Geometria

22 giugno 2015

Capitolo 1

Gruppi e anelli

1.1 Gruppi

Definizione 1.1.1. *Si definisce* gruppo *un insieme G non vuoto munito di un'operazione binaria interna $*\colon G \times G \to G$, ossia tale per cui sono rispettati gli assiomi seguenti:*

1. *vale la proprietà associativa, cioè $\forall g_1, g_2, g_3 \in G$ vale $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$;*
2. *esiste l'elemento neutro, cioè $\exists e \in G\colon \forall g \in G$, $g * e = e * g = g$;*
3. *esiste l'inverso, ossia $\forall g \in G\ \exists g' \in G\colon g * g' = g' * g = e$.*

Dove non ci saranno ambiguità, d'ora in poi indicheremo l'operazione interna del gruppo come una moltiplicazione, omettendo il simbolo $*$: scriveremo dunque $x * y = xy$. L'inverso di un elemento x sarà indicato, coerentemente, con x^{-1}.

La struttura di gruppo si compone sempre di un insieme e di un'operazione, perciò si identifica convenzionalmente con la coppia $(G, *)$; uno insieme può formare gruppi differenti in base all'operazione associata. Il gruppo è detto *commutativo* (o *abeliano*) se vale anche la proprietà commutativa, cioè $\forall x, y \in G$, $xy = yx$.

L'elemento neutro di un gruppo è sempre unico: se e ed e' rispettano la seconda proprietà, allora $e' = ee' = e$ quindi coincidono. Lo stesso vale per l'inverso, dato $x \in G$: se a e b sono due inversi di x, allora

$$b = eb = (ax)b = a(xb) = ae = a. \tag{1.1.1}$$

Elenchiamo di seguito alcuni esempi, più o meno immediati, di gruppi.

- Gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con l'usuale operazione di addizione. Più in generale, gli elementi di un campo qualsiasi formano un gruppo rispetto all'addizione.
- Gli insiemi $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$, privati dello zero, con l'usuale moltiplicazione. Lo stesso accade per gli elementi non nulli di un campo qualsiasi: dato un campo K, saremo soliti indicare il gruppo moltiplicativo $(K \setminus \{0\}, \cdot)$ con il simbolo $K^\times$.
- Le rotazioni in un piano, con l'operazione di composizione, che è anche abeliano.
- Le rotazioni in $\mathbb{R}^3$, sempre con la composizione, sono ancora un gruppo. Esso però non è abeliano, perché due rotazioni effettuate rispetto ad assi differenti in generale non commutano.
- L'insieme $\{-1, 1\}$ forma un gruppo rispetto alla moltiplicazione.

Definizione 1.1.2. *Un sottoinsieme H di un gruppo G è detto* sottogruppo *di G se è a sua volta un gruppo con l'operazione di G.*

In altre parole, H è un gruppo contenuto in un gruppo più grande. Questa definizione equivale alle richieste:

1. H deve essere chiuso rispetto all'operazione del gruppo G, ossia se $a, b \in H$ allora $ab, ba \in H$;
2. ogni elemento di H deve avere il suo inverso in H.

Di conseguenza, H deve anche contenere l'elemento neutro (lo stesso!) di G, poiché se $x \in H$, allora anche x^{-1} vi appartiene, dunque anche $xx^{-1} = e$.

Ogni gruppo ammette sempre due sottogruppi: il gruppo stesso e il *sottogruppo banale* $\{e\}$ del suo elemento neutro. Gli altri sottogruppi, se esistono, sono detti *propri*. Se un gruppo è abeliano, allora anche tutti i suoi sottogruppi lo sono. Alcuni esempi di sottogruppi sono i seguenti.

- L'insieme $\mathbb{T} = \{z \in \mathbb{C} \colon |z| = 1\}$, detto *gruppo circolare*, è un sottogruppo di $\mathbb{C}^\times$. Poiché $\mathbb{C}^\times$ è abeliano, lo è anche $\mathbb{T}$.
- In $\mathbb{R}^2$, sia $R(\theta)$ la rotazione antioraria di un angolo θ. L'insieme $\{R(0), R(\pi/2), R(\pi), R(3\pi/2)\}$ è un sottogruppo del gruppo delle rotazioni nel piano.

1.2 Relazioni di equivalenza

Una relazione binaria su un insieme X lega due elementi dell'insieme. Essa si definisce come un sottoinsieme di $X \times X$, intendendo che due elementi a, b sono messi in relazione da R se $(a, b) \in R$. Solitamente una relazione di questo tipo si indica con il simbolo $\sim$, cioè $a \sim b$.

Definizione 1.2.1. *La relazione $\sim$ è una relazione di equivalenza su X se è binaria e valgono le seguenti proprietà:*

1. *è riflessiva: $a \sim a$;*
2. *è simmetrica: se $a \sim b$, allora $b \sim a$;*
3. *è transitiva: se $a \sim b$ e $b \sim c$, allora anche $a \sim c$.*

Con questa relazione di equivalenza possiamo "raggruppare" gli elementi di X in vari insiemi di elementi tutti in relazione tra loro. Vediamo se questa suddivisione è buona, cioè se un elemento è categorizzato in uno solo di questi insiemi o meno.

Definizione 1.2.2. *Si chiama* classe di equivalenza *di un elemento $a \in X$, rispetto alla relazione $\sim$, l'insieme*

$$[a] = \{b \in X \colon b \sim a\}.$$

L'elemento a è detto rappresentante *della classe $[a]$.*

Teorema 1.2.3. Due classi di equivalenza, rispetto alla relazione $\sim$, $[a]$ e $[a']$ coincidono se e solo se $a \sim a'$.

Dimostrazione. Siano le due classi $[a] = \{x \in X \colon x \sim a\}$ e $[a'] = \{y \in X \colon y \sim a'\}$. Sia $[a] \subseteq [a']$: preso un elemento $x \in [a]$, si ha ovviamente che $x \sim a$. Poiché $a \sim a'$, per la proprietà transitiva $x \sim a'$ quindi $x \in [a']$, e viceversa per simmetria: allora $[a] \equiv [a']$. Poniamo ora le due classi coincidenti, siccome $a \in [a]$ e $a' \in [a']$, poichè le due classi coincidono si ha che a appartiene anche ad $[a']$ e a' appartiene anche ad $[a]$, quindi $a \sim a'$. □

Teorema 1.2.4. Due classi di equivalenza sono distinte se e solo se sono disgiunte: se $[a] \neq [b]$ allora $[a] \cap [b] = \varnothing$.

Dimostrazione. Sia per assurdo che esista un elemento $c \in [a] \cap [b]$. Allora esso è in relazione sia con a che con b, ma allora per la proprietà transitiva $a \sim b$, quindi le due classi coincidono, il che è una contraddizione. Le due classi devono quindi essere disgiunte. □

Le classi distinte individuate da una relazione di equivalenza in X costituiscono una partizione di X.

Definizione 1.2.5. *Sia $\{S_i\}_{i\in I}$ una famiglia di sottoinsiemi di un insieme X. Tale famiglia si dice* partizione *di X se:*

- $S_i \neq \varnothing\ \forall i \in I$;
- $S_i \cap S_j = \varnothing$ *per ogni* $i \neq j$;
- $\bigcup_{i\in I} S_i \equiv X$.

Sia $\{S_i\}_{i\in I}$ una partizione di un insieme X: si può sempre definire una relazione di equivalenza $\sim$ su X, ponendo che $\forall a, b \in X$, $a \sim b$ se e solo se $\exists i \in I : a, b \in S_i$. Una tale relazione soddisfa la definizione di relazione di equivalenza:

1. Qualsiasi $a \in X$ sta in almeno uno dei sottoinsiemi S_i, per il terzo punto della 1.2.5, quindi $a \sim a$.
2. Se esiste un $i \in I$ per cui $a, b \in S_i$, certamente scambiando l'ordine di b e a entrambi appartengono comunque a S_i, quindi se $a \sim b$ anche $b \sim a$.
3. Se $a \sim b$ e $b \sim c$, allora esiste $i \in I$ per il quale $a, b \in S_i$ ed esiste un altro indice $j \in I$ per cui $b, c \in S_j$. Se $i \neq j$, però, b non potrebbe appartenere ad entrambi perché la loro intersezione sarebbe vuota. Allora $i = j$, e per tale indice $a, b, c \in S_i$ (o S_j), quindi $a \sim c$.

1.3 Anelli

Definizione 1.3.1. *Un insieme non vuoto A, dotato di due operazioni binarie interne $*$ e $\diamond$, si dice anello se valgono le seguenti proprietà:*

1. *$(A, *)$ è un gruppo abeliano;*
2. *$(A, \diamond)$ è un semigruppo, cioè è solo associativo;*
3. *$\forall a, b, c \in A$ valgono $(a * b) \diamond c = (a \diamond c) * (b \diamond c)$ e $a \diamond (b * c) = (a \diamond b) * (a \diamond c)$.*

Intenderemo sempre che la seconda operazione avrà sempre la precedenza sulla prima, se non diversamente specificato: vale a dire, $x * y \diamond z$ significherà $x * (y \diamond z)$; in caso contrario si usano le parentesi dove necessario. D'ora in poi, per mantenere una notazione più familiare e semplice, ci riferiremo all'operazione $*$ come ad un'*addizione* (e la indicheremo con $+$), e all'operazione $\diamond$ come ad una *moltiplicazione*. Infatti l'addizione e la moltiplicazione che tutti conosciamo soddisfano questi assiomi, che comunque possono essere generalizzati ad operazioni differenti, come il prodotto tra polinomi o matrici.

L'anello si dice *commutativo* se anche $(A, \cdot)$ è commutativo, cioè $ab = ba\ \forall a, b \in A$; la commutatività dell'addizione è sempre garantita dal fatto che $(A, +)$ è abeliano. L'elemento neutro dell'addizione in un anello esiste sempre, dato che $(A, +)$ è un gruppo: indicheremo tale elemento con 0, o con 0_A se ci sarà bisogno di specificare l'anello al quale appartiene. L'esistenza dell'elemento neutro della moltiplicazione, invece, non è data per certa: se esiste, l'anello si dice *dotato di unità*, e la indicheremo con 1 o 1_A.

Ecco alcuni esempi di anelli.

- $\mathbb{Z}$ è un anello con le usuali operazioni di addizione e moltiplicazione, come del resto $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e ogni altro campo.
- L'insieme $K[x]$ dei polinomi (di grado qualunque) con termini presi da un campo K forma un anello con le note operazioni di somma e prodotto tra polinomi.

Definiamo per $n \in \mathbb{Z}$ l'addizione di a con se stesso $n - 1$ volte come

$$na = \underbrace{a + a + \cdots + a}_{n \text{ volte}}, \tag{1.3.1}$$

per $n \in \mathbb{N}$, e con $0a = 0_A$; per $n < 0$, basta porre $na = -(-n)a$ per ricondursi ai casi precedenti. Definiamo poi a moltiplicato con se stesso $n-1$ volte come

$$a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ volte}} \tag{1.3.2}$$

con $n > 0$, e (se esiste l'unità) $a^0 = 1_A$. Per $n < 0$ questa operazione non è definita.

Ricaviamo alcune semplici proprietà delle due operazioni.

- $0_A a = a 0_A = 0_A$. Possiamo infatti scrivere sempre $0_A a = (0_A + 0_A)a$, e per la proprietà distributiva abbiamo $0_A a = 0_A a + 0_A a$, per cui aggiungendo l'opposto $-0_A a$ ai due membri (esiste sempre, essendo $(A, +)$ un gruppo) troviamo $0_a a = 0$. La dimostrazione è analoga per $a0_A$.

- $(na)b = a(nb) = n(ab)$, che di dimostra facilmente sfruttando la proprietà distributiva partendo da $(a + a + \cdots + a)b$.

- $a(-b) = (-a)b = -(ab)$, ponendo $n = -1$ nella precedente.

Definizione 1.3.2. *Un elemento $a \neq 0_A$ di un anello A si dice* divisore dello zero *se esiste un elemento $b \in A$ tale che $ab = 0_A$ oppure $ba = 0_A$.*

Ovviamente i due casi coincidono se l'anello è commutativo, ma in generale non lo si può affermare.

Esempi

- L'insieme $\mathscr{C}(-1, 1)$ delle funzioni $f\colon (-1, 1) \to \mathbb{R}$ continue è un anello con addizione e moltiplicazione. In esso, definiamo le funzioni

$$f(x) = \begin{cases} 0 & -1 < x < 0 \\ x^2 & 0 \leq x < 1 \end{cases} \qquad \text{e} \qquad g(x) = \begin{cases} x^2 & -1 < x < 0 \\ 0 & 0 \leq x < 1 \end{cases}$$

  La f è un divisore dello zero, in quanto g non è la funzione identicamente nulla di $\mathscr{C}(-1, 1)$, ma $fg = 0$ per ogni $x \in (-1, 1)$. Per lo stesso motivo, ovviamente, anche g è divisore dello zero.

Teorema 1.3.3. Un anello A è privo di divisori dello zero se e solo se valgono le leggi di cancellazione per il prodotto.[1]

Dimostrazione. Supponiamo che A sia un anello privo di divisori dello zero, e prendiamo l'ipotesi $ax = ay$: dalla proprietà distributiva si ha $a(x - y) = 0$. Dato che non esistono divisori dello zero in A, se $a \neq 0$ deve necessariamente essere $x - y = 0$, ossia $x = y$. La dimostrazione per $xa = ya \Rightarrow x = y$ è del tutto analoga.

Partiamo ora dalle relazioni $ax = ay \Rightarrow x = y$ e $xa = ya \Rightarrow x = y$. Se esistessero $x, y \neq 0$ tali che $xy = 0$ (ossia x e y divisori dello zero), allora risulterebbe anche $xy = 0 = x0$ da cui $y = 0$, poiché valgono le leggi di cancellazione del prodotto. Ma ciò contraddice l'ipotesi che $x, y \neq 0$ quindi tali x e y non possono esistere: allora A è privo di divisori dello zero. □

Definizione 1.3.4. *Sia A un anello con unità. Un elemento $a \in A$ si dice* invertibile *se esiste $b \in A$ tale per cui $ab = ba = 1$. Tale b si indica con a^{-1}.*

Teorema 1.3.5. Se A è un anello dotato di unità, i suoi elementi invertibili non sono divisori dello zero.

[1] Ossia se per ogni $a, x, y \in A$ con $a \neq 0$ le relazioni $ax = ay$ e $xa = ya$ implicano $x = y$.

Dimostrazione. Se esistesse un elemento $a \in A$ invertibile e divisore dello zero, allora esisterebbe un elemento $b \in A \setminus \{0\}$ tale che $ab = 0$. Si ottiene però che

$$b = 1b = a^{-1}ab = a^{-1}0 = 0 \tag{1.3.3}$$

ossia $b = 0$, che contraddice l'ipotesi $b \neq 0$ legata all'esistenza di b. Dunque non può esistere un tale b: vale a dire, a non è un divisore dello zero. □

Definizione 1.3.6. *Un anello si dice* dominio d'integrità *se è commutativo ed è privo di divisori dello zero.*

Sono domini d'integrità gli anelli di $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con le usuali operazioni di somma e prodotto.

Definizione 1.3.7. *Si chiama* corpo *un anello dotato di unità in cui ogni elemento non nullo è invertibile.*

Definizione 1.3.8. *Si dice* campo *un corpo commutativo con almeno due elementi.*

Il piccolo teorema di Wedderburn afferma, inoltre, che ogni corpo finito è un campo. Possiamo dare una definizione alternativa di campo, equivalente alla precedente, basata su degli assiomi.

