precedentemente stabilito.

9.30 In $\mathbb{Q}[x]$, $(f, g) = 1$. In $\mathbb{Z}_7[x]$, $(\overline{f}, \overline{g}) = x + \overline{3}$.

9.46 4) In $(\mathbb{Z}/3\mathbb{Z})[x]$: $x^5 - \overline{1} = (x - \overline{1})(x^4 + x^3 + x^2 + x + \overline{1})$.
In $(\mathbb{Z}/5\mathbb{Z})[x]$: $x^5 - \overline{1} = (x - \overline{1})^5$.
In $(\mathbb{Z}/11\mathbb{Z})[x]$: $x^5 - \overline{1} = (x - \overline{1})(x - \overline{3})(x - \overline{4})(x - \overline{5})(x - \overline{9})$.

9.47 Per ogni $h \in \mathbb{Z}$, f_h è un polinomio monico a coefficienti interi; dunque è irriducibile in $\mathbb{Q}[x]$ se e soltanto se è irriducibile in $\mathbb{Z}[x]$. Facendo i conti, si trova che f_h è irriducibile in $\mathbb{Z}[x]$ se e solo se $h \neq \pm 1$.

9.49 Proviamo, innanzi tutto, che la restrizione di Φ a X è iniettiva. Siano f e g in X tali che $\Phi(f) = \Phi(g)$. Allora, $f - g^* = \Phi(f - g) = \Phi(f) - \Phi(g)$ (questo si verifica immediatamente) è l'applicazione costante 0. Ciò significa che, per ogni $x \in \mathbb{Z}/p\mathbb{Z}$,

$$0 = f - g^*(x) = (f - g)(x) = 0,$$

ovvero x è una radice di $f - g$. Se $f - g$ fosse diverso dal polinomio nullo, allora, per il Teorema che segue quello di Ruffini, $deg(f - g) \geq p$, che è contrario alla definizione dell'insieme X. Dunque $f - g = 0$, cioè $f = g$, e pertanto Φ è iniettiva.
Ora, gli elementi di X si scrivono in modo unico nella forma $a_0 + a_1x + a_2x^2 + \ldots + a_{p-1}x^{p-1}$, con a_0, a_1, $a_2, \ldots,$ a^{p-1} elementi del campo $\mathbb{Z}/p\mathbb{Z}$, ognuno dei quali può essere scelto in p modi diversi. Dunque $|\Phi(X)| = |X| = p^p = |F^F|$. Pertanto, ogni elemento di F^F è una funzione polinomiale.

10.4 Sia F un campo e sia $0 \neq f = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in F[x]$. Supponiamo che $a_0 \neq 0_F$. Allora, posto $g = a_0^{-1}(a_nx^{n-1} + \ldots + a_2x + a_1)$, si ha

$$x \cdot (-g) = a_0^{-1}(a_0 - f) = 1_F - a_0^{-1}f$$

e quindi $(x + (f))(-g + (f)) = x(-g) + (f) = 1_F + (f)$, provando che $x + (f)$ è invertibile in $F[x]/(f)$. Viceversa, sia $x + (f)$ invertibile in $F[x]/(f)$. Allora esiste $h = b_0 + b_1x + \ldots + b_mx^m \in F[x]$, tale che $(x + (f))(h + (f)) = xh + (f) = 1_f + (f)$; ovvero $xh - 1 \in (f)$. facendo il conto

$$xh - 1 = -1 + b_0x + b_1x^2 + \ldots + b_mx^{m+1},$$

che è un multiplo di (f) solo se a_0 divide -1, e questo comporta $a_0 \neq 0_F$.

10.26 L'ideale $I = (f, g)$ è generato dal massimo comun divisore d di f e g. Si trova che

$$f = (x^2 + x - 6)(x^2 + 1) \quad \text{e} \quad g = (x^2 + x - 6)(x^3 - x - 2),$$

e poiché $x^2 + 1$ e $x^3 - x - 2$ sono irriducibili (e non associati) si conclude che $I = (d)$, dove

$$d = x^2 + x - 6 = (x - 2)(x + 3).$$

Siccome d è riducibile, I non è un ideale massimale di $\mathbb{Q}[x]$. Sia $h \in \mathbb{Q}[x]$ tale che $h + I$ è un divisore dello zero di $\mathbb{Q}[x]/I$. Per un risultato visto, posso supporre che $\deg h \leq 1$, dato che d ha grado 2. Quindi $h = ax + b$, con $a, b \in \mathbb{Q}$. Se $h + I$ è divisore dello zero, esiste un altro polinomio (che posso ancora assumere di grado al più 1) $t = cx + d$, tale che

$$th + I = (t + I)(h + I) = 0_{\mathbb{Q}[x]/I} = I$$

ovvero tale che $th \in I = (d)$, cioè $d|th$. Ma allora h e t sono divisori propri di grado al più uno di d e quindi sono associati a $x - 2$ oppure a $x + 3$.

