Capitolo 1

Preliminari di algebra

1.1 Operazioni su insiemi

Definizione 1.1.1 (Prodotto cartesiano)**.** Dati due insiemi A, B, il loro **prodotto cartesiano**, indicato con $A \times B$, è l'insieme delle coppie ordinate (a, b) con $a \in A$ e $b \in B$, cioè $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Esempio 1.1.2. *1. Se $A = \{1, 2, 3\}$, $B = \{a, b\}$, allora*

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

2. Sia $\mathbb{R}$ l'insieme dei numeri reali, allora

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2.$$

Notiamo che le coppie sono ordinate, dunque per esempio $(1, 2) \neq (2, 1)$.

Definizione 1.1.3 (Operazione interna)**.** Sia S un insieme non vuoto. Un'**operazione interna in S o legge di composizione interna in S** è un'applicazione

$$S \times S \to S$$

avente dominio $S \times S$ e codominio S. Per esempio una tale operazione può essere denotata con uno dei simboli $*$, oppure $+$, o $\cdot$, o con altri simboli; nel primo caso essa associa ad una coppia (a, b) un elemento di S, denotato $a * b$.

Notare che il termine "applicazione" è sinomino di "funzione". Un altro termine usato a volte con lo stesso significato è "mappa".

Esempio 1.1.4. *Esempi di operazione interne.*

(i) $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*, la somma è un'operazione interna in $\mathbb{Z}$;*
$(a, b) \to a + b$*; per esempio*
$(1, 2) \to 1 + 2 = 3$.

(ii) $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, *il prodotto è un'operazione interna in* $\mathbb{Q}$;

$(x, y) \to x \cdot y$; *per esempio*

$(1, 2) \to 1 \cdot 2 = 2$.

(iii) Sia $X \neq \emptyset$ *un insieme non vuoto e sia* F *l'insieme delle applicazioni di* X *in* X, *cioè aventi* X *sia come dominio sia come codominio. Si noti che* F *non è vuoto in quanto contiene almeno l'applicazione identica* $id_X : X \to X$, *tale che* $id_X(x) = x$ *per ogni* $x \in X$.

$\circ : F \times F \to F$, *la composizione è un'operazione interna in* F;

$(f, g) \to f \circ g$, *dove* $f \circ g$ *è l'applicazione tale che* $(f \circ g)(x) = f(g(x))$ *per ogni* $x \in X$.

Gli esempi (i) e (ii) sono esempi di operazioni numeriche.

1.2 Gruppi

Definizione 1.2.1 (Gruppo)**.** Sia G un insieme e $*$ sia un'operazione in G. La coppia $(G, *)$ è detta un **gruppo** se valgono le seguenti proprietà:

(i) *Proprietà associativa*: per ogni $a, b, c \in G$, si ha $a * (b * c) = (a * b) * c$;

(ii) *Esistenza dell'elemento neutro*: esiste $e \in G$ tale che, per ogni $a \in G$, si ha $e * a = a * e = a$; e è detto elemento neutro di G;

(iii) *Esistenza dei simmetrici, o reciproci*: per ogni $a \in G$ esiste $a' \in G$ tale che $a * a' = e = a' * a$. a' è detto reciproco di a.

Se l'operazione è indicata additivamente, ossia con il simbolo $+$, l'elemento neutro è detto "zero" e indicato 0, mentre il reciproco di a è detto opposto di a e indicato $-a$. Se l'operazione è indicata moltiplicativamente, ossia con il simbolo $\cdot$ o $\times$, l'elemento neutro è detto "uno" o unità di G e indicato 1 o 1_G, mentre il reciproco di a è detto inverso di a e indicato a^{-1}.

Definizione 1.2.2 (Gruppo abeliano)**.** Il gruppo $(G, *)$ è detto **gruppo abeliano**, o commutativo, se vale la *proprietà commutativa*, cioè per ogni $a, b \in G$ vale $a * b = b * a$.

Esempio 1.2.3.

1. $(\mathbb{Z}, +)$ *è un gruppo abeliano.*

2. $(\mathbb{Z}, \cdot)$ *non è un gruppo: la proprietà associativa è verificata, e l'*1 *esiste, però alcuni elementi non hanno l'inverso in* $\mathbb{Z}$, *si dice che "non sono invertibili" in* $\mathbb{Z}$. *Per esempio* 0 *non ha inverso, e anche* $2 \cdot z \neq 1$ *per ogni* $z \in \mathbb{Z}$, *quindi* 2 *non è invertibile in* $\mathbb{Z}$.

3. $(\mathbb{Q}, +)$ *è un gruppo abeliano.*

4. $(\mathbb{Q} \setminus \{0\}, \cdot)$ *è un gruppo abeliano.*

   Infatti, osserviamo innanzitutto che il prodotto è un'operazione interna in $\mathbb{Q} \setminus \{0\}$*, perchè il prodotto di due numeri razionali non nulli è non nullo. Poi: vale la proprietà associativa, l'elemento neutro è l'*1*, e per ogni* $q \in \mathbb{Q} \setminus \{0\}$ *esiste* $q^{-1} = \frac{1}{q}$ *tale che* $q \cdot \frac{1}{q} = \frac{1}{q} \cdot q = 1$*.*

5. *Sia* $X \neq \emptyset$ *un insieme e sia* $I(X) = \{f : X \to X \mid f \text{ biiettiva}\}$ *l'insieme delle applicazioni biunivoche di* X *in sè.*

   $(I(X), \circ)$ *è un gruppo. Infatti:*

   (i) se $f, g : X \to X$ *sono biiettive, anche* $f \circ g$ *lo è, dunque la composizione è un'operazione interna in* $I(X)$*;*

   (ii) la composizione di funzioni è associativa: $(f \circ g) \circ h = f \circ (g \circ h)$*. Infatti per ogni* $x \in X$ *si ha* $((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$*.*

   (iii) l'applicazione identica $id_X : x \to x$*, per ogni* $x \in X$*, è l'elemento neutro di* $I(X)$*;*

   (iv) ricordiamo che un'applicazione è biiettiva se e solo se esiste l'applicazione inversa $f^{-1} : X \to X$*, tale che* $f(x) = y$ *se e solo se* $f^{-1}(y) = x$*. Infatti* f *è suriettiva e iniettiva, se e solo se, preso comunque un elemento* $y \in X$*, esiste ed è unico* $x \in X$ *tale che* $f(x) = y$*. L'applicazione* f^{-1} *è l'elemento inverso di* f *rispetto all'operazione* $\circ$*.*

Osserviamo che tutti i gruppi "numerici" sono abeliani. Invece il gruppo $I(X)$ non è abeliano se X ha almeno tre elementi.

Per esempio, sia $X = \{1, 2, 3\}$. Definiamo $f : X \to X$ ponendo

$$f(1) = 2, f(2) = 3, f(3) = 1,$$

e $g : X \to X$ ponendo

$$g(1) = 1, g(2) = 3, g(3) = 2.$$

Chiaramente $f \circ g \neq g \circ f$, in quanto esiste almeno un elemento $x \in X$ tale che $(f \circ g)(x) \neq (g \circ f)(x)$.