Definizione 1.3.9. *Si definisce* campo *la terna $(K, +, \cdot)$ in cui K è un insieme non vuoto e $+$ e $\cdot$ sono operazioni interne $K \times K \to K$, per le quali:*

- *$(K, +)$ è un gruppo abeliano, con elemento neutro 0_K;*
- *$(K \setminus \{0_K\}, \cdot)$ è un gruppo abeliano, con elemento neutro 1_K;*
- *vale la proprietà distributiva, per cui $\forall a, b, c \in K$ vale $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Questa definizione è in sostanza una generalizzazione della struttura di $(\mathbb{R}, +, \cdot)$. È quindi, ovviamente, un campo $(\mathbb{R}, +, \cdot)$, e lo sono anche $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.

1.4 Ideali

Definizione 1.4.1. *Sia A un anello e I un suo sottoinsieme. Se $(I, +)$ è un sottogruppo di $(A, +)$ e per ogni $x \in I$ e $a \in A$:*

- *$ax \in I$, allora I è detto* ideale sinistro*;*
- *$xa \in I$, allora I è detto* ideale destro*;*
- *$ax, xa \in I$, allora I è detto* ideale bilatero*.*

In altre parole, preso un elemento di un ideale sinistro (destro) possiamo moltiplicarlo a sinistra (destra) per qualsiasi elemento dell'anello e ottenere ancora un elemento dell'ideale. Nel caso di un anello commutativo, le tre definizioni naturalmente coincidono, e parleremo semplicemente di *ideale*.

Dalla chiusura di I rispetto alla somma otteniamo inoltre che qualsiasi ideale deve sempre contenere lo zero dell'anello. Ogni anello ammette sempre due ideali detti *banali*: $\{0\}$ e l'anello A stesso. Gli ideali non banali sono detti *propri*. Se l'anello è dotato di unità, allora un ideale è proprio se e solo se non la contiene: se infatti $I \ni 1$, allora poiché il prodotto $1a$ per qualsiasi a nell'intero anello deve essere incluso in I, tale ideale contiene tutti gli elementi di A, ma allora $I = A$.

Degli esempi importanti di ideali, che incontreremo in seguito, sono i seguenti.

- Dato $p \in \mathbb{Z}$, chiamiamo $p\mathbb{Z}$ l'insieme $\{x \in \mathbb{Z} \colon x = np, n \in \mathbb{Z}\}$ ossia l'insieme dei multipli interi di un certo intero p. Se $x, y \in p\mathbb{Z}$, siano essi $x = np$ e $y = mp$, allora $x + y = (n + m)p$ e poiché $n + m \in \mathbb{Z}$ allora $x + y \in p\mathbb{Z}$. Per un qualunque $z \in \mathbb{Z}$, inoltre, $xz = npz = (nz)p$ e $nz \in \mathbb{Z}$ quindi $xz \in p\mathbb{Z}$. L'insieme $p\mathbb{Z}$ è dunque un ideale di $\mathbb{Z}$, per qualunque p.

- I numeri pari formano l'insieme $2\mathbb{Z}$, che è un ideale per il punto precedente. I numeri dispari, invece, non formano un ideale, in quanto non comprendono lo zero.
- Nell'anello delle funzioni continue $\mathscr{C}(\mathbb{R})$, è un ideale l'insieme delle funzioni che si annullano in un dato punto, ad esempio per cui $f(1) = 0$.

Definiamo ora alcuni tipi particolari di ideali (per semplicità, le daremo per anelli commutativi).

Definizione 1.4.2. *Un ideale I di un anello A è detto* primo *se:*

- *è un sottoinsieme proprio di A;*
- *se $a, b \in A$ sono tali che $ab \in I$, allora almeno uno dei due appartiene a I.*

Questo concetto ricalca la definizione di *numeri primi*: se un numero $p \in \mathbb{Z}$ è primo, ogni volta che divide un prodotto xy con $x, y \in \mathbb{Z}$ allora p divide a oppure b. Le due definizioni sono in effetti collegate: un numero intero (positivo) n è primo se e solo se $n\mathbb{Z}$ è un ideale primo.

Definizione 1.4.3. *Un ideale A si dice* massimale *se $I \neq A$, per ogni ideale $J \supseteq I$ si ha o che $J = I$ oppure $J = A$.*

Gli ideali massimali sono dunque degli elementi massimali rispetto all'operazione di inclusione insiemistica tra gli *ideali propri* di un anello (escludendo quindi dalle opzioni l'anello stesso). Essi non sono contenuti propriamente in nessun altro ideale proprio dell'anello.

Se ogni elemento x di un ideale I, di un anello A, può essere scritto come

$$x = \sum_{i=1}^{n} a_k i_k$$

con $a_k \in A$ e $i_k \in I$, ossia come combinazione lineare di un numero finito di suoi elementi $\{i_k\}_{k=1}^{n}$, diciamo che l'ideale è *generato* da tali elementi, e si indica solitamente come $I = (i_1, \ldots, i_n)$. Il caso in cui l'ideale è generato da un solo elemento è di particolare importanza, e merita una sua definizione.

Definizione 1.4.4. *Un ideale I di un anello A si dice* principale *se è generato da un solo elemento.*

In linea con la notazione precedente, l'ideale principale generato da a si indica con (a). Si può dimostrare che l'ideale principale (a) è il più piccolo ideale che comprende a.

1.5 Anelli quoziente

Riprendiamo ora le relazioni di equivalenza, introdotte nel capitolo 1.2. Dati un ideale (bilatero) I di un anello A e due elementi $a, b \in A$, stabiliamo la relazione

$$a \sim b \Leftrightarrow a - b \in I.$$

È facile vedere, con le proprietà degli ideali, che tale relazione è anche di congruenza. Se $a \sim b$ si dice anche che a e b sono *congruenti modulo I*. Da essa possiamo costruire le classi di equivalenza nell'anello: la classe $[a]_I$ (indichiamo con il pedice $[\cdot]_I$ il fatto che la relazione è basata sull'ideale I, per maggiore chiarezza) consiste in tutti quegli elementi x di A che "distano a dall'ideale I", ossia tali per cui $x - a \in I$. Alternativamente, gli elementi $x \in [a]_I$ sono la somma di a e di un elemento dell'ideale I, e per questo motivo si indica la classe di equivalenza come $I + a$. Formalmente, dunque,

$$[a]_I = I + a = \{x \in A \colon x = a + i, i \in I\}.$$

Possiamo definire delle operazioni su queste classi come di seguito:

- l'addizione di $[a]_I = I + a$ e $[b]_I = I + b$ come la classe di rappresentante $a + b$, ossia $I + (a + b)$;

- analogamente, la moltiplicazione di due classi $[a]_I[b]_I = (I+a)(I+b)$ come la classe che ha come rappresentante il prodotto dei due rappresentanti, ossia $I+ab$.

Si può verificare che queste operazioni sono ben definite, ossia che non dipendono dalla scelta dei rappresentanti. Con queste due operazioni, l'insieme delle classi di equivalenza forma un anello, detto *anello quoziente* (rispetto alla relazione stabilita).

Definizione 1.5.1. *Dato un ideale bilatero I di un anello A, si chiama* anello quoziente *l'insieme, indicato con A/I, delle classi di equivalenza $[a]_I = \{x \in A \colon x = a+i, i \in I\}$, con le operazioni*

$$\begin{aligned}(I+a)+(I+b) &= I+(a+b)\\ (I+a)(I+b) &= I+ab.\end{aligned} \tag{1.5.1}$$

Lo zero dell'anello quoziente è indicato come $I+0$, ed è chiaramente l'ideale I stesso. Notiamo che se $a \in I$, allora $I+a$ è ancora lo zero di A/I: infatti, essendo I chiuso rispetto alla somma, l'addizione di un elemento dell'ideale (cioè I) con a (che è in I) produce ancora un elemento nell'ideale, vale a dire un elemento di $I = I+0$. L'identità moltiplicativa, se esiste, sarà indicata con $I+1$.

Proviamo a prendere il quoziente di A con gli ideali banali.

- Per $I = \{0\}$, scelto un $a \in A$ abbiamo che $b \in [a] = I+a$ se $b-a \in I$, cioè $b-a = 0$: ma ciò è possibile solo se $b = a$, dunque $I+a = \{a\}$ per qualsiasi $a \in A$.
- Per $I = A$, se $b \in I+a$ dovrà essere $b-a \in A$: questo è sempre vero qualsiasi sia b, quindi $I+a = A$ per qualsiasi a! Ciò significa che A/A è composto da un solo elemento.

L'ideale $I = 2\mathbb{Z}$ di $\mathbb{Z}$ è massimale: infatti se un ideale J contiene I, allora $J = k\mathbb{Z}$ per un $k \in N$ che sia divisore di 2. Ma allora $k \in \{1,2\}$, cioè $k\mathbb{Z}$ è ancora $2\mathbb{Z}$ oppure è tutto $\mathbb{Z}$. Perciò $2\mathbb{Z}$ è un ideale massimale; lo stesso di dimostra per qualsiasi $p\mathbb{Z}$ con p primo. Questo risultato si generalizza nel seguente teorema.

Teorema 1.5.2. Sia A un anello commutativo con unità e sia $I \subset A$ un ideale proprio: allora I è primo se e solo se A/I è un dominio d'integrità.

Dimostrazione. Supponiamo che A/I sia un dominio di integrità, per cui prese due classi $I+a$ e $I+b$, se $I+ab = I+0$ deve necessariamente risultare $I+a = I+0$ oppure $I+b = I+0$. Passando dalle classi di A/I agli elementi di A, il fatto che $I+ab$ sia $I+0$ significa che ab è nell'ideale I. Analogamente se $I+a = I+0$ significa che $a \in I$. Ma ciò vuol dire che se $ab \in I$ allora uno dei due tra a e b è necessariamente nell'ideale: questa è proprio la definizione di ideale primo, quindi I è primo.

Sia ora I un ideale primo: se $ab \in I$, almeno uno tra a e b deve appartenere a I. Nel linguaggio delle classi di equivalenza ciò significa che se $(I+a)(I+b) = I+ab = I+0$, allora $I+a = I+0$ oppure $I+b = 0$. Queste affermazioni sono equivalenti a dire che non esistono $a, b \notin I$ tali che $ab \in I$, cioè

$$\nexists I+a, I+b \in A/I \colon (I+a)(I+b) = I+0$$

quindi A/I è un dominio di integrità. □

Teorema 1.5.3. Sia A un anello commutativo con unità e sia $I \subset A$ un ideale proprio: I è massimale se e solo se A/I è un campo.

Dimostrazione. Sia I un ideale massimale: allora non può esistere un ideale J tale che $I \subset J \subset A$. Dimostriamo che A/I è un campo mostrando che ogni suo elemento non nullo è invertibile. Sia $I+a$ un elemento non nullo di A/I, ossia deve essere $a \notin I$. Fissato questo elemento, costruiamo l'insieme $J_a = \{j \in A \colon j = i+ax, i \in I, x \in A\}$. Sicuramente, poiché A è commutativo, lo è anche J_a. Inoltre è anche un ideale: infatti, dati $j_1 = i_1 + ax_1$, $j_2 = i_2 + ax_2$ e $b \in A$ abbiamo

$$\begin{aligned}j_i + j_2 &= \underbrace{i_1+i_2}_{\in I} + a(\underbrace{x_1+x_2}_{\in A}) \in J_a;\\ j_1 b = (i_1+ax_1)b &= \underbrace{i_1 b}_{\in I} + a(\underbrace{x_1 b}_{\in A}) \in J_a.\end{aligned} \tag{1.5.2}$$

Tutti gli elementi $i \in I$ sono della forma $i + a0$, dunque $I \subseteq J$. Esistono anche elementi di J che non appartengono a I? Dato che I è proprio, non può contenere l'unità, come avevamo già visto. Allora l'elemento $i + a1 = i + a$ appartiene a J, ma non a I.[2] Di conseguenza $I \subset J$: per la massimalità di I, però, ciò implica $J \equiv A$. Perciò J deve contenere l'unità, che potremo dunque scrivere come $i^* + ax^*$ per qualche $i^* \in I$ e $x^* \in A$. Preso questo x^*, vediamo che la classe $I + x^* \in A / I$ è l'inverso di $I + a$:

$$(I + x^*)(I + a) = I + ax^* = I + (1 - i^*) = I + 1 \tag{1.5.3}$$

poiché se $i^* + ax^* = 1$ allora $ax^* = 1 - i^*$, e $I - i^* = I$. Ma $I + 1$ è l'unità di A / I, dunque ogni elemento non nullo (ossia con $a \notin I$) di A / I ammette un inverso: ciò prova che A / I è un campo.

Sia ora A / I un campo: allora, poiché deve possedere almeno due elementi, I non può essere uguale ad A, perché come abbiamo già visto A / A contiene un solo elemento. Dunque I è un ideale proprio. Prendiamo ora un ideale J tale che $I \subseteq J \subseteq A$ con $I \neq J$. Esiste dunque un x che appartiene a J ma non a I, di conseguenza $I + x \neq I + 0$. Non essendo l'elemento nullo di A / I, che per ipotesi è un campo, $I + x$ è invertibile: esiste una classe $I + y \in A / I$ tale per cui

$$I + 1 = (I + y)(I + x) = I + xy,$$

quindi $xy = 1 + i^*$ per qualche $i^* \in I$. Ora, $I \subseteq J$, perciò $i^* \in J$, e analogamente $x \in J$ quindi anche $xy \in J$: ma allora anche $1 = xy - i^*$ appartiene a J. Dato che J contiene l'unità, segue necessariamente che $J = A$, perciò I è massimale. □

Corollario 1.5.4. In un anello commutativo con unità, ogni ideale massimale è primo.

Dimostrazione. Se I è massimale, per il teorema 1.5.3 A / I è un campo, quindi in particolare è anche un dominio di integrità: ma allora dal teorema 1.5.2 I è primo. □

L'implicazione inversa, ossia che ogni ideale primo è massimale, in generale è falsa (il problema sta nell'affermazione "un campo è un dominio d'integrità", che non si può invertire). Vedremo in che ambito essa è vera quando introdurremo i domini *a ideali principali*.

1.6 Omomorfismi di anelli

Definizione 1.6.1. *Siano $(A, +, \cdot)$ e $(B, *, \diamond)$ due anelli: un* omomorfismo *di anelli è un'applicazione $\varphi\colon A \to B$ che preserva le operazioni, cioè tale che per ogni $a, b \in A$ si ha*

$$\varphi(a + b) = \varphi(a) * \varphi(b) \text{ e } \varphi(ab) = \varphi(a) \diamond \varphi(b). \tag{1.6.1}$$

Se gli anelli sono dotati di unità, si richiede che l'omomorfismo, oltre alle operazioni, preservi anche l'unità, ossia $\varphi(1_A) = 1_B$.

Ad esempio la funzione da $\mathbb{Z}$ in sé definita come $\varphi(a) = 0$ per qualsiasi $a \in \mathbb{Z}$, cioè che porta qualsiasi elemento nello zero, chiaramente preserva le operazioni, ma non è un omomorfismo d'anelli in quanto $\varphi(1) = 0$ che ovviamente non è l'unità di $\mathbb{Z}$.

Definizione 1.6.2. *Sia $\psi\colon A \to B$ un omomorfismo di anelli. Si definisce* nucleo *di ψ e si denota con* $\operatorname{Ker} \psi$ *l'insieme*

$$\operatorname{Ker} \psi = \{a \in A\colon \psi(a) = 0_B\},$$

ossia l'insieme degli elementi di A che hanno lo zero di B come immagine.