10.27 (a) $f = x^4 + 4x^2 - 10$ è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein. Infatti $f \in \mathbb{Z}[x]$ ed il primo 2 divide tutti i coefficienti (tranne quello direttivo), e $2^2 = 4$ non divide il termine noto 10. Quindi $\mathbb{Q}[x]/(f)$ è un campo.

(b) In $(\mathbb{Z}/5\mathbb{Z})[x]$, si ha la riduzione

$$\overline{f} = x^4 + \overline{4}x^2 - \overline{10} = x^4 - x^2 = x^2(x^2 - \overline{1})$$

dunque $\overline{f}$ è riducibile in $(\mathbb{Z}/5\mathbb{Z})[x]$.

10.28 Sia $f = 1 - x^2$. Allora $f \in Y$. Sia quindi $g = b_0 + b_1x + \ldots + b_nx^n \in \mathbb{Q}[x]$; allora

$$fg = g - x^2g = b_0 + b_1x + (b_2 - b_0)x^2 + \ldots + (b_n - b_{n-2})x^n - b_{n-1}x^{n+1} - b_nx^{n+2}$$

e dunque, come si verifica facilmente, $fg \in Y$. Quindi $(f) \subseteq Y$.
Viceversa, sia $h = a_0 + a_1x + \ldots + a_nx^n \in Y$; allora $h(-1) = a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n = 0$, e dunque, per il teorema di Ruffini, $1 + x$ divide h. Inoltre $h(1) = a_0 + a_1 + a_2 + \ldots + a_n = 0 + 0 = 0$, e quindi anche $1 + x$ divide g. Di conseguenza, $f = (1 - x)(1 + x)$ divide g, ovvero $g \in (f)$. Quindi $Y \subseteq (f)$, e pertanto $Y = (f)$. Infine, poiché f non è irriducibile in $\mathbb{Q}[x]$, si conclude che $\mathbb{Q}[x]/Y$ non è un campo.

10.31 (a) VERA. (b) VERA. (c) FALSA.

10.32 Chiaramente $\sqrt{2} + \sqrt{7} \in \mathbb{Q}(\sqrt{2}, \sqrt{7})$, e quindi $\mathbb{Q}(\sqrt{2} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{7})$. Inoltre,

$$5 = 7 - 2 = (\sqrt{7} + \sqrt{2})(\sqrt{7} - \sqrt{2})$$

e quindi $\sqrt{7} - \sqrt{2} = 5(\sqrt{7} + \sqrt{2})^{-1} \in \mathbb{Q}(\sqrt{2} + \sqrt{7})$. Dunque

$$\sqrt{7} = \frac{(\sqrt{7} + \sqrt{2}) + (\sqrt{7} - \sqrt{2})}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{7}).$$

Similmente, $\sqrt{2} = (\sqrt{7} + \sqrt{2}) - \sqrt{7} \in \mathbb{Q}(\sqrt{2} + \sqrt{7})$. Dunque $\mathbb{Q}(\sqrt{2}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{7})$, e quindi $\mathbb{Q}(\sqrt{2}, \sqrt{7}) = \mathbb{Q}(\sqrt{2} + \sqrt{7})$.

10.33 (a) Per $h \in \mathbb{Z}$, E_h è un campo se e soltanto se $f_h = x^3 + hx^2 - hx + 2$ è irriducibile in $\mathbb{Q}[x]$. Poiché f_h è un polinomio monico a coefficienti interi, ed ha grado 3, esso è irriducibile in $\mathbb{Q}[x]$ se e soltanto se non ha radici in $\mathbb{Z}$. Ora, le eventuali radici intere di f_h sono divisori del suo termine noto 2. Dato che $f_h(1) = 3$, $f_h(-1) = 2h + 1$, $f_h(2) = 2h + 10$, e $f_h(-2) = 6h - 6$, si conclude che f_h è irriducibile (e quindi E_h è un campo) se e solo se $h \neq 1, -5$ (si tenga presente che $h \in \mathbb{Z}$).

(b) Gli elementi di E_2 sono del tipo $ax^2 + bx + c + (f_2)$, con $a, b, c \in \mathbb{Q}$. Facendo i conti, e tenendo conto che $x^3 + (f_2) = -2x^2 + 2x - 2 + (f_2)$, si trova che un tale $u \in E_2$ non esiste.