Osserviamo che in questo caso $I(X)$ ha sei elementi, corrispondenti alle permutazioni dell'insieme X; si veda il Capitolo 11.

Esercizi 1.

1. Costruire un esempio analogo al precedente per X insieme di n elementi, con $n \geq 3$ qualunque.

2. Se X ha n elementi, quanti elementi ha $I(X)$?

Proposizione 1.2.4. *Sia* $(G, *)$ *un gruppo.*

1. *L'elemento neutro in* G *è unico.*

2. *Ogni elemento* $g \in G$ *ha un unico reciproco.*

Dimostrazione. 1. Siano e, e' entrambi elementi neutri di G, ossia elementi di G tali che, per ogni $g \in G$, si ha $e * g = g * e = g$ e $e' * g = g * e' = g$. Allora $e * e' = e'$ perchè e è neutro, ma anche $e * e' = e$ perchè e' è neutro. Dunque $e = e'$.

2. Supponiamo che g', g'' siano entrambi reciproci di g. Allora si ha $g * g' = g' * g = e$ e anche $g * g'' = g'' * g = e$. Quindi

$$g' = g' * e = g' * (g * g'') = \text{per la proprietà associativa} = (g' * g) * g'' = e * g'' = g''$$

In conclusione si ha $g' = g''$. □

1.3 Relazioni d'equivalenza

Per questa sezione si vedano anche le note del corso propedeutico (Prof. Del Santo).

Una **relazione** in un insieme X è una proprietà che una coppia ordinata di elementi di X può verificare o meno. Per esempio la relazione "$<$" "minore" ha senso negli insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$; la relazione "$||$" "parallelo" ha senso nell'insieme delle rette del piano, o dei piani dello spazio.

In maniera più formale, una relazione in X è un sottinsieme R del prodotto cartesiano $X \times X$. In tal caso si dirà che x è in relazione R con y se la coppia ordinata $(x, y) \in R$. Si scrive anche xRy.

Per esempio la relazione $<$ in $\mathbb{Z}$ corrisponde al sottinsieme di $\mathbb{Z} \times \mathbb{Z}$: $\{(x, y) \mid x < y\}$. Analogamente la relazione $\leq$ corrisponde al sottinsieme di $\mathbb{Z} \times \mathbb{Z}$: $\{(x, y) \mid x \leq y\}$. La relazione di parallelismo nell'insieme delle rette del piano corrisponde alle coppie di rette (r, r') tali che r, r' sono distinte e parallele oppure sono uguali.

Simboli spesso usati per denotare relazioni sono $\equiv$, $\sim$, $\simeq$, $\cong$, ecc. Un altro esempio di relazione, in $\mathbb{R}$, è il seguente: $x \sim y$ se e solo se $x^2 = y$.

Noi saremo interessati a un tipo particolare di relazioni dette relazioni d'equivalenza.

Definizione 1.3.1 (**Relazione d'equivalenza).** Sia X un insieme e $\sim$ una relazione in X. Si dice che $\sim$ è una **relazione d'equivalenza** se valgono le tre proprietà:

1. riflessiva: per ogni $x \in X$ $x \sim x$;
2. simmetrica: se $x \sim y$ allora $y \sim x$;
3. transitiva: se $x \sim y$ e $y \sim z$ allora $x \sim z$.

Esempio 1.3.2.

1. L'uguaglianza è una relazione d'equivalenza in qualunque insieme X.
2. "Essere congruenti" è una relazione d'equivalenza nell'insieme dei triangoli del piano.
3. $\leq, <$ non sono relazioni d'equivalenza.

Il prossimo è un esempio fondamentale. Denotiamo con $\mathbb{N}$ l'insieme dei numeri naturali: $\mathbb{N} = \{0, 1, 2, 3 \ldots\}$.

Definizione 1.3.3 (**Congruenza modulo n).** Si fissi un naturale $n \in \mathbb{N}$. La relazione di congruenza modulo n è la relazione in $\mathbb{Z}$ così definita:

$$x \equiv y \pmod{n} \text{ se e solo se esiste } k \in \mathbb{Z} \text{ tale che } x - y = kn.$$

Si scrive anche $x \equiv_n y$. Si legge "x è congruo a y modulo n.

Proposizione 1.3.4. *La relazione di congruenza modulo n è una relazione d'equivalenza in $\mathbb{Z}$.*

Dimostrazione. 1. $x - x = 0x$ per ogni $x \in \mathbb{Z}$.

2. Se $x \equiv_n y$, si ha $x - y = kn$ per un opportno $k \in \mathbb{Z}$. Allora $y - x = (-k)n$.

3. Se $x \equiv_n y$ e $y \equiv_n z$, esistono $k, h \in \mathbb{Z}$ tali che $x - y = kn$, $y - z = hn$; ma allora $x - z = (x - y) + (y - z) = kn + hn = (k + h)n$, il che prova che $x \equiv_n z$. □

D'ora in poi supporremo sempre $n \geq 2$. La seguente osservazione è importante.

Proposizione 1.3.5. *$x \equiv_n y$ se e solo se x e y hanno lo stesso resto nella divisione per n.*

Dimostrazione. Infatti se x e y hanno lo stesso resto nella divisione per n, si ha: $x = qn+r$, $y = q'n + r$, dove $0 \leq r \leq n - 1$. Ma allora $x - y = (qn + r) - (q'n + r) = (q - q')n$ e perciò $x \equiv_n y$.

Viceversa se $x \equiv_n y$, si ha $x = y + kn$. Se r è il resto della divisione di y per n, vale la relazione $y = qn + r$ con $0 \leq r \leq n - 1$; perciò si ha $x = (qn + r) + kn = (q + k)n + r$, dunque r è anche il resto della divisione di x per n. □

Definizione 1.3.6 (**Classi d'equivalenza e insieme quoziente).** Sia X un insieme in cui è definita una relazione d'equivalenza $\sim$, sia $x \in X$. La **classe d'equivalenza** di x è il sottinsieme di X formato dagli elementi equivalenti a x:

$$[x] = \{y \in X \mid y \sim x\}.$$

Tale insieme si denota anche $[x]_\sim$.

L'insieme delle classi d'equivalenza è detto **insieme quoziente** di X rispetto alla relazione $\sim$ e si indica $X/\sim$.

L'insieme quoziente è un sottinsieme delle insieme delle parti di X, $\mathcal{P}(X)$. Osserviamo che $x \in [x]$ per la proprietà riflessiva. Quindi nessun elemento dell'insieme quoziente $X/\sim$ è l'insieme vuoto $\emptyset$. Inoltre le classi d'equivalenza ricoprono X, ossia X è l'unione delle classi d'equivalenza $[x]$, al variare di $x \in X$.

Definizione 1.3.7 (**Partizione).** Una **partizione** di un insieme X è un sottinsieme Π dell'insieme delle parti di X che gode delle proprietà:

1. nessun elemento di Π è vuoto;
2. l'unione degli insiemi di Π è uguale a X;
3. se $S, T \in \Pi$, e $S \neq T$ allora $S \cap T = \emptyset$.

Dunque due elementi di una partizione Pi o sono disgiunti o sono uguali.