Teorema 1.6.3. Se $\psi\colon A \to B$ è un omomorfismo di anelli, allora il suo nucleo è un ideale di A.

[2] Se $i + a \in I$, ossia $i + a = i'$ per qualche $i' \in I$, allora seguirebbe che $a = i' - i$, cioè $a \in I$.

Dimostrazione. Verifichiamo le proprietà di ideale: per $x, y \in \operatorname{Ker}\psi$ e $a \in A$, si ha

$$\psi(x+y) = \psi(x) + \psi(y) = 0_B + 0_B = 0_B \tag{1.6.2}$$

quindi $x + y \in \operatorname{Ker}\psi$, e

$$\psi(ax) = \psi(a)\psi(x) = \psi(a)0_B = 0_B \tag{1.6.3}$$

quindi anche $ax \in \operatorname{Ker}\psi$, e analogamente per xa. Allora $\operatorname{Ker}\psi$ è proprio un ideale di A. □

Come già visto negli omomorfismi tra gruppi, anche un omomorfismo tra gli anelli A e B è iniettivo se e solo se il suo nucleo è $\{0_A\}$. Se l'anello è commutativo, i suoi ideali sono tutti anche nuclei di omomorfismi di anelli.

1.7 Anelli dei polinomi

Passiamo ora a trattare un tipo di anelli molto importante: gli anelli composti da polinomi.

Definizione 1.7.1. *Si dice* polinomio *a coefficienti in un anello A una successione di elementi di A definitivamente nulla:*

$$p = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots).$$

I polinomi si rappresentano anche, più comunemente, indicando il posto di ogni elemento della successione con delle potenze di un'incognita, come ad esempio

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n. \tag{1.7.1}$$

Generalmente, indicheremo i polinomi semplicemente con delle lettere, senza usare la notazione "funzionale" $p(x)$ ma solo p. Useremo $p(x)$ invece quando esprimeremo il polinomio tramite le potenze di x, per evitare di confonderlo con i termini noti.

L'ultimo coefficiente non nullo del polinomio, a_n, che nella scrittura predecente è il coefficiente assegnato alla potenza di grado massimo, si dice *coefficiente direttivo*. Il termine a_0 è invece il *termine noto*.

Tra polinomi definiamo la somma come

$$\begin{aligned}(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) + (b_0, b_1, b_2, \dots, b_m, 0, 0, \dots) = \\ (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_m + b_m, a_{m+1} + 0, a_{m+2} + 0, \dots, a_n, 0, 0, \dots),\end{aligned} \tag{1.7.2}$$

dove in questo caso $n > m$, e il prodotto come il polinomio che ha come componente di posto k il coefficiente

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}. \tag{1.7.3}$$

Con queste due operazione è facile vedere che $A[x]$, l'insieme dei polinomi a coefficienti in A, è a sua volta un anello. Il polinomio unità di $A[x]$ è il polinomio avente come primo coefficiente l'unità di A, 1_A, e tutti i successivi nulli; il polinomio nullo è il polinomio con tutti i coefficienti nulli.

Possiamo definire un'applicazione lineare $j\colon A \to A[x]$ che porta un elemento di A nel polinomio avente come termine noto tale elemento, ossia la mappa

$$j(a) = (a, 0, 0, \dots).$$

Tale applicazione è un omomorfismo di anelli, in quanto preserva le operazioni e l'unità: infatti dati $a, b \in A$ risulta

$$\begin{aligned}j(a+b) = (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = j(a) + j(b) \\ j(ab) = (ab, 0, 0, \dots) = (a, 0, 0, \dots)(b, 0, 0, \dots) = j(a)j(b),\end{aligned}$$

mentre porta l'unità 1_A nel polinomio $(1_A, 0, 0, \dots)$ che è l'unità di $A[x]$. Si nota facilmente anche che tale omomorfismo j è iniettivo, dato che $\operatorname{Ker} j = \{0_A\}$.

Ordinando gli elementi del polinomio in ordine di indici crescenti, la posizione del coefficiente direttivo indica il *grado* del polinomio, che quando scritto come combinazione lineare di potenze è anche il grado della potenza massima che appare.

Un polinomio non nullo $p(x) = a_n x^n + \cdots + a_0 \in A[x]$, con $a_n \neq 0$, si dice di grado n, e si indica con $\deg p = \deg p(x) = n$. Convenzionalmente si assegna al polinomio (identicamente) nullo il grado -1. Se $a_n = 1$, il polinomio si dice *monico*.

Proprietà 1.7.2. Si hanno le seguenti proprietà tra i gradi dei polinomi e le operazioni:

- $\deg(a+b) \leq \max\{\deg a, \deg b\}$;
- $\deg(ab) \leq \deg a + \deg b$.[3]

Ad esempio, nell'anello $\mathbb{Z}/12\mathbb{Z}$, si considerino i due polinomi $a(x) = [6]x^2$ e $b(x) = [2]x$: si ha che $\deg a = 2$ e $\deg b = 1$. La loro somma è un polinomio di grado 2, ma per il prodotto si vede che sebbene nell'anello [6] e [2] non siano nulli, lo è il loro prodotto perché 12 appartiene alla stessa classe di equivalenza di 0, quindi $a(x)b(x) = [6][2]x^3 = [12]x^3 = [0]x^3 = [0]$; di conseguenza $\deg\big(ab\big) = -1 \neq \deg a + \deg b = 3$. Le due proprietà precedenti sono in ogni caso rispettate.

Il caso dell'uguaglianza accade quindi soltanto se non esistono divisori dello zero nell'anello, vale a dire che esso è un dominio d'integrità: in questo caso il prodotto di due elementi non nulli non è mai nullo.

Siano A e B due anelli con unità, e $f\colon A \to B$ un omomorfismo d'anelli con unità. Anche $\tilde{f}\colon A[x] \to B[x]$ definito come $\tilde{f}\big(p(x)\big) = f(a_n)x^n + \cdots + f(a_0)$, con $f(a_i) \in B$, allora, è un omomorfismo di anelli con unità. Non è detto però che sia $\deg \tilde{f}(p) = \deg p$: potrebbe accadere infatti che il coefficiente direttivo di p appartenga al nucleo di f. Infine, come richiesto dalla definizione, $\tilde{f}(1_{A[x]}) = \big(f(1_A), 0, 0, \dots\big) = (1_B, 0, 0, \dots) = 1_{B[x]}$.

1.8 Divisione tra polinomi

Sia $K[x]$ l'anello dei polinomi su un campo K: non avendo divisori dello zero, $ab \neq 0_K$ se a e b (elementi di K) non sono nulli. Vale sempre, allora, l'uguaglianza $\deg(fg) = \deg f + \deg g$.

Teorema 1.8.1 (Algoritmo euclideo delle divisioni successive)**.** Sia K un campo, e $a, b \in K[x]$, con b diverso dal polinomio nullo. Esistono sempre, e sono unici, due polinomi r e q tali che

$$a = qb + r, \text{ con } \deg r < \deg b. \tag{1.8.1}$$

Dimostrazione. Dimostriamo l'esistenza dei due polinomi, per induzione, su $n = \deg a$. Se $n = -1$, allora $q = r = 0$, cioè $qb + r = 0$, e poiché per ipotesi $\deg b \neq -1$ perché non è nullo, si ha automaticamente che $\deg b > -1 = \deg r$. I due polinomi cercati quindi sono entrambi dei polinomi identicamente nulli. Sia ora $n > -1$, e siano $a(x) = a_n x^n + \cdots + a_0$, $b(x) = b_m x^m + \cdots + b_0$.

- se $m > n$, allora poniamo $a = 0 \cdot b + a$ (scegliamo cioè $q = 0$ nella (1.8.1)), e ciò significa che il resto è proprio a. Dunque $\deg r = n < m = \deg b$.
- se $m \leq n$, definiamo $\tilde{a} = \tilde{a}(x) = a(x) - b_m^{-1} a_n x^{n-m} b(x)$. Il coefficiente di grado massimo dell'ultimo termine è $-b_m^{-1} a_n x^{n-m} b_m x^m = -b_m^{-1} b_m a_n x^{n-m+m} = -a_n x^n$, quindi $\deg \tilde{a} \leq n-1$ poiché il coefficiente di grado n, che è il grado massimo di a, è cancellato. Per l'ipotesi di induzione, quindi, esistono due polinomi $\tilde{q}$ e $\tilde{r}$ tali che $\tilde{a} = \tilde{q}b + \tilde{r}$, per cui $\deg \tilde{r} < \deg b$. Risulta quindi

$$\begin{aligned} a(x) &= \tilde{q}(x)b(x) + b_m^{-1} a_n x^{n-m} b(x) + \tilde{r}(x) = \\ &= \big(\tilde{q}(x) + b_m^{-1} a_n x^{n-m}\big) b(x) + \tilde{r}(x). \end{aligned}$$

[3] Contrariamente a ciò che ci si aspetterebbe, non è un'uguaglianza perché pur essendo i coefficienti direttivi dei due polinomi non nulli, potrebbero esistere divisori dello zero in A, dunque non è detto che se $a, b \in A$ non sono nulli si abbia necessariamente $ab \neq 0$.

Scelti $q(x) = \tilde{q}(x) + b_m^{-1} a_n x^{n-m}$ e $r(x) = \tilde{r}(x)$, si ha dunque l'uguaglianza $a = qb + r$ con $\deg r = \deg \tilde{r} < \deg b$.

Abbiamo trovato dunque che q e r secondo la (1.8.1) esistono sempre, qualunque sia il grado di a.

Siano q, r e $\overline{q}, \overline{r} \in A[x]$ tali da soddisfare entrambe (le coppie) la (1.8.1), ossia che $a = \overline{q}b + \overline{r}$ e $a = qb + r$, con $\deg \overline{r} < \deg b$ e $\deg r < \deg b$. Allora risulta

$$0 = a - a = (q - \overline{q})b + r - \overline{r} \tag{1.8.2}$$

Per la prima delle 1.7.2 risulta $\deg\big(r - \overline{r}\big) < \max\{\deg r, \deg \overline{r}\} < \deg b$. Se $\overline{q} \neq q$, poiché la loro differenza non sarebbe un polinomio nullo, si avrebbe $\deg(q - \overline{q}) \geq 0$, e il prodotto $(\overline{q} - q)b$ darebbe un polinomio di grado sicuramente maggiore di quello di b, poiché K non ha divisori dello zero: dunque $\deg\big((q - \overline{q})b\big) > \deg b$. Ma se dalla (1.8.2) risulta $(\overline{q} - q)b = r - \overline{r}$, quindi i loro gradi devono essere uguali. Troviamo allora

$$\deg(r - \overline{r}) = \deg\big((\overline{q} - q)b\big) > \deg b > \deg(r - \overline{r}) \tag{1.8.3}$$

che è chiaramente un assurdo. Di conseguenza deve essere $\overline{q} = q$ e $\overline{r} = r$, cioè i polinomi quoziente e resto sono unici. □

La dimostrazione di questo teorema è molto rigorosa, ma non è che una trascrizione "più tecnica" di quello che dovrebbe già essere noto dalla divisione tra polinomi (ma anche tra numeri naturali!):

- Se a è nullo, allora quoziente e resto sono entrambi nulli.
- Se a ha un grado minore di b, il quoziente è nullo e il resto è a stesso.
- Se a ha un grado maggiore di b, allora abbiamo una divisione "non banale" e ci aspettiamo un quoziente che ha come grado la differenza tra quelli di a e b.

Quando il resto della divisione è nullo, ossia $a = qb$, diremo che b *divide* a, e lo indicheremo con la notazione $a|b$. Poiché gli elementi dell'ideale principale (a) sono della forma ax per $x \in A$, vediamo subito che $a|b$ implica $b \in (a)$, e viceversa.

Definizione 1.8.2. *Dato un campo K, siano $a, b \in K[x]$ due polinomi non nulli. Si dice* massimo comune divisore *tra a e b ogni polinomio $d \in K[x]$ tale che:*

- *d divide sia a che b;*
- *se un altro polinomio c divide a e b, allora divide anche d.*

Questa definizione ricalca quella del massimo comune divisore tra numeri interi. Per i numeri in $\mathbb{Z}$, però, è noto che se z è il massimo comune divisore tra m e n, allora lo è anche $-z$. Anche per i polinomi vale un risultato simile: dato un massimo comune divisore in $K[x]$, tutti i suoi multipli per una costante in K lo sono ancora.

Teorema 1.8.3. Siano $a, b \in K[x]$ non nulli, e d un massimo comun divisore tra i due. Se d' è un altro massimo comune divisore, allora vale la relazione $d' = kd$ per qualche $k \in K \setminus \{0\}$.

Dimostrazione. Per la definizione di massimo comune divisore, d e d' dividono entrambi a e b, e si dividono a vicenda, ossia $d|d'$ e $d'|d$. Dunque esistono $\alpha, \beta \in K[x]$ tali che $d = \alpha d'$ e $d' = \beta d$. Otteniamo da queste due uguaglianze che $d = \alpha\beta d$. Poiché $d \neq 0$ — altrimenti dovrebbe essere $a = 0$, contro le ipotesi fatte — per le leggi di cancellazione si ha $\alpha\beta = 1$. La somma dei gradi di α e β deve quindi essere nulla, cioè il grado del polinomio unità: l'unico modo possibile affinché accada è che $\deg \alpha = \deg \beta = 0$, ossia che entrambi siano, oltre che polinomi, anche elementi (scalari) del campo K, cioè $\alpha = k \in K$ e $\beta = h \in K$. Ma allora $hk = 1$, cioè h e k sono invertibili, perciò non possono essere nulli. Dunque $d' = kd$ con $k \in K \setminus \{0\}$. □

A causa di questa arbitrarietà nella costante moltiplicativa, è conveniente stabilire la seguente definizione.

Definizione 1.8.4. *Dati $a, b \in K[x]$ non nulli, il massimo comune divisore di a e b con coefficiente direttivo unitario è detto* massimo comune divisore monico.

D'ora in poi, quando ci riferiremo al massimo comune divisore, sottintenderemo che prendiamo quello monico.

Teorema 1.8.5 (Algoritmo di Euclide)**.** Dato un campo K, e $a, b \in K[x]$ non nulli, esiste sempre un massimo comune divisore tra di loro.

Dimostrazione. Dato che $b \neq 0$, esistono $q_1, r_1 \in K[x]$ tali da poter scrivere $a = q_1 b + r_1$ e per cui $\deg r_1 < \deg b$. Se $r_1 = 0$, allora $a = qb$, quindi $b|a$ e ovviamente anche $b|b$; se esiste un $c \in K[x]$ tale che $c|a$, esso è b che è quindi il massimo comune divisore.

Se $r_1 \neq 0$, dividiamo b per esso: esistono $q_2, r_2 \in K[x]$ per cui $\deg r_2 < \deg r_1$ e

$$b = q_2 r_1 + r_2. \tag{1.8.4}$$

Se adesso $r_2 = 0$, troviamo che r_1 è il massimo comune divisore. Infatti, $r_1|b$ dal fatto che $b = r_1 q_2$, inoltre $a = q_1 b + r_1 = q_1(q_2 r_1) + r_1 = (q_1 q_2 + 1) r_1$ dunque $r_1|a$. Prendiamo dunque un $c \in K[x]$ che divida sia a che b: ciò significa che esistono $\alpha, \beta \in K[x]$ tali che $a = c\alpha$ e $b = c\beta$.

$$c\alpha = a = q_1 b + r_1 = q_1 c\beta + r_1 \Rightarrow r_1 = (\alpha - q_1\beta)c \tag{1.8.5}$$

ossia $c|r_1$. Il polinomio r_1 soddisfa dunque la definizione 1.8.2 di massimo comune divisore.