(c) Per $h = 1$ il polinomio f_1 si fattorizza $f_1 = (x^2 - x + 1)(x + 2)$, e E_1 non è un campo. Sia $I = (x^2 - x + 1)$. Allora $(f_1) \subseteq I$ (dato che $x^2 - x + 1$ divide f_1). In $\mathbb{Q}[x]/I$, sia $w = 2x - 1 + I$. Allora, tenendo conto che $x^2 + I = x - 1 + I$,

$$w^2 = (2x - 1)^2 + I = 4x^2 - 4x + 1 + I = 4(x - 1) - 4x + 1 + I = -3 + I$$

che è ciò che si voleva.

10.37 (a) Da $u+2=\sqrt[3]{5}$, segue $u^3+6u^2+12u+8=5$, e pertanto u è radice del polinomio

$$f=x^3+6x^2+12x+3.$$

f è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein, e dunque f è il polinomio minimo di u su $\mathbb{Q}$.

(b) Chiaramente, $\mathbb{Q}[u^2]\subseteq\mathbb{Q}[u]$. Viceversa, si ha $u^3=-6u^2-12u-3$, e quindi

$$u^4=-6u^3-12u^2-3u=36u^2+72u+18-12u^2-3u=24u^2+69u+18$$

e quindi

$$u=\frac{u^4-24u^2-18}{69}\in\mathbb{Q}[u^2].$$

Dunque $\mathbb{Q}[u]\subseteq\mathbb{Q}[u^2]$, e pertanto $\mathbb{Q}[u]=\mathbb{Q}[u^2]$.

(c) $u+2\in\mathbb{Q}[u]$ è una radice diversa da 1 del polinomio x^3-5.

10.43 (a) f è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein. La riduzione di f modulo 2 è x^4 che ovviamente è riducibile; quella modulo 3 è $x^4+x^3+\overline{1}$, che ammette $\overline{1}$ come radice e dunque è riducibile in $(\mathbb{Z}/3\mathbb{Z})[x]$. La riduzione di f modulo 5 è $x^4+\overline{4}x^3+\overline{3}=x^4-x^3+\overline{3}$, che ammette $-\overline{1}$ come radice, e dunque è riducibile in $(\mathbb{Z}/5\mathbb{Z})[x]$.

(b) Sia $\alpha\in\mathbb{C}$ una radice di f. Allora $\alpha^4-2=-4\alpha^3$, e quindi, elevando al quadrato, $\alpha^8-4\alpha^4+4=16\alpha^6$, e dunque α^2 è radice del polinomio $g=x^4-16x^3-4x^2+4\in\mathbb{Q}[x]$. Con il solito metodo (cioè valutando g nei divisori interi di 4), si prova che g non ha radici in $\mathbb{Q}$, e quindi che g non ha fattori di grado 1 (oppure 3) in $\mathbb{Q}[x]$. Supponiamo che g si decomponga nel prodotto di due fattori di grado 2 in $\mathbb{Q}[x]$. Allora uno di questi, sia x^2+ax+b, ammette α^2 come radice; ovvero $\alpha^4+a\alpha^2+b=0$. Ciò significa che α è radice di $h=x^4+ax^2+b$. Dunque f, che è il polinomio minimo di α su $\mathbb{Q}$, deve dividere h; siccome f e h sono entrambi monici, si deve avere $h=f$, il che non è possibile. In conclusione, g è irriducibile in $\mathbb{Q}[x]$, e partanto è il polinomio minimo di α^2 su $\mathbb{Q}$.

10.44 È sufficiente provare che se f è irriducibile, allora $Rew(f)$ è irriducibile. Supponiamo che g sia un fattore irriducibile di $Rew(f)$, di grado n, e sia $a\in\mathbb{C}$ una radice di g (esiste per il teorema fondamentale dell'algebra). Allora il grado di $\mathbb{Q}(a)$ su $\mathbb{Q}$ è uguale a n. D'altra parte si verifica facilmente che, poiché a è radice di $Rew(f)$, $a\neq 0$ (dato che il termine noto di $Rew(f)$ è $a_n\neq 0$), e che a^{-1} è radice di f. Essendo f irriducibile, f è il polinomio minimo di a^{-1} su $\mathbb{Q}$. Ma, chiaramente, $\mathbb{Q}(a^{-1})=\mathbb{Q}(a)$, e quindi il grado del polinomio minimo di a^{-1} è uguale al grado del polinomio minimo di a, che è n. Dunque $n=\deg(f)=\deg(Rew(f))$, e quindi $Rew(f)=g$ è irriducibile.

10.50 La sola radice di x^5-1 nel campo E (comunque sia stato costruito, purché abbia ordine 27) è 1_E.