Proposizione 1.3.8. *L'insieme quoziente $X/\sim$ di una relazione d'equivalenza in X è una partizione di X.*

Dimostrazione. Le prime due proprietà sono già state osservate. Per provare la terza, consideriamo due classi d'equivalenza $[x], [y]$ tali che $[x] \cap [y] \neq \emptyset$. Allora esiste $z \in [x] \cap [y]$, cioè $z \sim x$ e $z \sim y$. Per le proprietà simmetrica e transitiva segue che $x \sim y$. Proviamo che di conseguenza $[x] = [y]$. Infatti, se $u \in [x]$, allora $u \sim x$, ma $x \sim y$, dunque per la proprietà transitiva $u \sim y$ e segue che $u \in [y]$. Abbiamo così provato che $[x] \subset [y]$. L'inclusione opposta è analoga. □

Esempio 1.3.9.

1. L'insieme quoziente $\mathbb{Z}/\equiv_n$ si denota $\mathbb{Z}_n$. $\mathbb{Z}_n$ ha n elementi, uno per ciascuno degli n resti della divisione per n: $0, 1, 2, \ldots, n-1$. Infatti se x ha resto r nella divisione per n, $x = qn + r$ dunque $x \equiv_n r$. Gli elementi di $\mathbb{Z}_n$ si denotano anche $[r]_n$ o $\bar{r}$. Dunque $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Un insieme S si dice finito se esiste un numero naturale n tale che S è in biiezione con l'insieme $\{1, 2, 3, \ldots, n-1, n\}$. Dunque $\mathbb{Z}_n$ è un insieme finito con n elementi.

1.4 Operazioni in $\mathbb{Z}_n$

Sia $n \geq 2$. Nell'insieme $\mathbb{Z}_n$ si possono definire due operazioni, di somma e di prodotto, **indotte** dalle operazioni in $\mathbb{Z}$.

Siano $\bar{x}, \bar{y} \in \mathbb{Z}_n$. Definiamo

$$\bar{x} + \bar{y} = \overline{x + y},$$

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}.$$

Il prodotto si denota anche semplicemente $\bar{x}\bar{y}$. Queste operazioni di somma e prodotto sono **ben definite**, in quanto non dipendono dai particolari rappresentanti scelti per le due classi. Infatti, sia $\bar{x} = \bar{x}'$ e $\bar{y} = \bar{y}'$. Allora si ha $x' = x + kn, y' = y + hn$, per $k, h \in \mathbb{Z}$ opportuni. Quindi $(x + y) - (x' + y') = (x + y) - (x + kn + y + hn) = -(k + h)n$, da cui segue che $x + y \equiv_n x' + y'$.

Analogamente $xy - x'y' = xy - (x+kn)(y+hn) = -(xh+yk+khn)n$ e perciò $xy \equiv_n x'y'$.

Dalle proprietà della somma in $\mathbb{Z}$ seguono facilmente le proprietà della somma in $\mathbb{Z}_n$:

1. proprietà associativa: $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$;
2. la classe $\bar{0}$ è l'elemento neutro della somma;
3. $\overline{-x} = -\bar{x}$;
4. proprietà commutativa: $\bar{x} + \bar{y} = \bar{y} + \bar{x}$. Ne segue

Proposizione 1.4.1. *$(\mathbb{Z}_n, +)$ è un gruppo abeliano.*

Analogamente, dalle proprietà del prodotto in $\mathbb{Z}$ segue che valgono le seguenti proprietà del prodotto in $\mathbb{Z}_n$:

1. proprietà associativa: $(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z})$;
2. $\bar{1}$ è l'unità del prodotto;
3. proprietà commutativa: $\bar{x}\bar{y} = \bar{y}\bar{x}$;
4. proprietà distributiva: $(\bar{x} + \bar{y})\bar{z} = \bar{x}z + \bar{y}z$.

1.5 Campi

Definizione 1.5.1 (Campo). Sia K un insieme dotato di due operazioni, chiamate somma e prodotto e denotate $+$ e $\cdot$. La terna $(K, +, \cdot)$ si dice un **campo** se valgono le seguenti proprietà:

1. K è un gruppo abeliano rispetto alla somma;
2. proprietà associativa del prodotto;
3. esiste elemento unità;
4. ogni elemento **non nullo** di K ammette inverso;
5. proprietà commutativa del prodotto;
6. proprietà distributiva del prodotto rispetto alla somma: per ogni $a, b, c \in K$ si ha: $(a + b) \cdot c = ac + bc$.

Esempio 1.5.2.
1. Campi numerici: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,
2. $(\mathbb{Z}, +, \cdot)$ non è un campo perchè soltanto 1 e -1 hanno inverso.

Proposizione 1.5.3 (Proprietà generali dei campi)**.** *1. Per ogni $a \in K$ $0 \cdot a = 0$;*
2. Legge di annullamento del prodotto. Se $a \cdot b = 0$, allora $a = 0$ oppure $b = 0$;
3. Sia -1 l'opposto di 1 e $a \in K$. Allora $(-1) \cdot a = -a$.

Dimostrazione. 1. Usando la proprietà che 0 è elemento neutro per la somma e la proprietà distributiva si ottiene:

$$0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a.$$

Sommando $-(0 \cdot a)$ a ambo i membri, si ottiene $0 \cdot a = 0$.

2. Sia $a \cdot b = 0$. Se $a = 0$ abbiamo finito, sia dunque $a \neq 0$. Allora esiste a^{-1}. Moltiplicando ambo i membri a sinistra per a^{-1} otteniamo

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

ma $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$ per il punto precedente, dunque $b = 0$.

3. $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a =$ proprietà distributiva $= ((-1) + 1) \cdot a = 0 \cdot a = 0$. Analogamente $a + (-1) \cdot a = 0$. □

La legge di annullamento del prodotto garantisce che $K \setminus \{0\}$ è chiuso rispetto al prodotto. Si pu o anche esprimere dicendo che in K non vi sono divisori dello zero. Dunque le condizioni 2 – 5 della definizione di campo si possono riassumere dicendo che $(K \setminus \{0\}, \cdot)$ è un gruppo abeliano.

D'ora in poi lavorando in un campo K useremo spesso le notazioni compatte:
$a - b = a + (-b)$
$ab = a \cdot b$
$\frac{a}{b} = a/b = ab^{-1}$: quest'ultima notazione ha senso perchè il prodotto è commutativo.

Un insieme dotato di due operazioni, che sia un gruppo abeliano rispetto alla somma, ma verificante solo la proprietà associativa per il prodotto e la proprietà distributiva (ma non necessariamente la 3., la 4. e la 5.) è detto *anello*. Se il prodotto è commutativo, è detto *anello commutativo*; se in più esiste l'unità del prodotto, è detto anello commutativo con unità. Per esempio $\mathbb{Z}$ è un anello commutativo con unità.

Un insieme verificante tutti gli assiomi di campo, eccetto la proprietà commutativa del prodotto, è detto *corpo*. Un esempio importante è il corpo dei quaternioni.

Vogliamo ora determinare per quali n $\mathbb{Z}_n$ è un campo. A tale scopo consideriamo la tabella di moltiplicazione di $\mathbb{Z}_n \setminus \{0\}$ per $n = 2, 3, 4, 5$. Per semplicità di scrittura indicheremo gli elementi di $\mathbb{Z}_n$ omettendo il segno sopra.