Se invece $r_2 \neq 0$, ancora possiamo dividere r_1 per r_2, dato che esistono $q_3, r_3 \in K[x]$ tali che $\deg r_3 < \deg r_2$ e

$$r_1 = q_3 r_2 + r_3. \tag{1.8.6}$$

Se $r_3 = 0$, allora esattamente come prima si dimostra che r_2 è il massimo comune divisore tra a e b. Se $r_3 \neq 0$, iteriamo ancora una volta dividendo r_2 per r_3 e distinguendo i casi se il resto di questa divisione è nullo o no.

Il procedimento deve necessariamente avere un termine, in quanto a partire da $\deg b$ si ha la successione decrescente

$$\deg b > \deg r_1 > \deg r_2 > \dots \tag{1.8.7}$$

e si giunge dopo un numero finito di passi con un resto nullo. Sia dunque $r_k = 0$: abbiamo che

$$\begin{aligned} r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} &= q_k r_{k-1} \end{aligned} \tag{1.8.8}$$

perciò $r_{k-1}|r_{k-2}$. Dalll'equazione precedente vediamo allora che $r_{k-1}|r_{k-3}$ e così via per tutti i resti precedenti, fino a dividere anche b e dunque a dalla prima equazione $a = q_1 b + r_1$. Infine, se un $c \in K[x]$ dividesse a e b, allora dividerebbe r_1: ma allora divide anche r_2 (con un ragionamento analogo al precedente) e così via si vede che divide tutti i resti fino a r_{k-1}. Dunque il massimo comun divisore di a e b è proprio r_{k-1}. □

Teorema 1.8.6 (Identità di Bézout)**.** Dato un campo K e $a, b \in K[x]$, se d è il loro massimo comune divisore, allora esistono $\xi, \eta \in K[x]$ tali per cui si ha

$$d = \xi a + \eta b. \tag{1.8.9}$$

Dimostrazione. La determinazione di tali ξ e η si può fare tramite l'algoritmo di Euclide delle divisioni successive. Se il massimo comun divisore è uno tra a o b, la tesi è ovvia, prendendo $\xi = 1$ e $\eta = 0$ o viceversa.

Effettuiamo la prima divisione ottenendo $a = q_1 b + r_1$, da cui $r_1 = a - q_1 b$. Se r_1 è il massimo comune divisore, ci basta porre $\xi = 1$ e $\eta = -q_1$. Altrimenti, seguendo il teorema precedente dividiamo b (sappiamo che $r_1 \neq 0$, altrimenti b sarebbe il massimo comun divisore) come $b = q_2 r_1 + r_2$. Se r_2 è il massimo comune divisore,

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 - q_1 q_2) b \tag{1.8.10}$$

perciò poniamo $\xi = -q_2$ e $\eta = 1 - q_2 q_2$ per trovare la (1.8.9). Altrimenti dividiamo ancora r_1 per r_2 (anche stavolta, $r_2 \neq 0$ perché r_1 non è il massimo comun divisore) e procediamo, una volta trovato il massimo comune divisore, ad esprimerlo tramite i resti delle divisioni precedenti fino a risalire ad a e b. Anche in questo caso, come nell'algoritmo di Euclide, il numero di iterazioni è finito quindi in un numero finito di passi siamo sicuri di trovare due termini ξ e η che soddisfino la (1.8.9). □

Vediamo un esempio pratico: siano $a(x) = x^3 - 5$ e $b(x) = x^2 + 4$, due polinomi in $\mathbb{Q}[x]$. Dividiamo a per b con l'algoritmo di Euclide, ottenendo

$$\begin{aligned} x^3 - 5 &= x \cdot (x^2 + 4) + (4x - 5) \\ x^2 + 4 &= \Big(\frac{1}{4}x + \frac{5}{16}\Big)(4x - 5) + \frac{41}{16} \\ 4x - 5 &= \Big(\frac{64}{41}x - \frac{80}{41}\Big) \cdot \frac{41}{16} \end{aligned}$$

perciò $\frac{41}{16}$, ossia 1, (se lo prendiamo monico), è il massimo comune divisore di a e b.

1.9 Polinomi primi e irriducibili

Definizione 1.9.1. *Dato $a \in K[x]$ con $\deg a > 0$, esso si dice* primo *se ogniqualvolta $a|bc$ allora $a|b$ o $a|c$.*

Il seguente lemma mostra un legame tra i polinomi primi e i corrispettivi ideali principali generati da essi.

Lemma 1.9.2. Dato $a \in K[x]$ con $\deg a > 0$, l'ideale (a) è primo se e solo se a è primo.

Dimostrazione. Siano $b, c \in K[x]$. Se (a) è primo e $a|bc$, allora $bc \in (a)$. Per la definizione di ideale primo, però, ciò implica che $b \in (a)$ o $c \in (a)$, ossia $a|b$ o $a|c$. Dunque a è primo.

Sia ora a un polinomio primo: se $a|bc$ allora $a|b$ oppure $a|c$. Ma $a|bc$ implica $bc \in (a)$, e analogamente $a|x$ implica $x \in (a)$. Allora (a) è un ideale primo. □

Definizione 1.9.3. *Sia $a \in K[x]$ con $\deg a = n > 0$. Esso si dice* irriducibile *se è divisibile solo per i polinomi $c \in K[x]$ con $\deg c = 0$ e per quelli della forma λa, con $\lambda \in K \setminus \{0\}$.*

Notiamo subito che tutti i polinomi di grado 1, ossia della forma $p(x) = x - \alpha$, sono sempre irriducibili.

Teorema 1.9.4. Dato un campo K, un polinomio in $K[x]$ di grado positivo è irriducibile se e solo se è primo.

Dimostrazione. Sia $a \in K[x]$ irriducibile: prendiamo $b, c \in K[x]$ e supponiamo che $a|bc$. Mostriamo che se a non divide b, allora $a|c$. Escludiamo il caso $b = 0$, per il quale si avrebbe che $a|b$: abbiamo quindi $a, b \neq 0$. Sia dunque d il massimo comune divisore tra a e b. Essendo a irriducibile, abbiamo che o $d = \lambda$ o $d = \mu a$, per $\lambda, \mu \in K \setminus \{0\}$. Il secondo caso non è possibile, perché a quel punto $a = \mu^{-1} d$ quindi dividerebbe b. Dunque $d = \lambda$, con $\lambda = 1$ prendendo il polinomio monico. Per l'identità di Bézout 1.8.6, abbiamo allora

$$d = 1 = \xi a + \eta b$$

per qualche $\xi, \eta \in K[x]$. Moltiplicando per c, otteniamo $c = c\xi a + c\eta b$: poiché per ipotesi però $a|bc$, esiste $g \in K[x]$ tale per cui $ga = bc$. Allora

$$c = c\xi a + \eta g a = (c\xi + \eta g)a$$

ossia $a|c$.

Sia ora $a \in K[x]$ primo: se fosse riducibile, allora $\exists f, g \in K[x]$ (diversi da multipli scalari di a) con $\deg f, \deg g > 0$ tali che $a = fg$: allora $a|fg$. Essendo primo, però, divide sicuramente uno dei due, sia esso f: esiste quindi $\xi \in K[x]$, non nullo, per il quale $f = a\xi$. Ma allora

$$a = fg = a\xi g \Rightarrow (1 - \xi g)a = 0$$

ossia $\xi g = 1$: di conseguenza $\deg \xi + \deg g = 0$. Dato che $\deg g > 0$ e $\deg \xi \geq 0$, questo è assurdo: ciò prova che non esistono f, g diversi da multipli scalari di a e di grado positivo che dividono a, che quindi non è riducibile. □

Teorema 1.9.5 (di fattorizzazione unica)**.** Ogni polinomio $a \in K[x]$, con $\deg a > 0$, può essere scritto come un prodotto

$$up_1 \cdots p_n \tag{1.9.1}$$

dove $u \in K$ e tutti i p_i sono irridubicili. La fattorizzazione è essenzialmente unica, nel senso che se $a = kp_1 \cdots p_n = hq_1 \cdots q_t$ con $h, k \in K$ e p_i, q_i irriducibili, allora $n = t$ e a meno di permutazioni $p_i = cq_i$ con $c \in K$ per ogni i.

Dimostrazione. Dimostriamo per induzione su $n \coloneqq \deg a$.

Per prima cosa sia $n = 1$: per quanto già detto, essendo di primo grado è già irriducibile, quindi è la fattorizzazione cercata, che è ovviamente anche unica.

Supponiamo che la tesi sia vera da 1 a n. Se a è irriducibile, la dimostrazione è conclusa, altrimenti scriviamo $a = gh$ per qualche $g, h \in K[x]$. Se g e h sono entrambi irriducibili abbiamo trovato la fattorizzazione; se non è questo il caso, almeno uno tra g e h ha comunque un grado minore di quello di a, e per l'ipotesi di induzione è dunque riducibile. Procediamo scomponendo g o h, fino a trovare $a = p_1 p_2 \dots p_n$, dove ogni p_i è irriducibile.

Ammettiamo che esistano due fattorizzazioni

$$a = up_1p_2 \cdots p_n = vq_1q_2 \cdots q_t. \tag{1.9.2}$$

con $u, v \in K$. Poiché p_1 divide a, divide uno dei fattori q_i al secondo membro, e sicuramente non v. Riordiniamoli in modo che $p_1|q_1$: poiché q_1 è irriducibile, ciò significa che $q_1 = k_1 p_1$, con $k_1 \in K$ (l'ipotesi $p_1 \in K$ è chiaramente da escludere). Troviamo allora

$$up_1 \cdots p_n = vk_1p_1q_2 \cdots q_t. \tag{1.9.3}$$

ed essendo $K[x]$ un dominio d'integrità e $p_1 \neq 0$ possiamo dividere per esso ottenendo

$$up_2 \cdots p_n = vk_1q_2 \cdots q_t. \tag{1.9.4}$$

Ora al primo membro abbiamo $n - 1 < n$ fattori p_i, e proseguendo con lo stesso ragionamento precedente vediamo che al secondo ne abbiamo $t - 1 = n - 1$, dunque per l'ipotesi di induzione abbiamo che $p_i = k_i q_i$ per qualche $k_i \in K$ per ogni $2 \leq i \leq n$, e ciò prova la tesi. □

A questo punto, possiamo dividere tutti i fattori irriducibili per delle costanti opportune in K per renderli monici, come nel seguente corollario.

Corollario 1.9.6. Dato $a \in K[x]$, con $\deg a = s > 0$, esso si può sempre scrivere univocamente come $a = ka_1 \dots a_s$, in cui

- $k \in K \setminus \{0\}$ è il coefficiente direttivo di a;
- a_i, $\forall i \in \{1, \dots, s\}$ è monico e irriducibile.

Dimostrazione. Preso $a \in K[x]$, possiamo esprimerlo come $a = k_1 a_1$ con a_1 monico. Se si esegue lo stesso ragionamento su $a = p_1 \dots p_t$, nel teorema precedente, si ottiene $a = k_1 k_2 \dots k_s a_1 \dots a_s$ con i vari a_i monici e irriducibili $\forall i \in \{1, \dots, n\}$, si ha che $k_1 k_2 \dots k_s \in K$, perciò deve essere il coefficiente direttivo del polinomio corrispondente. □

1.10 Domini a ideali principali

Definizione 1.10.1. *Un dominio d'integrità A è detto* a ideali principali *se è tutti i suoi ideali propri sono principali, ossia se per ogni ideale $I \subset A$ esiste $a \in A$ per cui $I = (a)$.*

Dimostriamo subito l'inverso del corollario 1.5.4 che avevamo anticipato.

Teorema 1.10.2. In un dominio a ideali principali, un ideale è primo se e solo se è massimale.

Dimostrazione. Abbiamo già dimostrato nel corollario 1.5.4 che se un ideale è primo, allora è anche massimale. Sia A un dominio a ideali principali, I un suo ideale primo e J un altro ideale tali che $I \subseteq J \subseteq A$. Sappiamo che esistono $a, b \in A$ tali che $I = (a)$ e $J = (b)$. Poiché $(a) \subseteq (b)$, si ha $a \in (b)$ quindi esiste $x \in A$ tale che $a = xb$: allora $a|xb$. L'ideale I è primo, quindi anche a è un polinomio primo, perciò abbiamo che $a|b$ oppure $a|x$. Nel primo caso, si ha $b \in (a)$ perciò $(a) = (b)$, ossia $I = J$. Nel secondo caso, esiste $y \in A$ tale che $ya = x$, ma allora $x = y(xb) = x(yb)$. Poiché A è un dominio di integrità, e $x \neq 0$, ciò implica che $yb = 1$, e di conseguenza $1 \in (b)$. Ma un ideale che contiene l'unità coincide con l'anello intero, perciò $(b) = A$. Ciò prova che I è massimale. □

Mostriamo ora che possiamo sfruttare molte utili proprietà, come la completa equivalenza tra "primo" e "irriducibile", nello studio degli anelli di polinomi in una incognita, in virtù del seguente teorema.

Teorema 1.10.3. Dato un campo K, l'anello $K[x]$ è un dominio a ideali principali.

Dimostrazione. Sia I un ideale di $K[x]$. Se $I = \{0\}$, ovviamente $I = (0)$ quindi è un ideale principale. Se $I \neq \{0\}$ allora in esso ci sono dei polinomi di grado maggiore di zero. Poniamo

$$m \coloneqq \min\{\deg p \colon p \in I\}$$

che esiste per il principio del buon ordinamento.[4] Sia $g \in I \setminus \{0\}$ tale che $\deg g = m$: vogliamo mostrare che $(g) = I$. Chiaramente $(d) \subseteq I$ dalla definizione di ideale. Prendiamo inolte $y \in I$: certamente esistono $q, r \in K[x]$ tali per cui $\deg r < \deg y$ e $y = qg + r$. Di conseguenza, $r = y - qg \in I$: se però $r \neq 0$, avremmo $\deg r < \deg g$ che viola l'ipotesi fatta (g ha il grado minore tra tutti i polinomi di I). Deve necessariamente essere allora $r = 0$, da cui $y = qg$. Ma allora $g|y$, e poiché questo vale per ogni $y \in I$ risulta $I \subseteq (d)$. Ciò prova che $I = (d)$, perciò ogni ideale di $K[x]$ è un ideale principale. □

Corollario 1.10.4. Ogni ideale principale $I \in K[x]$, con $I \neq (0)$, ha un unico generatore monico.

Dimostrazione. Poniamo $I = (g)$ con $g(x) = a_n x^n + \cdots + a_0$ con $a_n \neq 0$. Possiamo allora moltiplicare g per a_n^{-1}, ottenendo che I è anche generato da $\tilde{g} = a_n^{-1} g$ che è monico, cioè $(\tilde{g}) = (g)$: ciò prova l'esistenza di un generatore monico di I. Dimostriamone l'unicità: sia $I = (h)$, con h monico. Poiché $(h) = (\tilde{g})$, risulta che $\tilde{g}|h$ e $h|\tilde{g}$ ossia esistono $\alpha, \beta \in K[x]$ per cui $h = \alpha\tilde{g}$ e $\tilde{g} = \beta h(x)$. Quindi $h = \alpha\beta h$, e poiché $I \neq \{0\}$ e $K[x]$ è un dominio d'integrità risulta $\alpha\beta = 1$. Dunque $\alpha, \beta \in K \setminus \{0\}$: $h = \alpha\tilde{g}$ per ipotesi è monico, e dato che lo è anche $\tilde{g}$ si ottiene $\alpha = 1$. Di conseguenza $h = \tilde{g}$, cioè il generatore monico è unico. □

Teorema 1.10.5. Sia (g) un ideale non nullo di $K[x]$. Ogni classe laterale di $(g) \in K[x] \,/\, g$ si può rappresentare univocamente nella forma $(g) + r$, con $\deg r < \deg g$.

Dimostrazione. Una classe laterale dell'ideale (g) è del tipo $(g) + f$, per $f \in K[x]$. Per il teorema 1.8.5 esistono sempre $q, r \in K[x]$, con $\deg r < \deg g$ tali che $f = qg + r$. Si ha allora

$$(g) + f = (g) + qg + r = (g) + r,$$

[4] Il principio del buon ordinamento afferma che *ogni insieme di numeri naturali non vuoto contiene un numero che è più piccolo di tutti gli altri.*

dato che $qg \in (g)$, quindi un tale r esiste. Mostriamo che è unico. Supponiamo che esista anche un $r' \in K[x]$ tale che la classe laterale si possa rappresentare come $(g) + r'$, con $\deg r' < \deg g$. Dalle proprietà 1.7.2 risulta

$$\deg(r' - r) \leq \max\{\deg r', \deg r\} < \deg g.$$

Ora, nel caso $\deg(r' - r) \geq 0$, se fosse $r' - r \in (g)$ allora si avrebbe $r' - r = hg$ per qualche $h \in K[x]$, ma allora $\deg(r' - r) = \deg(hg)$ e contemporaneamente

$$\deg(r' - r) < \deg g \geq \deg(hg)$$

che porta ad una contraddizione. Dunque $\deg(r' - r) = 0$, ossia $r' - r = 0 = 0 \cdot g$ perciò $r' - r \in (g)$. Avendo i due rappresentanti in relazione, le due classi laterali sono equivalenti. □

Corollario 1.10.6. Sia K un campo finito e $g \in K[x]$ di grado $n > 0$. Allora $|K[x] / (g)| = |K|^n$.

Dimostrazione. Sapendo che le classi laterali sono scritte come $(g) + r(x)$, ora ipotizziamo due casi, cioè $\deg r(x) = 0$, oppure $\deg r(x) = -1$, ricaviamo:

$$\begin{aligned} &\deg r(x) = 0 \text{ si ha } (g) + r(x) = (g) + a_0, \\ &\deg r(x) = 1 \text{ si ha } (g) + r(x) = (g) + a_1 x + a_0. \end{aligned}$$

Nel primo caso si ritrovano tutte le possibili combinazioni degli $a_0 \in K$, che sono m, nel secondo caso le possibili combinazioni sono m^2. Si può arrivare dunque a dimostrare la tesi. □

Teorema 1.10.7. Sia $g \in K[x]$ con $\deg g > 0$. L'ideale (g) è massimale se e solo se g è irriducibile.

Dimostrazione. Non bisogna far altro che applicare dei teoremi già visti in precedenza:

$$(g) \text{ è massimale } \Leftrightarrow (g) \text{ è primo } \Leftrightarrow g \text{ è primo } \Leftrightarrow g \text{ è irriducibile}$$

per i teoremi, in ordine, 1.10.2, 1.9.2 e 1.9.4. □

Corollario 1.10.8. Dato $g \in K[x]$ con $\deg g > 0$, $K[x] / (g)$ è un campo se e solo se g è irriducibile.

Dimostrazione. Dal teorema precedente abbiamo che g è irriducibile se e solo se (g) è massimale. Collegando anche il teorema 1.5.3 troviamo la tesi. □

Vediamo un esempio concreto delle conseguenze di questi teoremi. Partiamo dall'anello $\mathbb{R}[x]$ dei polinomi a coefficienti reali, e un polinomio irriducibile di grado maggiore di 1, come $x^2 + 1$. Essendo irriducibile, l'ideale $(x^2 + 1)$ è primo e massimale, e $\mathbb{R}[x] / (x^2 + 1)$ un campo. I suoi elementi, dal teorema 1.10.5, si scrivono tutti come un elemento di $(x^2 + 1)$ più un polinomio di primo grado, ossia se $p \in \mathbb{R}[x] / (x^2 + 1)$ allora

$$p = (x^2 + 1) + ax + b. \tag{1.10.1}$$

Prendiamo un'altro elemento $q = (x^2 + 1) + cx + d$. La somma di due elementi è definita in modo naturale come

$$p + q = (x^2 + 1) + ax + b + (x^2 + 1) + cx + d = (x^2 + 1) + (a + c)x + b + d \tag{1.10.2}$$

e il prodotto come

$$pq = [(x^2 + 1) + ax + b] \cdot [(x^2 + 1) + cx + d] = (x^2 + 1) + acx^2 + (ad + bc)x + bd. \tag{1.10.3}$$

Il termine acx^2 però ha lo stesso grado di $x^2 + 1$, quindi non deve comparire. Possiamo in effetti trovare un modo per eliminarlo: aggiungendo e sottraendo ac al risultato, otteniamo

$$\begin{aligned} pq &= (x^2 + 1) + acx^2 + ac + (ad + bc)x + bd - ac = \\ &= (x^2 + 1) + ac(x^2 + 1) + (ad + bc)x + bd - ac = \\ &= (x^2 + 1) + (ad + bc)x + bd - ac \end{aligned} \tag{1.10.4}$$

dato che $ac(x^2+1) \in (x^2+1)$ quindi viene "assorbito" dall'ideale.

Prendiamo ora l'insieme $\mathbb{R}^2$ delle coppie di numeri reali, e dotiamolo delle operazioni

$$\begin{aligned}(b,a)+(\beta,\alpha) &= (b+\beta, a+\alpha)\\ (b,a)(\beta,\alpha) &= (a\beta+b\alpha, b\beta-a\alpha).\end{aligned} \tag{1.10.5}$$

Questa struttura individua un ulteriore campo, di cui non è difficile notare il legame con il precedente $\mathbb{R}[x]/(x^2+1)$. Troviamo infatti un isomorfismo $\gamma\colon \mathbb{R}[x]/(x^2+1) \to \mathbb{R}^2$, definito come

$$\gamma\colon (x^2+1)+ax+b \mapsto (b,a) \tag{1.10.6}$$

che li lega. Ovviamente quest'ultimo campo $\mathbb{R}^2$, con le operazioni definite, non è altro che il campo complesso come costruito da Hamilton, ma con la coppia (a,b) in ordine contrario. Per passare alla notazione comune $a+ib$ non dobbiamo far altro che definire un nuovo insieme $\hat{\mathbb{C}} = \{a+ib\colon a,b \in \mathbb{R}\}$ con le note operazioni, e tale che $i^2=-1$. L'isomorfismo che mette in relazione i due campi è evidentemente un $\varphi\colon \mathbb{C} \to \hat{\mathbb{C}}$ per il quale

$$\varphi(b,a) = a+ib. \tag{1.10.7}$$

1.11 Radici di un polinomio

Definizione 1.11.1. *Dato un anello A commutativo e con unità e un polinomio $p \in A[x]$, si dice* radice *di p un elemento $\alpha \in A$ per cui $p(\alpha)=0$.*

Teorema 1.11.2 (di Ruffini)**.** Dato un campo K e un polinomio $p \in K[x]$, α è una radice di p se e solo se $(x-\alpha)|p$.

Dimostrazione. Sia α una radice di p. Possiamo dividere p per $x-\alpha$, il cui grado non è nullo, ottenendo che

$$p(x) = q(x)(x-\alpha)+r(x)$$

con $\deg r < \deg\big((x-\alpha)\big) = 1$. Dato che $\deg r \in \{0,1\}$, quindi, $r(x)=k$ per qualche $k \in K$, eventualmente $k=0$ se $\deg r = -1$. Ma essendo α una radice di p, valutando $p(\alpha)$ otteniamo

$$0 = p(\alpha) = q(\alpha)(\alpha-\alpha)+k = k$$

perciò $k = r(x) = 0$: di conseguenza $p(x) = q(x)(x-\alpha)$, ossia $(x-\alpha)|p$.

Sia ora $(x-\alpha)|p$: possiamo dunque scrivere $p(x) = g(x)(x-\alpha)$ per qualche $g \in K[x]$. Ma allora, valutandolo in α, risulta

$$p(\alpha) = g(\alpha)(\alpha-\alpha) = 0$$

quindi α è una radice di p. □

Per esempio, sia $f(x) = a_1x+a_0 \in K[x]$ con $a_1 \neq 0$. Si ha che $\alpha = -\frac{a_0}{a_1}$ è sempre una radice.

Si può, visti i teoremi precedenti, porre una relazione tra la presenza di una radice e la possibilità di ridurre un polinomio. Sia $f(x) \in K[x]$ e $\deg f(x) > 1$, se $f(x)$ ammette una radice α, allora $f(x)$ deve essere riducibile come $f(x) = (x-\alpha)g(x)$.

Non è detto, in generale, che ogni polinomio riducibile abbia necessariamente una radice: basta prendere in $\mathbb{R}[x]$ il polinomio x^4+2x^2+1. Esso si può scomporre in $(x^2+1)(x^2+1)$, che chiaramente non hanno radici reali. Se invece il polinomio *è riducibile* e ha grado 2 o 3, allora certamente ha una radice: in fatti almeno uno dei fattori in cui è scomposto deve avere grado 1, cioè sarà della forma $x-\lambda$, perciò tale λ è una radice.

Un caso importante è quello dei numeri complessi: in tale campo, si può sempre scomporre un polinomio (non costante) in un prodotto di opportuni polinomi di primo grado, per via del seguente teorema (che non dimostriamo).

Teorema 1.11.3 (Teorema fondamentale dell'algebra)**.** Ogni polinomio in $\mathbb{C}[x]$ di grado positivo ammette sempre una radice in $\mathbb{C}$.

Definizione 1.11.4. *Siano K un campo, $f \in K[x]$ e $\alpha \in K$. Si dice che α è una radice di f con* molteplicità algebrica *$r \in \mathbb{N}$ se $(x-\alpha)^r | f$ ma $(x-\alpha)^{r+1}$ non divide f.*

In particolare, una radice di molteplicità algebrica 1 è detta *semplice*.

Teorema 1.11.5. Sia $f \in K[x]$ con $\deg f \geq 0$. Date le radici distinte $\alpha_1, \dots, \alpha_k$ di f con molteplicità algebrica rispettivamente $r_1, \dots, r_k$, si ha che $\sum_{i=1}^{n} r_i \leq \deg f$.

Dimostrazione. Secondo il teorema 1.9.5, scriviamo f come

$$f = p_1 p_2 \dots p_k, \tag{1.11.1}$$

con ogni p_i primo. Data una radice α_1, si ha che $(x-\alpha_1)|f$, quindi divide uno dei p_i. Riordiniamo l'ordine del prodotto in modo che $(x-\alpha_1)|p_1$: poiché p_1 è primo, quindi irriducibile, dovrà essere della forma $h(x-\alpha_1)$ con $h \in K \setminus \{0\}$. Raccogliendo tutti i fattori di questo tipo nel prodotto otteniamo

$$f(x) = (x-\alpha_1)^{k_1} u(x) \tag{1.11.2}$$

con ovviamente $k_1 \geq r_1$ (altrimenti r_1 non sarebbe la molteplicità di α_1), e $x-\alpha_1$ che non divide u. Allo stesso modo, però, $(x-\alpha_1)^{r_1} | f$, dunque

$$f(x) = (x-\alpha_1)^{r_1} v(x). \tag{1.11.3}$$

Eguagliando le due espressioni trovate abbiamo

$$(x-\alpha_1)^{k_1} u(x) = (x-\alpha_1)^{r_1} v(x) \quad \Rightarrow \quad (x-\alpha_1)^{r_1-k_1} v(x) = u(x) \tag{1.11.4}$$

dato che $K[x]$ è un dominio d'integrità. Se ora $r_1 > k_1$, si avrebbe che $x-\alpha_1 | u$, ma ciò contrasta la scelta di k_1: allora $r_1 = k_1$ da cui

$$f(x) = (x-\alpha_1)^{r_1} u(x). \tag{1.11.5}$$

Passiamo alla radice α_2: poiché $\alpha_2 \neq \alpha_1$, certamente $x-\alpha_2$ non divide $(x-\alpha_1)^{r_1}$, quindi dovrà dividere u. Procediamo in questo modo fino ad esaurire le radici α_i, giungendo a una forma

$$f(x) = (x-\alpha_1)^{r_1} \cdots (x-\alpha_k)^{r_k} g(x). \tag{1.11.6}$$

Allora dalle proprietà 1.7.2 otteniamo

$$\deg f = \sum_{i=1}^{k} r_i + \deg g \geq \sum_{i=1}^{k} r_i \tag{1.11.7}$$

come volevamo dimostrare. □

Corollario 1.11.6 (Principio d'identità dei polinomi)**.** Siano $\alpha_1, \dots, \alpha_{n+1}$ elementi distinti di K. Se $f, g \in K[x]$, al più di grado n, sono tali che $f(\alpha_i) = g(\alpha_i)\ \forall i \in \{1, \dots, n+1\}$, allora $f = g$.

Dimostrazione. Supponiamo per assurdo che sia $f \neq g$. Allora si ha che $f - g \neq 0$, perciò $n \geq \deg(f-g) \geq 0$. Se $f(\alpha_i) = g(\alpha_i)\ \forall i \in \{1, \dots, n+1\}$, allora ogni α_i è radice di $f-g$, che ha quindi $n+1$ radici. Per il teorema precedente, però, risulterebbe $\deg(f-g) \geq \sum_{k=1}^{n+1} r_i \geq n+1$ (nel migliore dei casi, $\deg(f-g) = n+1$ se ogni radice è semplice), che è assurdo perché come visto si ha $\deg(f-g) \leq n$. Dunque deve essere $f - g = 0$, ossia $f = g$. □

Capitolo 2

Spazi vettoriali

2.1 Proprietà principali

Definizione 2.1.1. *Dato un campo K, un insieme V non vuoto e due operazioni interne $+\colon V \times V \to V$ e $\cdot\colon K \times V \to V$, la terna $(V, +, \cdot)$ si definisce* spazio vettoriale *sul campo K se sono soddisfatte le seguenti proprietà:*

- *$(V, +)$ è un gruppo abeliano;*
- *$1_K x = x$ per ogni $x \in V$;*
- *la proprietà associativa, ossia se $\forall \lambda, \mu \in K$ e $\forall x \in V$, si ha $\lambda(\mu x) = (\lambda\mu)x$;*
- *la proprietà distributiva, ossia se $\forall \lambda, \mu \in K$ e $\forall x, y \in V$, si ha $(\lambda + \mu)x = \lambda x + \mu x$ e $\lambda(x + y) = \lambda x + \lambda y$.*

Gli elementi di V si chiamano *vettori* mentre quelli di K *scalari*. L'elemento neutro della somma, che per le proprietà note dei gruppi esiste ed è unico, sarà indicato con 0, oppure 0_V in caso di ambiguità. Lo zero e l'unità del campo K seguono la convenzione già usata per la quale saranno indicati con 0 e 1, o anche 0_K e 1_K; il fatto che 0 indichi sia lo zero di K che quello di V sarà spesso chiaro dal contesto.

Esempi

- $(\mathbb{R}^n, +, \cdot)$, l'insieme delle n-uple ordinate di numeri reali, è uno spazio vettoriale su $\mathbb{R}$, infatti $\forall \lambda \in \mathbb{R}$ si ha, rappresentando i vettori come colonne,

$$\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

  eccetera definendo somma e prodotto per scalare componente per componente.