$n = 2$

$\cdot$	1
1	1

$n = 3$

$\cdot$	1	2
1	1	2
2	2	1

$n = 4$

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$n = 5$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Dalle tabelle segue che $\mathbb{Z}_4$ non è un campo, perchè $\bar{2}$ non è invertibile, mentre $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ lo sono. In effetti, vale il seguente teorema.

Teorema 1.5.4. *Sia $n \geq 2$. Allora $\mathbb{Z}_n$ è un campo se e solo se n è un numero primo.*

Dimostrazione. Supponiamo dapprima che n non sia primo, e dimostriamo che $\mathbb{Z}_n$ non è un campo. Infatti, se n non è primo, esistono due interi a, b con $1 < a, b < n$ tali che $n = ab$. Passando alle classi di equivalenza nel quoziente $\mathbb{Z}_n$ si ottiene $\bar{n} = \bar{0} = \bar{a}\bar{b}$, che contraddice la Proposizione 1.5.3, punto 2, in quanto $\bar{a} \neq 0$ e $\bar{b} \neq 0$: $\bar{a}$ e $\bar{b}$ sono divisori dello zero.

Supponiamo ora che n sia primo e vogliamo dimostrare che $\mathbb{Z}_n$ è un campo.

Useremo le due seguenti proprietà.

1. Siano p un numero primo e $a, b \in \mathbb{Z}$. Se $p|ab$, allora o $p|a$ o $p|b$ (il segno | significa "divide"). Tale proprietà segue immediatamente dal Teorema fondamentale dell'aritmetica, ossia dall'esistenza e unicità della scomposizione in fattori primi.

2. *Principio della piccionaia.* Se X è un insieme **finito** e $f : X \to X$ è un'applicazione iniettiva, allora f è anche suriettiva, e quindi è una biiezione. Infatti, se f è iniettiva, f stabilisce una biiezione fra X e $f(X)$, dunque pure $f(X)$ è finito e ha lo stesso numero di elementi di X. Essendo $f(X) \subset X$ segue che $f(X) = X$.

Fissiamo dunque $\bar{a} \in \mathbb{Z}_n$, con n primo. Supponiamo $\bar{a} \neq 0$. Vogliamo dimostrare che $\bar{a}$ è invertibile. Consideriamo l'applicazione $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ definita da $\varphi(\bar{x}) = \bar{a}\bar{x}$: φ è la moltiplicazione per $\bar{a}$.

Osserviamo dapprima che φ è iniettiva. Infatti, se $\varphi(\bar{x}) = \varphi(\bar{y})$ ciò significa che $\bar{a}\bar{x} = \bar{a}\bar{y}$. Per definizione del prodotto in $\mathbb{Z}_n$, allora $\overline{ax} = \overline{ay}$, e quindi $ax \equiv ay \pmod{n}$. Perciò n divide $ax - ay = a(x - y)$. Dalla proprietà 1. segue che o $n|a$ o $n|x - y$. La prima è impossibile perchè $\bar{a} \neq 0$ per ipotesi, dunque $n|x - y$, ossia $\bar{x} = \bar{y}$; abbiamo così provato che φ è iniettiva.

Dunque per il Principio della piccionaia φ è anche suriettiva. Allora l'immagine di $\mathbb{Z}_n$ in φ, $\varphi(\mathbb{Z}_n)$ è tutto $\mathbb{Z}_n$. Quindi per ogni elemento $\bar{z}$ di $\mathbb{Z}_n$ esiste un $\bar{y} \in \mathbb{Z}_n$ tale che $\bar{z} = \varphi(\bar{y}) = \bar{a}\bar{y}$. In particolare se si prende $\bar{1} \in \mathbb{Z}_n$ esiste un $\bar{y}$ tale che $\bar{1} = \bar{a}\bar{y}$: questo $\bar{y}$ è l'inverso di $\bar{a}$ in $\bar{Z}_n$.

□

Dunque per ogni primo p, esiste il campo finito $\mathbb{Z}_p$ con p elementi.
Il principio della piccionaia è anche chiamato principio dei cassetti. Lo si può formulare dicendo che una piccionaia con n caselle può contenere al massimo n piccioni, se non se ne vogliono mettere due nella stessa casella. Oppure: se m piccioni sono distribuiti in n caselle con $m > n$, in qualche casella ci devono stare almeno due piccioni.

Esercizi 2.

1. Sia $n \in \mathbb{N}$ un naturale non primo. Sia $1 < x < n$. Dimostrare che $\bar{x} \in \mathbb{Z}_n$ è invertibile se e solo se x è primo con n, cioè il massimo comun divisore di x e n è uguale a 1. (Suggerimento: usare l'algoritmo euclideo della divisione, il massimo comun divisore di x e n può essere espresso nella forma $ax + bn$, con opportuni $x, n \in \mathbb{Z}$).

2. In $\mathbb{R}^2$ si definiscano le seguenti operazioni:

   somma : $(x, y) + (x', y') = (x + x', y + y')$;
   prodotto : $(x, y)(x', y') = (xx' - yy', xy' + yx')$.

   Verificare che $\mathbb{R}^2$ con tali operazioni è un campo.

   Questo è un modo per introdurre il campo dei numeri complessi $\mathbb{C}$.

Capitolo 2

Spazi vettoriali

D'ora in poi K denoterà un campo fissato. Per esempio K può essere $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, o $\mathbb{Z}_p$ con p un numero primo.

Definizione 2.0.1 (Operazione esterna). Un'operazione esterna con operatori in K su un insieme V è un'applicazione $K \times V \to V$. Data una coppia (λ, v) con $\lambda \in K, v \in V$, il corrispondente è indicato semplicemente λv.

In questo capitolo definiremo gli spazi vettoriali sul campo K, si tratta di insiemi dotati di due operazioni, una somma interna e un'operazione esterna con operatori in K, detta prodotto, verificanti certe proprietà. Un'operazione esterna su un insieme V con operatori in K è un'applicazione $K \times V \to V$.

Ma prima vediamo alcuni esempi, che si possono interpretare come "prototipi" di spazio vettoriale.

2.1 Primi esempi di spazio vettoriale

Esempio 2.1.1.

a) $K^n = \underbrace{K \times \cdots \times K}_{n}$, il prodotto cartesiano di n copie di K.