- L'anello dei polinomi $\mathbb{R}[x]$ è uno spazio vettoriale su $\mathbb{R}$ con l'addizione e il prodotto per un numero reale, dove moltiplicare un polinomio per $\lambda \in \mathbb{R}$ equivale a moltiplicare per tale scalare tutti i suoi termini.
- L'insieme delle funzioni (qualunque) definite da un insieme $X \neq \varnothing$ e a valori reali forma uno spazio vettoriale, con le operazioni di addizione e prodotto per numero reale "puntuali", ossia $(f + g)(x) = f(x) + g(x)$ e $(\lambda f)(x) = \lambda f(x)$.
- Ogni campo può essere visto come spazio vettoriale su se stesso: ad esempio $(\mathbb{R}, +, \cdot)$ è uno spazio vettoriale su $\mathbb{R}$, e $(\mathbb{C}, +, \cdot)$ è uno spazio vettoriale su $\mathbb{C}$ ma anche su $\mathbb{R}$ se lo consideriamo come l'insieme delle coppie $(a, b) = a + ib$ con $a, b \in \mathbb{R}$.

Elenchiamo ora una serie di proprietà di base sugli spazi vettoriali, in cui assumiamo V come spazio vettoriale su un campo K.

Proprietà 2.1.2. Per ogni vettore $x \in V$, $0_K x = 0_V$.

Dimostrazione. Lo 0_K si può sempre scrivere come somma di 0_K con se stesso, quindi $0_K x = (0_K + 0_K)x = 0_K x + 0_K x$. Poiché V è abeliano, sommando l'inverso di $0_K x$ ai due membri si ottiene $0_K x = 0_V$ □

Proprietà 2.1.3. Per ogni scalare $a \in K$ e $\forall x \in V$, $-(ax) = (-a)x$.

Dimostrazione. Per la proprietà precedente si ha $0_V = 0_K x$, e lo zero scalare si scrive come somma degli inversi $a + (-a)$, quindi $0_V = [a + (-a)]x = ax + (-a)x$, che significa che $(-a)x$ è il vettore inverso di ax rispetto alla somma, ossia $(-a)x = -(ax)$. □

Proprietà 2.1.4. Per ogni $a \in K$, $a0_V = 0_V$.

Dimostrazione. Si ha che $a0_V = a(0_V + 0_V) = a0_V + a0_V$, e come per la proprietà 2.1.2 poiché V è abeliano si somma ai due membri dell'uguaglianza l'inverso di $a0_V$, ottenendo $a0_V = 0_V$. □

Proprietà 2.1.5. Se $ax = 0_V$ per $a \in K$ e $x \in V$, allora $a = 0_K$ o $x = 0_V$.

Dimostrazione. Se $a = 0_K$ è ovvia, se invece $a \neq 0_K$ allora esiste il suo inverso, $a^{-1} \in K$, rispetto al prodotto in K (cioè tale che $aa^{-1} = 1_K$). Quindi $0_V = a^{-1}0_V$, e poiché per per ipotesi $ax = 0$ segue che $0_V = a^{-1}(ax) = (aa^{-1})x = 1_K x = x$, perciò $x = 0_V$. □

Proprietà 2.1.6. Per ogni $a, b \in K$ e per ogni $x \in V$, se $ax = bx$ allora $a = b$ oppure $x = 0_V$.

Dimostrazione. Se vale che $ax = bx$, allora aggiungendo l'inverso di bx per la somma si ottiene $ax - (bx) = 0_V$. Inoltre per la proprietà distributiva questo è uguale ad $ax + (-b)x = (a - b)x = 0_V$. Per la proprietà 2.1.5, infine, $a + (-b) = 0_K$ oppure $x = 0_V$. Sommando b alla prima delle due risulta $a = b$ o $x = 0_V$. □

Proprietà 2.1.7. Per ogni scalare $\lambda \in K$ e $\forall x, y \in V$, se $\lambda x = \lambda y$ allora $\lambda = 0_K$ o $x = y$.

Dimostrazione. Da $\lambda x = \lambda y$ risulta $\lambda x + \big(-(\lambda y)\big) = \lambda x + \lambda(-y) = 0_V$. Per la proprietà distributiva equivale a $\lambda\big(x + (-y)\big) = 0_V$, da cui sempre per la 2.1.5 $\lambda = 0_K$ oppure $x + (-y) = 0_V$, da cui sommando y ai due membri risulta $\lambda = 0_K$ oppure $x = y$. □

2.2 Sottospazi vettoriali

Definizione 2.2.1. *Sia V uno spazio vettoriale sul campo K. Un suo sottoinsieme $W \subseteq V$ non vuoto si dice* sottospazio *vettoriale se $(W, +, \cdot)$, con le operazioni indotte da V, è a sua volta uno spazio vettoriale.*

In altre parole un sottospazio (ometteremo spesso l'attributo "vettoriale" per brevità) è un sottoinsieme che risulta chiuso rispetto alle due operazioni dello spazio vettoriale che lo contiene. Per verificare che un insieme W sia un sottospazio bisogna dunque provare che le combinazioni lineari di elementi di W siano ancora in W: una condizione necessaria facile da verificare è che W deve contenere lo 0_V.

Ogni spazio vettoriale V contiene sempre due spazi vettoriali, che sono banalmente $\{0_V\}$ e V stesso. Vediamone altri esempi.

- Preso lo spazio vettoriale $\mathbb{R}^n$, l'insieme

$$N = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ 0 \end{pmatrix} : x_1, \ldots, x_{n-1} \in \mathbb{R} \right\}$$

è un sottospazio vettoriale, perché ognuna delle due operazioni dà sempre come risultato un vettore con l'n-esima componente nulla.

- Dato $\mathbb{R}[x]$, l'insieme dei polinomi di grado non maggiore di n, indicato con $\mathbb{R}_n[x] = \{p(x) = a_0 + a_1x + \cdots + a_nx^n : a_0, a_1, \ldots, a_n \in \mathbb{R}\}$, formano un sottospazio vettoriale di $\mathbb{R}[x]$. Infatti la somma di due poliniomi di grado massimo n è ancora un polinomio di grado massimo n, mentre moltiplicando un polinomio per uno scalare non nullo si moltiplicano i coefficienti di ogni termine per tale scalare, quindi il grado rimane immutato. Moltiplicando per zero si ottiene invece un polinomio nullo, che ha ancora ovviamente grado minore di n. Lo stesso vale per $\mathbb{C}_n[x] \leq \mathbb{C}[x]$.
- L'insieme $\mathscr{C}(\mathbb{R})$ delle funzioni definite da $\mathbb{R}$ a $\mathbb{R}$ e continue è un sottospazio vettoriale dello spazio delle funzioni $f : \mathbb{R} \to \mathbb{R}$. Infatti sommando due funzioni continue si ottiene una funzione continua, e ovviamente anche moltiplicando una funzione continua per uno scalare.

Teorema 2.2.2. Sia V uno spazio vettoriale su un campo K e sia $\{W_i\}_{i\in I}$ un insieme di sottospazi vettoriali di V. Allora la loro intersezione $\bigcap_{i\in I} W_i$ è ancora un sottospazio vettoriale di V.

Dimostrazione. Siano $w_1, w_2 \in \bigcap_{i\in I} W_i$. Allora $\forall i \in I$, w_1 e w_2 appartengono a W_i (appartengono a tutti i sottospazi). Poiché i W_i sono sottospazi vettoriali, allora accade sempre che $\forall i \in I$, $w_1 + w_2 \in W_i$, quindi appartengono anche a $\bigcap_{i\in I}$. Un ragionamento analogo si effettua per il prodotto per scalare. Quindi $\bigcap_{i\in I}$ è un sottospazio vettoriale di V. □

Il teorema non vale se al posto dell'intersezione si effettua l'unione dei W_i: ad esempio le due rette $x = 0$ e $y = x$, rappresentate in forma vettoriale come $\left\{\binom{x}{0} : x \in \mathbb{R}\right\}$ e $\left\{\binom{x}{x} : x \in \mathbb{R}\right\}$, sono banalmente due sottospazi vettoriali di $\mathbb{R}^2$. Prendendo però un elemento del primo e uno del secondo, $\binom{1}{0}$ e $\binom{1}{1}$, sommandoli si ottiene $\binom{2}{1}$ che non appartiene all'unione dei due sottospazi.

Definizione 2.2.3. *Siano V uno spazio vettoriale su K e $S \subseteq V$ un insieme non vuoto. Si dice* sottospazio generato *di V, e si indica con $\langle S\rangle$, un sottospazio vettoriale che soddisfa le seguenti due proprietà:*

- *$S \subseteq \langle S\rangle$;*
- *se $W \leq V$ tale che $S \subseteq W$, allora $\langle S\rangle \leq W$.*

Teorema 2.2.4. Siano V uno spazio vettoriale su K e $S \subseteq V$ un insieme non vuoto, esiste sempre $\langle S\rangle$ ed è unico.

Dimostrazione. Mostriamo l'esistenza: costruiamo l'insieme $\langle S\rangle = \bigcap_{i\in I} Z_i$ dove $\{Z_i\}_{i\in I}$ sono tutti sottospazi vettoriali di V che includono S; ogni Z_i non è vuoto perché include S. Sicuramente $\langle S\rangle$ è, a sua volta, un sottospazio di V per il teorema 2.2.2. S è contenuto in ogni Z_i, quindi è incluso anche in $\langle S\rangle = \bigcap_{i\in I} Z_i$. Inoltre, sia W un sottospazio di V tale che $S \subseteq W$: allora $S \subseteq \langle S\rangle \subseteq W$. Poiché $\langle S\rangle$ è un sottospazio vettoriale, per ogni $x, y \in S$ e $\lambda, \mu \in K$ (x e y appartengono a $\langle S\rangle$ e a W), mentre $\lambda x + \mu y \in \langle S\rangle$, quindi $\langle S\rangle \leq W$. Tale $\langle S\rangle$ rispetta dunque la definizione 2.2.3.

Vediamo ora l'unicità. Se Z_1, Z_2 sono due sottospazi vettoriali di V che soddisfano la definizione 2.2.3, allora $S \subseteq Z_1$ e $S \subseteq Z_2$. Se poi per un altro sottospazio vettoriale W si ha $S \subseteq W$, allora sempre dalla definizione si deve avere $Z_1 \leq W$ e analogamente $Z_2 \leq W$. Ma anche Z_2 è un sottospazio di V e $S \subseteq Z_2$, dunque $Z_1 \leq Z_2$, e allo stesso modo $Z_2 \leq Z_1$, quindi $Z_1 = Z_2$. □

Definiamo ora la somma di sottospazi come l'insieme $U + W = \{u + w : u \in U, w \in W\}$: esso è un sottospazio vettoriale, infatti

$$(u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2) \in U + W$$
$$\lambda(u + w) = \lambda u + \lambda w \in U + W.$$

Dimostriamo inoltre che $U + W$ è lo spazio generato dall'unione dei due sottospazi, seguendo la definizione 2.2.3.

Teorema 2.2.5. Siano U, W sottospazi vettoriali di V su un campo K. Allora $\langle U \cup W \rangle \equiv U + W$.

Dimostrazione. Ogni $u \in U$ si può scrivere come $u + 0_W = u + 0_V$ che quindi appartiene a $U + W$, quindi $U \subseteq U + W$ e analogamente $W \subseteq U + W$, quindi $U \cup W \subseteq U + W$. Consideriamo un sottospazio vettoriale T di V che includa $U \cup W$: ogni elemento $u + w$ appartiene anche a T per qualunque u e w, ma allora $U + W$ è un sottoinsieme di T oltre che uno spazio vettoriale, e ciò lo rende un sottospazio vettoriale di T. Abbiamo allora dimostrato che $U + W$ soddisfa la definizione 2.2.1, perciò $U + W = \langle U \cup W \rangle$. □

2.3 Sistemi di generatori

Sia V uno spazio vettoriale su K, e $S \subseteq V$ un insieme non vuoto. Le combinazioni lineari (sempre finite!) di elementi di S sono definite come

$$\sum_{i=1}^{n} \lambda_i s_i = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_n s_n,$$

con $\lambda_i \in K$, $s_i \in S$ e $n \in \mathbb{N}$.

Teorema 2.3.1. Sia V uno spazio vettoriale su K, e $S \subseteq V$ non vuoto. Allora

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} \lambda_i s_i \colon \lambda_i \in K, s_i \in S, i = 1, 2, \ldots, n, n \in \mathbb{N} \right\}.$$

Dimostrazione. Questo particolare $\langle S \rangle$ deve soddisfare la definizione 2.2.3:

- gli elementi s_i appartengono a S, e possiamo esprimerli come $s_i = 1_K s_i$ quindi $S \subseteq \langle S \rangle$;
- se $W \leq V$ e $S \subseteq W$, allora dato che $\langle S \rangle \supseteq S$ se prendiamo una combinazione lineare di due elementi di S, lo è anche di elementi di W, e poiché il risultato è sempre un elemento di $\langle S \rangle$ quest'ultimo è un sottospazio vettoriale di W. □

Per l'unicità del sottospazio generato, questa è anche l'unica forma che $\langle S \rangle$ assume.

Definizione 2.3.2. *Sia V uno spazio vettoriale sul campo K e sia $S \subseteq V$ un insieme non vuoto. S è detto* sistema di generatori *per V se $\langle S \rangle = V$.*

Il fatto che con alcuni elementi di uno spazio $V = \langle S \rangle$ possiamo ricostruire tramite delle combinazioni lineari tutti i restanti è molto utile, in quanto possiamo dedurre molte proprietà di V studiando soltanto S. La situazione però si può ancora migliorare, come vedremo in seguito: il problema principale è che, senza ulteriori ipotesi, potrebbero esistere molti modi di esprimere $v \in V$ in termini di combinazioni lineari di elementi di S.

Esempi

- Come già detto, i vettori di $\mathbb{R}^n$ sono definiti dalle loro coordinate, quindi possono essere scritti come combinazioni lineari di questi elementi: allora

$$\mathbb{R}^n = \left\langle \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\} \right\rangle$$

  I vettori dello spazio generatore sono a tutti gli effetti dei versori di $\mathbb{R}^n$; in questo esempio sono i versori allineati con gli assi cartesiani.

- $\mathbb{R}[x]$ è generato da $\{1, x, x^2, \dots, x^n, \dots\}$; questo insieme è infinito, perché non esiste un polinomio "di grado massimo". Ogni $x \in \mathbb{R}[x]$ è determinato da una combinazione lineare di questi componenti, in modo univoco.
- In $\mathbb{R}^2$ si può individuare il sistema di generatori $\left\{\binom{0}{1}, \binom{1}{0}, \binom{1}{1}\right\}$. Con questo insieme però si può scrivere l'elemento $\binom{2}{2}$ in due modi diversi, ossia come $2\binom{0}{1} + 2\binom{1}{0} + 0\binom{1}{1}$ ma anche come $0\binom{0}{1} + 0\binom{1}{0} + 2\binom{1}{1}$.

Definizione 2.3.3. *Sia V uno spazio vettoriale su K, e $\{v_i\}_{i\in I} \subseteq V$. Si dice che l'insieme $\{v_i\}_{i\in I}$ è* linearmente dipendente *se esiste $I_0 \subseteq I$, di cardinalità n finita, e un insieme di scalari $\{\lambda_i\}_{i\in I}$ non tutti nulli tali per cui*

$$\sum_{i\in I} \lambda_i v_i = 0_V.$$

Nell'ultimo degli esempi precedenti l'insieme $\left\{\binom{0}{1}, \binom{1}{0}, \binom{1}{1}\right\}$ è linearmente dipendente.
Ovviamente, un sistema che non è linearmente dipendente si dice *linearmente indipendente.*

Definizione 2.3.4. *Un insieme finito di vettori $\{v_1, v_2, \dots, v_k\}$ si dice* linearmente indipendente*, se in ogni combinazione lineare dei k vettori che produce 0_V i coefficienti sono tutti nulli:*

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0_V \quad \Rightarrow \quad \lambda_1 = \lambda_2 = \cdots = \lambda_k = 0_K.$$

Un insieme infinito di vettori $\{v_i\}_{i\in I}$ è linearmente indipendente se $\forall J \subseteq I$ di cardinalità finita $\{v_j\}_{j\in J}$ è linearmente indipendente.

Alcuni esempi di insiemi linearmente indipendenti:

- il sistema che genera $K_n[x]$, ossia $\{1, x, x^2, \dots, x^n\}$, è linearmente indipendente perché un polinomio è identicamente nullo se e solo se tutti i coefficienti dei vari termini sono nulli. Lo stesso vale per i polinomi di grado non limitato di $K[x]$, poiché la definizione è verificata da "blocchi" di termini.
- l'insieme $\{v, w, 0_V, z\} \subset V$ spazio vettoriale su K non lo è, poiché $0_K v + 0_K w + 1_K 0_V + 0_K z = 0_V$ anche se uno dei coefficienti, 1_K, non è nullo. In generale ogni insieme che contenga l'elemento nullo dello spazio è sempre linearmente dipendente.

Il seguente teorema indica un modo più semplice di verificare questa definizione.

Teorema 2.3.5. Un insieme di vettori $\{v_i\}_{i\in I} \subset V$ è linearmente dipendente se e solo se almeno uno di essi è una combinazione lineare di un numero finito dei rimanenti.

Dimostrazione. Sia dato un insieme $\{v_i\}_{i=1}^k$ linearmente dipendente: esiste allora una combinazione lineare $\sum_{n=1}^k \lambda_n v_n = 0_V$ senza che tutti i λ_n siano nulli. Trascurando nella serie gli eventuali termini nulli, possiamo allora scrivere $\lambda_1 v_1 = -\lambda_2 v_2 - \cdots - \lambda_n v_n$. Poiché λ_1 non è nullo, esiste il suo inverso rispetto al rapporto, $(\lambda_1)^{-1}$, e moltiplicando la precedente equazione per questo risulta che il primo termine è $(\lambda_1)^{-1}(\lambda_1 v_1) = (\lambda_1^{-1}\lambda_1)v_1 = v_1$ da cui

$$v_1 = (\lambda_1^{-1})(-\lambda_2 v_2 - \cdots - \lambda_n v_n),$$

cioè v_1 è combinazione lineare degli altri vettori dell'insieme.

Viceversa, sia $v^* \neq 0_V$ un vettore dell'insieme dato, combinazione lineare (in cui quindi i coefficienti non possono essere tutti nulli) di alcuni dei vettori rimanenti, quindi

$$v^* = \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_r v_r.$$

Portando tutto al primo termine risulta $v^* - \mu_1 v_1 - \mu_2 v_2 - \cdots - \mu_r v_r = 0_V$ sebbene non siano tutti nulli, ossia l'insieme dei v_i è linearmente dipendente. □

2.4 Basi e dimensioni

Definizione 2.4.1. *Si chiama* base *di uno spazio vettoriale V ogni sistema S linearmente indipendente che genera S.*

La base in un certo senso "codifica" tutto ciò che è necessario sapere dello spazio vettoriale: tramite delle combinazioni lineari possiamo ricostruire tutto lo spazio a partire da un numero limitato di elementi. Il vantaggio delle basi è che esiste sempre un unico modo di esprimere ogni vettore dello spazio in termini dei suoi elementi, come dimostriamo nel teorema seguente.

Teorema 2.4.2. Sia $\{e_i\}_{i\in I}$ un insieme di V. Esso è una base di V se e solo se ogni elemento $v \in V$ non nullo si può scrivere in modo univoco come combinazione lineare finita, a coefficienti non nulli, di elementi di $\{e_i\}_{i\in I}$.

Gli elementi v non devono essere nulli, perché 0_V si può scrivere come combinazione lineare di *qualunque* sistema di vettori; inoltre i coefficienti della combinazione non devono essere nulli poiché altrimenti si potrebbe affermare che $v = ae_1 + be_2$ ma anche $v = ae_1 + be_2 + 0_K e_3 + \cdots + 0_K e_n + \ldots$ a piacere.

Dimostrazione. Dimostriamo che la condizione è necessaria. Sia $\{e_i\}_{i\in I}$ una base di V: essa per definizione genera tutto V. Preso un elemento $v \in V$ non nullo, possiamo scriverlo come una combinazione lineare finita

$$v = \sum_{i\in I_0} \lambda_i e_i, \tag{2.4.1}$$

con $I_0 \subset I$ di cardinalità finita. Dimostriamo che questa scrittura è unica: supponiamo che $\forall i \in I_0$ $\lambda_i \neq 0_K$ (eventuali termini nulli nella combinazione lineare si trascurano), e supponiamo che esista anche

$$v = \sum_{j\in J_0} \mu_j e_j \tag{2.4.2}$$

con $\mu_j \neq 0_K$ $\forall j \in J_0 \subset I$ e tale J_0 di cardinalità finita. Sommando gli opposti della (2.4.2) alla (2.4.1) si ha

$$\sum_{i\in I_0} \lambda_i e_i + \sum_{j\in J_0} -\mu_j e_j = 0_V.$$

Sia $I_0 \neq J_0$, e prendiamo $j_0 \in J_0$ ma $\notin I_0$. L'elemento e_{j_0}, nella combinazione, è associato a un coefficiente $-\mu_{j_0} \neq 0_K$ (quindi esiste il suo reciproco). Portando $-\mu_{j_0} e_{j_0}$ al secondo membro dell'uguaglianza e moltiplicando per il reciproco di μ_{j_0} risulta

$$\sum_{i\in I_0} (\lambda_i \mu_{j_0}^{-1}) e_i + \sum_{j\in J_0} (\mu_j \mu_{j_0}^{-1}) e_j = e_{j_0},$$

cioè uno degli e_i è espresso come combinazione lineare degli altri, vale a dire la base è linearmente dipendente, il che è assurdo: quindi non può esistere un j_0 che appartiene a J_0 ma non a I_0. Ponendo $j_0 \in I_0$ e $\notin J_0$ si ottiene allo stesso modo un altra contraddizione. Allora non può che essere $I_0 = J_0$, ma ciò significa che

$$\sum_{i\in I_0} (\lambda_i - \mu_i) e_i = 0_V,$$

cui segue che $\lambda_i = \mu_i$ $\forall i \in I_0$, cioè le (2.4.1) e (2.4.2) sono identiche: dunque la scrittura di v in termini della base è unica.

Mostriamo ora che la condizione è anche sufficiente: innanzitutto, $\langle \{e_i\}_{i\in I} \rangle = V$ perché per ipotesi possiamo scrivere ogni vettore di V come combinazione lineare di elementi di questo insieme. Supponiamo per assurdo che $\{e_i\}_{i\in I}$ sia linearmente dipendente, ossia che esista $I_0 \subset I$ di cardinalità finita per cui

$$\sum_{i\in I_0} \lambda_i e_i = 0_V, \tag{2.4.3}$$

e come prima che $\lambda_i \neq 0_K \ \forall i \in I_0$. Considerando un $i^* \in I_0$, λ_{i^*} non è nullo, quindi moltiplicando la (2.4.3) per il suo inverso si trova

$$\sum_{i \in I_0} (\lambda_{i^*}^{-1} \lambda_i) e_i = 0_V.$$

Isolando il termine in i^* si ottiene poi che

$$\sum_{i^* \neq i \in I_0} (\lambda_{i^*}^{-1} \lambda_i) e_i = -e_{i^*} \tag{2.4.4}$$

vale a dire che e_{i^*} si esprime come combinazione lineare di altri elementi dell'insieme. Ma allora ogni volta che scriviamo un vettore come combinazione lineare che contenga e_{i*} possiamo scegliere di usare, indifferentemente, il primo o il secondo membro della (2.4.4), e ciò viola l'ipotesi che la scrittura di ogni vettore di V in termini degli e_i sia unica. Dunque un tale I_0 non può esistere: dunque l'insieme è linearmente indipendente, e dato che genera V è una sua base. □

Definizione 2.4.3. *Sia V uno spazio vettoriale su K: esso si dice di dimensione finita se ammette un sistema finito di generatori, altrimenti si dice di dimensione infinita.*

Teorema 2.4.4. Sia $G \subset V$ un sistema di generatori di V finito. Se $S \subseteq G$ è linearmente indipendente, allora esiste una base B di V tale che $S \subseteq B \subseteq G$.

Dimostrazione. Si supponga che V abbia dimensione finita: allora esiste un sistema di generatori G.[1] Escludiamo il caso in cui $V \equiv \{0_V\}$ perché non esisterebbe nemmeno una base.

Indichiamo con S_n il fatto che nell'insieme linearmente indipendente S ci siano n vettori. Potrebbe essere che $\langle S_n \rangle \equiv V$, ma allora possiamo scegliere subito S_n come base per V, e poiché $B = S_n \subseteq G$ il teorema è dimostrato. Sia allora $\langle S_n \rangle \neq V$: deve esistere $x_{n+1} \in G$, ma $\notin \langle S_n \rangle$ (perché altrimenti dato che $\langle S \rangle \supseteq G$ si avrebbe che $\langle S_n \rangle \equiv V$). Definiamo $S_{n+1} = S_n \cup \{x_{n+1}\}$, per cui sicuramente vale $S_n \subseteq S_{n+1} \subseteq G$. Questo S_{n+1} è un insieme linearmente indipendente, altrimenti avremmo che $x_{n+1} \in \langle S_n \rangle$. Se $\langle S_{n+1} \rangle = V$ il teorema è dimostrato, altrimenti procediamo aggiungendo un altro elemento di $G \setminus \langle S_{n+1} \rangle$. Iteriamo il processo per $n+2$, $n+3$ e così via: il processo deve necessariamente terminare poiché

$$S_n \subseteq S_{n+1} \subseteq S_{n+2} \subseteq \cdots \subseteq G$$

e G è finito. Esisterà dunque $k \in \mathbb{N}$ per cui $\langle S_{n+k} \rangle = \langle G \rangle$, e anche in questo caso abbiamo trovato che S_{n+k} (che è ancora linearmente indipendente per costruzione) è base di V. □

Sempre in $\mathbb{R}^3$, per esempio, una delle possibili basi è quella composta dai tre versori $\{e_1, e_2, e_3\} = \{(1,0,0), (0,1,0), (0,0,1)\}$, ma anche $\{e_1, e_2, e_2 + e_3\}$ è un'altra base. In effetti ruotando e_1, e_2 e e_3 di un angolo qualsiasi si ottiene un altra base, e se ne ottengono ancora delle altre moltiplicando per degli scalari (anche differenti) i tre versori. Quindi le basi di uno spazio vettoriali sono infinite; quello che non cambia è il numero di elementi di queste basi, che è sempre costante (in questo esempio, la base è sempre composta da tre vettori).

Corollario 2.4.5. Ogni spazio vettoriale $V \neq \{0_V\}$ di dimensione finita ammette almeno una base.

Dimostrazione. L'esistenza di un sistema di generatori G per V è garantita (semmai prendiamo $G = V$). In tale insieme, un elemento singolo $v \neq 0_V$ forma da solo un insieme linearmente indipendente $\{v\}$. Il teorema precedente assicura dunque l'esistenza di una base $\mathcal{B}$ di V tale che $\{v\} \subseteq \mathcal{B} \subseteq G$. □

Teorema 2.4.6. Sia V uno spazio vettoriale di dimensione finita, contenente una base di n vettori. Allora:

[1] Esiste sempre un sistema di generatori per qualsiasi spazio: nel peggiore dei casi, V genera se stesso, ossia $\langle V \rangle = V$, dunque possiamo prendere $G = V$. La dimensione finita di V ci assicura che esiste un tale G finito.

1. ogni sistema linearmente indipendente S di n vettori è una base di V;
2. ogni sistema U di $m > n$ vettori è linearmente dipendente;
3. ogni sistema W di $m < n$ vettori non può generare V, cioè $\langle W \rangle \neq V$;
4. ogni sistema T di n vettori per cui $\langle T \rangle = V$ è una base.

Dimostrazione.

1. Siano $\{e_i\}_{i=1}^n$ una base di V, e $S = \{f_i\}_{i=1}^n$ un insieme finito linearmente indipendente. Allora
$$f_1 = \sum_{i=1}^{n} \lambda_i e_i.$$
Poiché S è linearmente indipendente, almeno un λ_i non è nullo, quindi $f_1 \neq 0_V$, e riordinando i vettori nella combinazione possiamo supporre che sia $\lambda_1 \neq 0_K$: in questo modo $\lambda_1 e_1 \neq 0_V$. Portando quest'ultimo termine al secondo membro e moltiplicando per $\mu_1 = \lambda_1^{-1}$ risulta con opportuni $\mu_i \in K$ che
$$e_1 = \mu_1 f_1 + \sum_{i=2}^{n} \mu_i e_i.$$
Ogni vettore di V è una combinazione lineare di elementi di $\{e_i\}_{i=1}^n$, ma sostituendo e_1 con l'espressione trovata sopra abbiamo $\forall v \in V$
$$v = \sum_{i=1}^{n} \lambda_i e_i = \lambda_1 \left(\mu_1 f_1 + \sum_{i=2}^{n} \mu_i e_i \right) + \sum_{i=2}^{n} \lambda_i e_i$$
che quindi può essere espresso anche come combinazione lineare di $\{f_1, e_2, \ldots, e_n\}$ anziché degli $\{e_i\}_{i=1}^n$, quindi anche l'insieme $\{f_1, e_2, \ldots, e_n\}$ è un sistema di generatori di V. Dunque troviamo anche che
$$f_2 = \sigma_1 f_1 + \sum_{i=1}^{n} \sigma_i e_i.$$
Almeno uno dei σ_i non è nullo, altrimenti sarebbe che $f_2 = \sigma_1 f_1$ che contraddice l'indipendenza lineare degli f_i. Supponendo $\sigma_2 \neq 0_K$, si esplicita e_2 moltiplicando per σ_2^{-1}, ottenendo
$$e_2 = \rho_1 f_1 + \rho_2 f_2 + \sum_{i=3}^{n} \rho_i e_i.$$
L'insieme $\{f_1, f_2, e_3, \ldots, e_n\}$ è ancora un sistema di generatori di V. Si itera il procedimento ottenendo alla fine che $\{f_1, f_2, \ldots, f_n\}$ è ancora un sistema di generatori per V, e dunque ne è una base dato che è linearmente indipendente.

2. Sia U con $m > n$ elementi linearmente indipendente, e si prenda $U' \subset U$ tale che abbia n elementi (dunque $U \setminus U' \neq \varnothing$). Per il punto 1 U' è una base di V, quindi i vettori di U' generano anche quelli di $U \setminus U'$. Ciò contraddice l'indipendenza lineare di U, che deve essere quindi linearmente dipendente.

3. Sia W con $m < n$ elementi un sistema di generatori di V: allora deve esistere una base con al più m vettori, tanti quanti ce ne sono in W. Per il punto precedente, la base $\{e_i\}_{i \in I}$ (considerata nel punto 1) ha più vettori della base estratta da W, quindi sarebbe linearmente dipendente, che è assurdo. Allora W non può essere un sistema di generatori di V.