$K^n = \{x = (x_1, \ldots, x_n) \mid x_i \in K \ \forall i = 1, \ldots, n\}$. Per $n = 1$ si ritrova K. La somma interna e il prodotto esterno con operatori in K sono definiti membro a membro come segue.

$$\begin{aligned} + : K^n \times K^n &\to K^n \text{ tale che} \\ (x, y) &\to x + y = (x_1 + y_1, \ldots, x_n + y_n) \end{aligned}$$

$$\begin{aligned} \cdot : K \times K^n &\to K^n \text{ tale che} \\ (\lambda, x) &\to \lambda \cdot x = (\lambda x_1, \ldots, \lambda x_n) \end{aligned}$$

Gli elementi di K sono detti scalari. Osserviamo che lo stesso simbolo $+$ si usa per denotare sia la somma in K sia la somma in K^n.

b) Fissiamo due numeri naturali m, n: $M(m \times n, K)$ denota l'insieme delle **matrici a m righe e n colonne** con elementi (o entrate) in K. Per dare una tale matrice bisogna dare un elemento di K^{mn}, ossia una mn-upla di elementi di K; questi vanno scritti suddividendoli in m righe (orizzontali) e n colonne (verticali) e numerati con un doppio indice, il primo indica la riga e varia da 1 a m e il secondo la colonna e varia da 1 a n:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

$M(m \times n, K)$ è in biiezione con K^{mn}, cambia solo la scrittura. Anche la somma di matrici e il prodotto esterno con operatori in K (come quelle in K^{mn}) sono definiti membro a membro. Date due matrici A, B e uno scalare $\lambda \in K$, si pone

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + bm1 & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix},$$

$$\lambda A = \begin{pmatrix} \lambda a_{11} & \lambda a_{12} & \dots & \lambda a_{1n} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{m1} & \lambda a_{m2} & \dots & \lambda a_{mn} \end{pmatrix}.$$

Per indicare la matrice A come sopra, si usa anche la notazione compatta $A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$

c) Sia $\mathbb{C}$ il campo complesso; si definisce un'operazione "esterna" con operatori in $\mathbb{R}$ semplicemente restringendo il prodotto interno in $\mathbb{C}$:

$$\begin{aligned} \cdot : \mathbb{R} \times \mathbb{C} &\to \mathbb{C} \\ (\lambda, a + ib) &\to \lambda \cdot (a + ib) = \lambda a + i\lambda b \end{aligned}$$

d) Vettori geometrici del piano: vettori applicati e vettori liberi.

Un **vettore applicato** è un segmento orientato, ha punto iniziale e punto finale; può essere pensato come una coppia ordinata (A, B) di punti del piano, dove A è il punto iniziale, o di applicazione, e B il punto finale. Ha una lunghezza, se è stata fissata un'unità di misura, e se la lunghezza è $\neq 0$ ha anche direzione e verso.

Un **vettore libero, o vettore geometrico, o semplicemente vettore** è una classe d'equivalenza di vettori applicati per la relazione di equipollenza, secondo cui due vettori applicati sono equipollenti se hanno le stessa direzione, la stessa lunghezza e lo stesso verso, ossia stanno su rette parallele e muovendo la retta dell'uno parallelamente a se stessa è possibile sovrapporlo all'altro. Un vettore libero avente come rappresentante la coppia (A, B) si denota $\overrightarrow{AB}$ o $B - A$.

Ogni vettore ha uno e un solo rappresentante applicato in A, comunque si fissi il punto A. Questa osservazione permette di definire la **somma** di due vettori: se $v = \overrightarrow{AB}$ e $w = \overrightarrow{BC}$, si pone $v + w = \overrightarrow{AC}$. Se $v = \overrightarrow{AB}$ e $w = \overrightarrow{AB'}$, allora risulta $v + w = \overrightarrow{AD}$, dove D è il quarto vertice del parallelogramma di lati AB e AB'. La somma di vettori verifica la proprietà associativa e commutativa. Il vettore nullo è $\overrightarrow{AA}$. L'opposto di $\overrightarrow{AB}$ è $\overrightarrow{BA}$.

Si definisce il prodotto di un numero reale $\lambda \in \mathbb{R}$ per un vettore v, λv: ha la direzione di v, lunghezza pari a $|\lambda|$ per la lunghezza di v e verso concorde o discorde con v a seconda che $\lambda > 0$ o $\lambda < 0$.

L'insieme dei vettori liberi del piano con queste due operazoni è uno spazio vettoriale reale. In maniera analoga si possono definire i vettori dello spazio tridimensionale.

L'algebra lineare nasce da questo esempio e dallo studio dei sistemi lineari di equazioni, che si vedrà in seguito.

2.2 K-spazi vettoriali

Definizione 2.2.1 (K-spazio vettoriale)**.** Sia K un campo. Un insieme non vuoto V è uno spazio vettoriale su K, o K-spazio vettoriale, se in V sono date due operazioni:

- un'operazione interna detta somma,
- un'operazione esterna con operatori in K detta prodotto,

per cui valgono i seguenti assiomi:

(V1) V è un gruppo abeliano rispetto alla somma; lo zero è detto vettore nullo e indicato con 0_V o semplicemente 0; l'opposto di un elemento $v \in V$ è denotato $-v$;

(V2) le due operazioni sono legate dalle seguenti quattro proprietà:

1. $\forall\ \lambda, \mu \in K, v \in V$ si ha $(\lambda + \mu)v = \lambda v + \mu v$;
2. $\forall\ \lambda \in K, v, w \in V$ si ha $\lambda(v + w) = \lambda v + \lambda w$;
3. $\forall\ \lambda, \mu \in K, v \in V$ si ha $\lambda(\mu v) = (\lambda\mu)v$;
4. $\forall\ v \in V$ vale $1 \cdot v = v$, dove 1 è l'unità di K.

Gli elementi di V sono detti vettori, quelli di K scalari. I quattro esempi precedenti sono tutti spazi vettoriali. Nell'esempio a) il vettore nullo è $0 = (0, \ldots, 0)$, $-(x_1, \ldots, x_n) = (-x_1, \ldots, -x_n)$. L'esempio b) è simile: lo zero è la matrice nulla avente in tutte le posizioni lo 0 di K. Gli esempi c) e d) sono entrambi spazi vettoriali su $\mathbb{R}$.

Proposizione 2.2.2 (Proprietà degli spazi vettoriali)**.** *In ogni spazio vettoriale valgono le seguenti proprietà.*

(i) $0 \cdot v = 0\ \forall v \in V$;

(ii) $\lambda \cdot 0 = 0\ \forall \lambda \in K$;

(iii) *Se* $\lambda v = 0$*, allora o* $\lambda = 0$ *o* $v = 0$*;*

(iv) $(-1)v = -v$.

Dimostrazione. (i) $0 \cdot v = (0+0)v = 0v + 0v$, perciò $0v = 0$;

(ii) $\lambda \cdot 0 = \lambda(0+0) = \lambda \cdot 0 + \lambda \cdot 0$, perciò $\lambda \cdot 0 = 0$;

(iii) Sia $\lambda v = 0$; se $\lambda \neq 0$, esiste $\lambda^{-1} \in K$ tale che $\lambda\lambda^{-1} = \lambda^{-1}\lambda = 1$. Allora $v = 1 \cdot v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v) = \lambda^{-1} \cdot 0 = 0$ per il punto (i).

(iv) $v + (-1)v = 1 \cdot v + (-1)v = (1-1)v = 0 \cdot v = 0$.

□

Vediamo ora altri esempi importanti, iniziamo con quello dei polinomi.

Esempio 2.2.3. L'insieme dei polinomi a coefficienti in un campo K nella indeterminata t è l'insieme denotato con $K[t]$ delle espressioni del tipo $a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$, dove $a_0, \ldots, a_n$ sono elementi di K detti coefficienti del polinomio, e $n \geq 0$ è un numero intero. Dare un polinomio equivale a dare la successione dei coefficienti $a_0, \ldots, a_n$. Il grado di un polinomio è il massimo n tale che $a_n \neq 0$. Se tutti i coefficienti sono nulli si ha il polinomio nullo, il cui grado non è definito. Si noti che un polinomio non è una funzione. Osserviamo che $K[t]$ contiene K, come insieme dei polinomi di grado 0 più il polinomio nullo.