4. Se $\langle T \rangle = V$, T deve avere almeno n elementi per il punto 3; allora esiste $T' \subseteq T$ che è una base di V. Se T' avesse meno di n elementi, contraddirrebbe il punto 3 prima citato, quindi deve averne esattamente n, perciò $T \equiv T'$, e T è linearmente indipendente. Poiché genera V, T ne è anche una base.

□

Corollario 2.4.7. Sia V uno spazio vettoriale di dimensione finita, contenente una base di n vettori. Ogni altra base V ha a sua volta esattamente n vettori.

Definizione 2.4.8. *Dato uno spazio vettoriale $V \neq \{0_V\}$ su K di dimensione finita, si dice* dimensione *di V su K il numero di vettori di una sua base qualunque.*

La dimensione di V (su K) si indica con $\dim_K V$ o anche solo, se non ci sono ambiguità, con $\dim V$. Convenzionalmente, allo spazio contenente soltanto $\{0_V\}$ si assegna la dimensione 0.

Ad esempio, preso un campo generico K, nello spazio K^n (insieme delle n-uple di elementi in K) possiamo vedere facilmente che ogni base possiede n elementi, dunque $\dim_K K^n = n$. La dimensione può cambiare però se modifichiamo il campo su cui definiamo lo spazio vettoriale: un noto esempio è $\mathbb{C}^n$. Ovviamente, sul campo complesso, abbiamo $\dim_{\mathbb{C}} \mathbb{C}^n = n$; allo stesso tempo, però, possiamo vedere $\mathbb{C}^n$ come spazio vettoriale su $\mathbb{R}$: ogni componente di un vettore di $\mathbb{C}^n$ è una coppia di numeri reali, perciò $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$.

Teorema 2.4.9. Sia V uno spazio vettoriale su un campo K, e W un suo sottospazio. Se $\dim_K V$ è finita, allora $\dim_K W \leq \dim_K V$.

Dimostrazione. Nel caso banale in cui $W = \{0_V\}$, la sua dimensione è 0 quindi è ovviamente minore o uguale della dimensione di V, qualunque essa sia.

Siano $m := \dim_K W$ e $n := \dim_K V$. Se W non contiene soltanto il vettore nullo, una base $\mathcal{B}$ (che possiede m elementi) qualunque di W è un insieme linearmente indipendente anche in V. Se $m > n$, per il teorema 2.4.6 $\mathcal{B}$ sarebbe linearmente dipendente, il che è assurdo poiché è una base, dunque $\dim_K W = m \leq n = \dim_K V$. □

Teorema 2.4.10. Sia V uno spazio vettoriale di dimensione finita, W un suo sottospazio e $\mathcal{B}_W$ una base di W. Allora tale base si può estendere per formare una base di V, cioè $\exists \mathcal{B}_V : \mathcal{B}_W \subseteq \mathcal{B}_V$.

Dimostrazione. Prendiamo una base $\mathcal{B}_W$ di W e un sistema di generatori G, finito, di V. Sicuramente $\mathcal{B}_W \cup G$ genera ancora V. Esso contiene inoltre la base di W che per definizione è linearmente indipendente. Per il teorema 2.4.4 allora possiamo trovare una base $\mathcal{B}_V$ di V tale che $\mathcal{B}_W \subseteq \mathcal{B}_V \subseteq (\mathcal{B}_W \cup G)$, e ciò prova la tesi. □

Ad esempio, $\mathbb{R}$ è un sottospazio di $\mathbb{R}^3$: prendendo una base $\{v\}$ del primo, si ottiene una base del secondo semplicemente aggiungendo due vettori (distinti) perpendicolari a v.

Definizione 2.4.11. *Un insieme $\{V_i\}_{i \in I}$ di sottospazi vettoriali di V si dice linearmente indipendente se comunque si scelga un vettore $x_i \neq 0$ per ciascun V_i, l'insieme $\{x_i\}_{i \in I}$ è linearmente indipendente.*

Teorema 2.4.12. Un insieme $\{V_i\}_{i \in I}$ di sottospazi vettoriali di V è linearmente indipendente se e solo se $\forall k \in I$ si ha che l'intersezione tra V_k e lo spazio generato dai restanti V_i contiene soltanto lo zero, cioè[2]

$$V_k \cap \sum_{j \in I \setminus \{k\}} V_j = \{0\}.$$

Dimostrazione. Se i sottospazi V_i sono linearmente indipendenti, e per assurdo $V_k \cap \sum_{j \in I \setminus \{k\}} V_j \neq \{0\}$ per qualche $k \in I$, allora esisterebbe un elemento $v_k \in V_k$ non nullo che è combinazione lineare di elementi dei restanti sottospazi, cioè $v_k = x_{i_1} + \cdots + x_{i_r}$ con $\{i_1, \ldots, i_r\} \subseteq I \setminus \{k\}$. Ma allora l'insieme $\{V_i\}_{i \in I}$ dei sottospazi non sarebbe linearmente indipendente, contraddicendo l'ipotesi, quindi l'uguaglianza deve essere vera.

Viceversa, se prendessimo una combinazione lineare nulla di elementi uno da ciascun sottospazio

$$a_{i_1} v_{i_1} + \cdots + a_{i_k} v_{i_k} = 0 \tag{2.4.5}$$

[2]Ricordiamo che la somma di più spazi vettoriali è lo spazio generato dalla loro unione, ossia $\sum_i V_i = \left\langle \bigcup_i V_i \right\rangle$.

con $v_{i_j} \in V_{i_j}$ appartenenti tutti a sottospazi distinti, e ci fosse $a_{i^*} \neq 0$, allora potremmo scrivere

$$v_{i^*} = \sum_{j \in I \setminus \{i^*\}} c_j v_j \tag{2.4.6}$$

ma allora $v_{i^*} \in V_{i^*}$ e anche $v_{i^*} \in \sum_{j \in I \setminus \{i^*\}} V_j$, ossia esiste un $i^* \in I$ tale per cui

$$V_{i^*} \cap \sum_{j \in I \setminus \{i^*\}} V_j \neq \{0\}$$

che contraddice l'ipotesi. Dunque nella (2.4.5) si ha $a_j = 0$ per ogni $j \in I$, cioè i sottospazi sono linearmente indipendenti. □

Teorema 2.4.13. Sia $\{V_i\}_{i \in I}$ un insieme linearmente indipendente di sottospazi vettoriali di V. Se $\forall i \in I$ il sistema di vettori $S_i \subset V_i$ è linearmente indipendente, allora $\bigcup_{i \in I} S_i$ è linearmente indipendente in V.

Dimostrazione. Consideriamo un sistema linearmente indipendente di vettori $S_i = \{x_k\}_{k=1}^{n_i} \subset V_i$ e ipotizziamo per assurdo che l'unione non sia linearmente indipendente. Questo implica che, considerando gli elementi $x_k^i \in S_i$ con $i \in I_0$ e $1 \leq k \leq n_i$ (in cui $I_0 \in I$ ha cardinalità finita) troviamo

$$\sum_{1 \leq k \leq n_i} \lambda_k^i x_k^i = 0,$$

con λ_k^i nulli per ogni i, k tranne (almeno) un $\lambda_{k^*}^{i^*}$. Posto $y^i = \sum_{k=1}^{n_i} \lambda_k^i x_k^i$ sappiamo che $\sum_{i \in I_0} y^i = 0$ e che $y^{i^*} \neq 0$, ma allora

$$y^{i^*} = -\sum_{i \in I_0 \setminus \{i^*\}} y^i \quad \Rightarrow \quad V_{i^*} \cap \sum_{i \in I_0 \setminus \{i^*\}} V_i \ni y^{i^*} \neq 0$$

che contraddice l'indipendenza lineare dei sottospazi, per il teorema 2.4.12. L'unione S dei vari S_i è allora linearmente indipendente. □

Definizione 2.4.14. *Uno spazio vettoriale V si dice* somma diretta *di un insieme di sottospazi vettoriali $\{V_i\}_{i \in I}$ se $\{V_i\}_{i \in I}$ è linearmente indipendente e se $\sum_{i \in I} V_i = V$.*

Per indicare che V è composto dalla somma diretta degli spazi V_i si usa la scrittura $V = \bigoplus_{i \in I} V_i$. Per verificare che due spazi siano in somma diretta, per esempio che $V = W \oplus U$, dove W, U sono sottospazi di V, è sufficiente verificare che:

- $U + W = V$, cioè $\langle U \cup W \rangle = V$, ossia che l'unione delle basi contenga una base di V;
- $U \cap W = \{0\}$.

Esempi

- Lo spazio $\mathbb{R}[x]$ è generato dall'insieme $\{1, x, x^2, \dots\}$. Posto $V_j = \langle \{x^j\} \rangle$, con $j \in \mathbb{N}_0$, si ha che
$$\mathbb{R}[x] = \bigoplus_{j \in \mathbb{N}_0} V_j.$$
- In $\mathbb{R}^3$, siano $V_1 = \left\langle \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \right\rangle$ e $V_2 = \left\langle \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \right\rangle$. Certamente $V_1 + V_2 = \mathbb{R}^3$, ma la somma non è diretta poiché la loro intersezione è l'asse y.

2.5 Spazi quoziente

Sia W un sottospazio vettoriale di V. Definiamo la relazione $x \sim y$, con $x, y \in V$, se $x - y \in W$. È una relazione di equivalenza, perché soddisfa le tre proprietà della definizione 1.2.1:

- è riflessiva perché $x - x = 0 \in W$ per ogni $x \in V$;
- è simmetrica perché se $x - y = w \in W$, allora $-w = y - x \in W$;
- è transitiva perché se $x - y = w_1 \in W$ e $y - z = w_2 \in W$ allora anche $w_1 + w_2 = x - y + (y - z) = x - z \in W$.

Prendiamo un elemento $a \in V$: la sua classe di equivalenza, detta anche classe laterale, è formata dunque da tutti i $v \in V$ tali che $a - v \in W$, cioè

$$[a]_W = \{x \in V \colon x - a = w \in W\} = \{w + a \colon w \in W\}.$$

Poiché ogni elemento di $[a]_W$ è somma di un elemento (qualsiasi) di W e di a, indichiamo la classe di equivalenza anche come $W + a$.[3] L'insieme delle classi di equivalenza definite da questa relazione è lo spazio quoziente $V \,/\, W$.

Esso possiede una struttura di spazio vettoriale, con le operazioni indotte da V sui rappresentanti. Più precisamente, definiamo la somma tra due classi e il prodotto per scalare come

$$(W + a) + (W + b) = W + a + b, \qquad \lambda(W + a) = W + \lambda a. \tag{2.5.1}$$

Le definizioni appaiono del tutto naturali se interpretiamo W in queste formule come un elemento, appunto, di W: allora troviamo $W + W = W$ e $\lambda W = W$, essendo che sommando due elementi di W o moltiplicandoli per uno scalare otteniamo ancora un elemento in W, per cui possiamo immaginare di svolgere le (2.5.1) proprio come normali operazioni tra vettori.

Osservazione 2.5.1. Se anche fosse $[a]_W = [a']_W$ e $[b]_W = [b']_W$, non è detto a priori che si abbia $[a + b]_W = [a' + b']_W$ o $[\lambda a]_W = [\lambda a']_W$ come conseguenza della proprietà transitiva.[4] Perché ciò accada serve un'ulteriore condizione, che la relazione sia una *relazione di congruenza*, ossia che sia compatibile con le operazioni in V. Questo fatto si verifica facilmente sfruttando la struttura di sottospazio vettoriale di W. Se $x \sim x'$ e $y \sim y'$, allora $x - x' = w_1$ e $y - y' = w_2$ per qualche $w_1, w_2 \in W$. Sommandoli, otteniamo $W \ni w_1 + w_2 = x - x' + y - y' = (x + y) - (x' + y')$: allora $x + y \sim x' + y'$. Anche per il prodotto con uno scalare $\lambda \in K$, si ottiene analogamente che se $z - z' = w_3 \in W$, allora si ha che $W \ni \lambda w_3 = \lambda(z - z') = \lambda z - \lambda z'$ perciò $\lambda z \sim \lambda z'$.

La terna $(V \,/\, W, +, \cdot)$ è dunque per quanto mostrato uno spazio vettoriale su K, dove V è a sua volta uno spazio vettoriale sul medesimo campo. Infatti, oltre alle proprietà appena dimostrate, esiste l'elemento neutro rispetto all'addizione, che è $W + 0_V$ (si indica anche solamente con W), e l'opposto, che è $-(W + a) = W + (-a)$.

Teorema 2.5.2. Sia $W \leq V$ con V di dimensione finita. La dimensione di V/W è finita e vale $\dim V - \dim W$.

Dimostrazione. Il sottospazio W ha certamente dimensione finita: siano $n \coloneqq \dim W$ e $n + m \coloneqq \dim V$. Sia $\{e_i\}_{i=1}^{n}$ una base di W. Essa si può estendere ad una base di V, per il teorema 2.4.10. Allora sia $\mathcal{B} = \{e_1, e_2, \ldots, e_n, f_{n+1}, \ldots, f_{n+m}\}$ una base di V.

Ora, presa una classe $W + a$, il rappresentante $a \in V$ si può scrivere come combinazione lineare degli elementi di $\mathcal{B}$:

$$a = \mu_1 e_1 + \cdots + \mu_n e_n + \mu_{n+1} f_{n+1} + \cdots + \mu_{n+m} f_{n+m}.$$

[3] È inutile in questo contesto specificare le classi laterali *destre* e *sinistre*, dato che la somma è commutativa, quindi $W + a = a + W$.

[4] Ovviamente con $a \neq a'$ e $b \neq b'$, altrimenti sarebbe ovvia.

Poiché i termini fino a $\lambda_n e_n$ individuano un elemento di W, risulta $W + a = W + \mu_1 f_{n+1} + \cdots + \mu_m f_{n+m}$. Per come è definita la somma nello spazio quoziente questo è equivalente ad $W + a = \mu_1(W + f_{n+1}) + \cdots + \mu_m(W + f_{n+m})$: l'insieme $\{W + f_{n+i}\}_{i=1}^m$ genera dunque V / W.

Verifichiamo che è anche linearmente indipendente. Prendiamo una combinazione lineare nulla

$$\lambda_1(W + f_{n+1}) + \lambda_2(W + f_{n+2}) + \cdots + \lambda_m(W + f_{n+m}) = 0_{V/W} = W + 0_V. \tag{2.5.2}$$

Essa è per definizione equivalente a $W + (\lambda_1 f_{n+1} + \cdots + \lambda_m f_{n+m})$. Per l'uguaglianza precedente, quindi, deve essere

$$\sum_{i=1}^{m} \lambda_i f_{n+i} \sim 0_V \quad \Rightarrow \quad \sum_{i=1}^{n} \lambda_i f_{n+i} \in W. \tag{2.5.3}$$

Ma gli f_{n+i} sono tutti vettori che non appartengono a W: dato che formano insieme agli e_i la base $\mathcal{B}$, non è possibile che una combinazione lineare degli f_{n+i} dia un elemento di W (che, ricordiamo, è generato da $\{e_i\}_{i=1}^n$), altrimenti $\mathcal{B}$ sarebbe linearmente dipendente. Se la loro somma deve essere in W, quindi, l'unico modo è che tutti i λ_i siano nulli. Ma allora l'insieme $\{W + f_{n+i}\}_{i=1}^m$ è linearmente indipendente, come volevasi dimostrare: perciò è una base di V / W.

La dimensione dello spazio quoziente è di conseguenza $\dim V / W = m = \dim V - \dim W$. □