I polinomi si sommano e si moltiplicano per elementi di K in maniera naturale e costituiscono un K-spazio vettoriale.

Esempio 2.2.4. Siano K un campo e S un insieme arbitrario. Consideriamo l'insieme delle applicazioni di dominio S e codominio K:

$$\mathcal{F}(S, K) = \{f : S \to K\}.$$

In questo insieme introduciamo due operazioni definite punto per punto. Se $f, g \in \mathcal{F}(S, K)$ si definisce la loro somma $f + g$ come l'applicazione $S \to K$ che manda un elemento $s \in S$ in $(f+g)(s) := f(s) + g(s)$. Analogamente, si definisce il prodotto λf di uno scalare λ per f, ponendo $(\lambda f)(s) = \lambda f(s)$. Si hanno così in $\mathcal{F}(S, K)$ una somma interna e un prodotto esterno con operatori in K. Elemento neutro per la somma è l'applicazione nulla 0 tale che $0(s) = 0$ per ogni $s \in S$. Gli assiomi di spazio vettoriale si verificano facilmente sfruttando le proprietà di campo di K.

2.3 Sottospazi vettoriali

Sia V un K-spazio vettoriale. Sia $W \subset V$ un sottinsieme di V.

Definizione 2.3.1 (**Sottospazio vettoriale).** Si dice che W è un **sottospazio vettoriale** di V se

1. $W \neq \emptyset$;
2. se $w, w' \in W$ allora $w + w' \in W$: si dice che W è chiuso rispetto alla somma;

3. se $w \in W$ e $\lambda \in K$, allora $\lambda w \in W$: W è chiuso rispetto al prodotto esterno.

A volte si ometterà l'aggettivo vettoriale e si parlerà semplicemente di sottospazi di V. Attenzione però che in seguito introdurremo anche una seconda definizone, quella di sottospazio affine di uno spazio vettoriale.

Osservazione 1. Se W è un sottospazio vettoriale di V, allora il vettore nullo appartiene a W. Infatti: W non è vuoto, dunque prendiamo un vettore $w \in W$, ma allora $0 \cdot w = 0 \in W$. Analogamente anche $-w = (-1)w \in W$.

Osservazione 2. $W = \{0\}$, l'insieme costituito dal solo vettore nullo è un sottospazio, detto sottospazio nullo, in qualunque spazio vettoriale. Invece tutto lo spazio vettoriale V è sottospazio vettoriale di se stesso, detto sottospazio improprio.

Vediamo esempi di sottinsiemi dello spazio vettoriale $\mathbb{R}^2$ che sono sottospazi vettoriali e altri che non lo sono.

Esempio 2.3.2. Sia $V = \mathbb{R}^2$.

1. $W_1 = \{(x_1, x_2) \in \mathbb{R}^2 \mid 2x_1 + 3x_2 = 4\}$ non è sottospazio, ad esempio perchè non contiene il vettore nullo di $\mathbb{R}^2$, che è la coppia $(0, 0)$.

2. $W_2 = \{(x_1, x_2) \in \mathbb{R}^2 \mid 2x_1 + 3x_2 = 0\}$ è sottospazio: è una retta passante per l'origine. Analogamente risulta un sottospazio l'insieme delle soluzioni di una qualunque equazione del tipo $ax_1 + bx_2 = 0$, con $a, b \in \mathbb{R}$.

3. $W_3 = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 + x_2^2 \leq 1\}$ non è sottospazio, non è chiuso rispetto al prodotto esterno.

4. $W_4 = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 \geq 0, x_2 \geq 0\}$ non è sottospazio, non contiene gli opposti dei suoi elementi non nulli.

Vediamo ora un esempio nell'$\mathbb{R}$-spazio vettoriale $\mathbb{R}[t]$.

Esempio 2.3.3. Sia $\mathbb{R}[t]_d$ l'insieme dei polinomi di grado d, con $d \geq 1$ fissato: non è sottospazio vettoriale perchè non è chiuso rispetto alla somma. Per esempio, sia $d = 3$ e consideriamo $f(t) = 1 + 2t - t^2 + t^3$ e $g(t) = 5 + t - t^3$; $f(t) + g(t) = 6 + 3t + t^2$ ha grado 2. Invece $\mathbb{R}[t]_{\leq d}$, l'insieme dei poliomi di grado minore o uguale a d risulta sottospazio vettoriale.

Osserviamo che le operazioni di somma e di prodotto in V si possono restringere a un sottospazio W, perchè W è chiuso rispetto a somma e prodotto e contiene il vettore nullo. Rispetto a tali operazioni W risulta anch'esso essere un K-spazio vettoriale.

2.4 Intersezione di sottospazi vettoriali e sottospazio generato

Proposizione 2.4.1. *Ogni intersezione di sottospazi vettoriali di un K-spazio vettoriale V è un sottospazio vettoriale di V.*

Dimostrazione. Sia $\{W_i\}_{i\in I}$ una famiglia di sottospazi di V, indiciata su un insieme d'indici I. Sia W la loro intersezione: $W = \bigcap_{i\in I} W_i$. Chiaramente il vettore nullo 0 appartiene a W perchè appartiene a ogni sottospazio W_i. Siano $u, w \in W$: ciò significa che $u, w \in W_i$ per ogni $i \in I$; ma ogni W_i è sottospazio vettoriale di V dunque $u + w \in W_i$ per ogni $i \in I$. Quindi concludiamo che $u + w \in W$. Analogamente, se $u \in W$ e $\lambda \in K$, siccome $u \in W_i$ per ogni $i \in I$, si ha $\lambda u \in W_i$ per ogni i e quindi $\lambda u \in W$. □

Esempio 2.4.2. In $V = K[t]$ consideriamo la famiglia di sottospazi $W_i = K[t]_{\leq i}$, con I l'insieme degli interi ≥ 0. Si ha $\bigcap_{i\in I} W_i = K$. In questo caso i sottospazi considerati formano una catena $W_0 \subset W_1 \cdots \subset W_n \subset \cdots$ e perciò l'intersezione è il primo elemento della catena.

Osserviamo che un'unione di sottospazi vettoriali non è in generale un sottospazio. Per esempio se consideriamo due rette distinte passanti per l'origine in $\mathbb{R}^2$ come nell'esempio 2.3.2, la loro unione non è un sottospazio, in quanto non è chiusa rispetto alla somma.

Osserviamo che, se W è un sottospazio di V, $w_1, w_2 \in W$ e $\lambda, \mu \in K$, allora $\lambda w_1 + \mu w_2 \in W$. Infatti λw_1 e μw_2 appartengono a W per il punto 3. della definizione, e quindi anche $\lambda w_1 + \mu w_2 \in W$ per il punto 2. Un vettore della forma $\lambda w_1 + \mu w_2$ è detto *combinazione lineare* di w_1 e w_2. Vediamo ora che vale anche il viceversa.

Proposizione 2.4.3. *Sia $W \neq \emptyset$, $W \subset V$ un sottinsieme di uno spazio vettoriale V. Supponiamo che ogni combinazione lineare di due elementi di W appartenga ancora a W, allora W è un sottospazio vettoriale.*

Dimostrazione. Per ipotesi, per ogni scelta di vettori $w_1, w_2 \in W$ e scalari $\lambda, \mu \in K$ si ha $\lambda w_1 + \mu w_2 \in W$. Se si prende $\lambda = \mu = 1$ si ottiene che $w_1 + w_2 \in W$, quindi W è chiuso rispetto alla somma, mentre se si prende $\lambda = 0$ o $\mu = 0$ si ottiene la chiusura rispetto al prodotto esterno. □

Dato un qualunque sottinsieme S di uno spazio vettoriale V, si può considerare il più piccolo sottospazio contenente S, che è l'intersezione di tutti i sottospazi di V che contengono S. E` detto **sottospazio generato da** S e denotato $L(S)$ oppure $\langle S \rangle$. Per caratterizzare i suoi elementi avremo bisogno della nozione di combinazione lineare.

2.5 Combinazioni lineari

Definizione 2.5.1 (Combinazione lineare). Siano dati vettori $v_1, \ldots, v_n$ di uno spazio vettoriale V. Una loro **combinazione lineare** è un vettore della forma $\lambda_1 v_1 + \cdots + \lambda_n v_n$, con $\lambda_1, \ldots, \lambda_n$ elementi di K, detti coefficienti della combinazione lineare.

Esempio 2.5.2.

1. Se $\lambda_1 = \cdots = \lambda_n = 0$ si ottiene il vettore nullo $0 = 0v_1 + \cdots + 0v_n$: questa è detta **combinazione lineare banale**.
2. Se $\lambda_i = 1$ per un certo indice i e tutti gli altri coefficienti sono nulli, si ottiene il vettore v_i.
3. Se $\lambda_1 = \lambda_2 = 1$ e tutti gli altri coefficienti sono nulli, si ottiene $v_1 + v_2$.

4. Se $n = 1$, le combinazioni lineari dell'unico vettore v sono del tipo λv, al variare di λ in K: sono detti multipli di v o vettori proporzionali a v.

Proposizione 2.5.3. *Siano $v_1, \ldots, v_n \in V$. Il sottospazio generato da $S = \{v_1, \ldots, v_n\}$ è l'insieme di tutte le combinazioni lineari di $v_1, \ldots, v_n$. Lo si denota con il simbolo $\langle v_1, \ldots, v_n \rangle$ o $L(v_1, \ldots, v_n)$. E` anche detto chiusura lineare di S.*

Dimostrazione. Dimostriamo innanzitutto che l'insieme delle combinazioni lineari di $v_1, \ldots, v_n$ è un sottospazio vettoriale W di V. Certamente contiene il vettore nullo. La somma di due combinazioni lineari è una combinazione lineare: $(\lambda_1 v_1 + \cdots + \lambda_n v_n) + (\mu_1 v_1 + \cdots + \mu_n v_n) =$ usiamo la proprietà associativa e commutativa della somma e la 1. degli spazi vettoriali $= (\lambda_1 + \mu_1)v_1 + \cdots + (\lambda_n + \mu_n)v_n$, e dunque è anche questa una combinazione lineare di $v_1, \ldots . v_n$. Infine un multiplo di una combinazione lineare è una combinazione lineare: $\alpha(\lambda_1 v_1 + \cdots + \lambda_n v_n) = (\alpha\lambda_1)v_1 + \cdots + (\alpha\lambda_n)v_n$. Anche qui abbiamo usato gli assiomi di spazio vettoriale. Osserviamo poi che W contiene S, perchè ogni elemento v_i è combinazione lineare di $v_1, \ldots, v_n$. Infine, se U è un sottospazio che contiene $v_1, \ldots, v_n$, contiene anche ogni loro combinazione lineare, quindi contiene W. Perciò W è il più piccolo sottospazio che contiene $v_1, \ldots, v_n$. □

Esempio 2.5.4. Il sottospazio generato da un vettore v è $\langle v \rangle = \{\lambda v \mid \lambda \in K\}$, l'insieme dei multipli di v. Il sottospazio generato dal vettore nullo è il sottospazio nullo $\{0\}$.

Osservazione 3. Con dimostrazione simile alla precedente, si ottiene che, se S è un insieme infinito, il sottospazio $L(S)$ generato da S è l'insieme delle **combinazioni lineari finite** di elementi di S. In altre parole si considerano tutte le possibili combinazioni lineari di un numero finito di vettori appartenenti a S.

Il prossimo esempio è fondamentale.

Esempio 2.5.5. Sia $V = K^n$, il $K-$spazio vettoriale i cui elementi sono le n-uple ordinate di elementi di K. Introduciamo la notazione:

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1).$$

Calcoliamo una generica combinazione lineare di $e_1, \ldots, e_n$:

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = \lambda_1(1, 0, \ldots, 0) + \lambda_2(0, 1, 0 \ldots) + \cdots + \lambda_n(0, 0, \ldots, 0, 1) = (\lambda_1, \ldots, \lambda_n).$$

Di conseguenza $K^n = \langle e_1, \ldots, e_n \rangle$, perchè ogni vettore di K^n si può esprimere come una loro combinazione lineare. Si dice che $e_1, \ldots, e_n$ generano K^n o sono un sistema di generatori di K^n.

Esempio 2.5.6. Sia $V = K[t]$. Consideriamo l'insieme infinito

$$S = \{1, t, t^2, \ldots, t^n, \ldots\}.$$

Le combinazioni lineari finite di elementi di S sono tutti e soli i polinomi, quindi $K[t] = L(S)$. Le potenze di t sono un sistema di generatori di $K[t]$.

Esempio 2.5.7. Consideriamo in $\mathbb{R}^2$ i vettori $v_1 = (1, 4), v_2 = (2, -2)$. Una loro combinazione lineare è un vettore della forma

$$\lambda_1 v_1 + \lambda_2 v_2 = \lambda_1(1, 4) + \lambda_2(2, -2) = (\lambda_1 + 2\lambda_2, 4\lambda_1 - 2\lambda_2),$$

dove $\lambda_1, \lambda_2 \in \mathbb{R}$.

2.6 Dipendenza e indipendenza lineare

Definizione 2.6.1 (**Vettori linearmente indipendenti).** Siano $v_1, \ldots, v_n \in V$. Sono detti **linearmente indipendenti** se ogni loro combinazione lineare nulla è banale. In altre parole: da $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$ segue che $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$. Una combinazione lineare nulla deve avere tutti i coefficienti nulli.

Altrimenti i vettori $v_1, \ldots, v_n$ sono detti linearmente dipendenti: esistono $\lambda_1, \ldots, \lambda_n \in K$, **non tutti nulli** tali che $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$.

Osserviamo che un singolo vettore v è linearmente dipendente se esiste $\lambda \neq 0$ tale che $\lambda v = 0$. Per la Proposizione 2.2.2 (iii) questo si può verificare solo se $v = 0$.

Proposizione 2.6.2. *Siano $v_1, \ldots, v_n$ vettori di V: $v_1, \ldots, v_n$ sono linearmente dipendenti se e solo se almeno uno di essi è combinazione lineare dei rimanenti.*

Dimostrazione. Supponiamo che $v_1, \ldots, v_n$ siano linearmente dipendenti e che $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ sia una loro combinazione lineare nulla non banale. Allora esiste almeno un coefficiente $\lambda_i \neq 0$. Quindi esiste il suo inverso in K: λ_i^{-1}. Possiamo scrivere $\lambda_i v_i = -\lambda_1 v_1 - \cdots - \lambda_{i-1} v_{i-1} - \lambda_{i+1} v_{i+1} - \cdots - \lambda_n v_n$. Moltiplichiamo ora a sinistra per λ_i^{-1} e otteniamo: $\lambda_i^{-1}(\lambda_i v_i) = v_i = -\lambda_1 \lambda_i^{-1} v_1 - \cdots - \lambda_{i-1}\lambda_i^{-1} v_{i-1} - \lambda_{i+1}\lambda_i^{-1} v_{i+1} - \cdots - \lambda_n \lambda_i^{-1} v_n$.

Viceversa se $v_1 = \alpha_2 v_2 + \cdots + \alpha_n v_n$, possiamo scrivere $1 \cdot v_1 - \alpha_2 v_2 - \cdots - \alpha_n v_n = 0$: siccome il coefficiente di v_1 è uguale a 1, è diverso da 0, abbiamo così ottenuto una combinazione lineare nulla ma non banale di $v_1, \ldots, v_n$. Analogo ragionamento se al posto di v_1 abbiamo un qualunque altro vettore v_i. □

Corollario 2.6.3. *Due vettori v_1, v_2 sono linearmente dipendenti se e solo se uno è combinazione lineare, cioè multiplo, dell'altro. In tal caso i due vettori si dicono proporzionali.*

Esempio 2.6.4. Nello spazio vettoriale $\mathbb{Q}^3$ i vettori $v_1 = (1, 2, 3), v_2 = (2, 4, 5)$ sono linearmente indipendenti; mentre $w_1 = (0, 1, 0), w_2 = (0, -1, 0)$ sono linearmente dipendenti.

Osservazione 4.

1. Dato un vettore v, i vettori $\{v, 2v\}$, o $\{v, -v\}$, o $\{v, \lambda v\}$ qualunque sia λ, sono linearmente dipendenti.

2. Se sono dati vettori $v_1, \ldots, v_n$, con $v_i = 0$ per qualche indice i, allora $v_1, \ldots, v_n$ sono linearmente dipendenti. Infatti si ha la combinazione lineare nulla non banale $0v_1 + \cdots + 0v_{i-1} + 1v_i + 0v_{i+1} + \cdots + 0v_n = 0$.

3. Supponiamo che $v_1, \ldots, v_m$ siano linearmente dipendenti. Se aggiungo altri vettori qualunque $v_{m+1}, \ldots, v_n$, ottengo vettori $v_1, \ldots, v_n$ ancora linearmente dipendenti. Infatti basta aggiungere a una combinazione lineare nulla non banale di $v_1, \ldots, v_m$ la combinazione lineare di $v_{m+1}, \ldots, v_n$ con coefficienti tutti 0.

Esempio 2.6.5. Consideriamo in $\mathbb{R}^3$ i tre vettori $v_1 = (1, 2, 3)$, $v_2 = (1, -1, 0)$, $v_3 = (0, 1, 4)$. Sono linearmente dipendenti o indipendenti? Consideriamo una loro combinazione lineare nulla $x_1 v_1 + x_2 v_2 + x_3 v_3 = 0$ e analizziamo se può essere ottenuta con coefficienti non tutti nulli o meno.

$$x_1(1, 2, 3) + x_2(1, -1, 0) + x_3(0, 1, 4) = (x_1 + x_2, 2x_1 - x_2 + x_3, 3x_1 + 4x_3) = (0, 0, 0)$$

se e solo se (x_1, x_2, x_3)) è una soluzione del sistema di equazioni

$$\begin{cases} x_1 + x_2 & = 0 \\ 2x_1 - x_2 + x_3 & = 0 \\ 3x_1 \qquad + 4x_3 & = 0. \end{cases}$$

Si tratta di un sistema lineare omogeneo di 3 equazioni nelle 3 incognite x_1, x_2, x_3. In questo caso per risolverlo si può procedere esprimendo $x_2 = -x_1$ (dalla prima equazione), e $x_3 = -3/4x_1$ (dalla terza equazione), e poi sostituire nella seconda. Si ottiene $9/4x_1 = 0$ e quindi $x_1 = x_2 = x_3 = 0$. Si conclude che i tre vettori sono linearmente indipendenti.

Se sono dati 6 vettori in $\mathbb{R}^{13}$, per capire se sono linearmente indipendenti si scrive un sistema lineare omogeneo di 13 equazioni in 6 incognite. Un capitolo successivo sarà interamente dedicato alla teoria dei sistemi lineari di equazioni.

Proposizione 2.6.6. *Se $v_1, \ldots, v_n$ sono vettori linearmente indipendenti, ogni vettore $v \in L(v_1, \ldots, v_n)$ si esprime* **in maniera unica** *come loro combinazione lineare.*

Dimostrazione. La relazione $v = \lambda_1 v_1 + \ldots + \lambda_n v_n = \mu_1 v_1 + \ldots + \mu_n v_n$, si può riscrivere $\lambda_1 v_1 + \ldots + \lambda_n v_n - \mu_1 v_1 - \ldots - \mu_n v_n = 0$, o anche $(\lambda_1 - \mu_1)v_1 + \ldots + (\lambda_n - \mu_n)v_n = 0$: questa è una combinazione lineare nulla di $v_1, \ldots, v_n$, che sono linearmente indipendenti, perciò si ha $\lambda_1 - \mu_1 = \cdots = \lambda_n - \mu_n = 0$. □

L'affermazione della proposizione precedente si può anche rovesciare, ossia se ogni vettore di $L(v_1, \ldots, v_n)$ ha un'unica espressione come combinazione lineare di $v_1, \ldots, v_n$, questi sono linearmente indipendenti. Infatti se $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 = 0v_1 + \cdots + 0v_n$, per l'unicità si deve avere $\lambda_1 = \cdots = \lambda_n = 0$.

Concludiamo questo capitolo estendendo la definizione di lineare indipendenza a famiglie qualunque, non necessariamente finite, di vettori.

Definizione 2.6.7 (**Famiglia libera).** Una famiglia di vettori $\{v_i\}_{i \in I}$ è detta **libera** o **linearmente indipendente**, se lo è ogni sua sottofamiglia finita. Ciò significa che non esiste una combinazione lineare nulla non banale di alcuna sottofamiglia finita di vettori presi fra i v_i.

Per esempio, in $K[t]$ le potenze di t costituiscono una famiglia libera, per definizione di polinomio.

Esercizi 3.

1. Dimostrare l'affermazione che l'unione di due rette distinte per l'origine in $\mathbb{R}^2$ non è un sottospazio vettoriale, in quanto non è chiusa rispetto alla somma.

2. Dimostrare che, se W, W' sono sottospazi vettoriali di V e $W \cup W'$ è anch'esso sottospazio vettoriale, allora o $W \subset W'$ o $W' \subset W$.