UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Facoltà di Scienze Matematiche, Fisiche e Naturali

ALGEBRA I UNITÀ

M. Chiara Tamburini

Anno Accademico 2011/2012

Indice

Capitolo I

Relazioni e funzioni

1 Funzioni

Siano X e Y degli insiemi. Una *funzione* f con *dominio* X e *codominio* Y assegna, a ogni elemento $x \in X$, *uno e un solo* elemento $y \in Y$. Scriviamo $y = f(x)$ o anche $x \mapsto y$ e diciamo che y è *l'immagine di* x per f. L'elemento x si dice una *preimmagine* di y. Poniamo inoltre:

$$f(X) \ := \ \{f(x) \mid x \in X\} \ = \ \{y \in Y \mid \text{esiste } x \in X \text{ tale che } f(x) = y\}\,.$$

Una funzione con dominio X e codominio Y si indica mediante

$$f : X \to Y$$

o anche mediante

$$X \ \xrightarrow{f} \ Y.$$

(1.1) Definizione *Due funzioni* $X \xrightarrow{f} Y$ *e* $Z \xrightarrow{h} T$ *sono* uguali *solo quando* $X = Z$, $Y = T$ *e, per ogni* $x \in X$, $f(x) = h(x)$.

(1.2) Definizione *Una funzione* $f : X \to Y$ *si dice:*

1) iniettiva *se, per ogni* $x_1,\ x_2 \in X$*:*

$$f(x_1) = f(x_2) \implies x_1 = x_2 \ ;$$

2) suriettiva *se , per ogni* $y \in Y$*, esiste* $x \in X$ *tale che* $f(x) = y$*;*

3) bijettiva *se è iniettiva e suriettiva.*

Equivalentemente $f : X \to Y$ è iniettiva, se elementi distinti di X hanno immagini distinte in Y; è suriettiva, se $f(X) = Y$.

Se le funzioni f, g sono tali che il codominio di f coincide con il dominio di g, allora si può applicare prima f e poi g, ottenendo la *funzione prodotto* gf. Precisamente:

(1.3) Definizione *Date le funzioni*

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

si dice prodotto *di f e g la funzione*

$$X \xrightarrow{gf} Z$$

tale che, per ogni $x \in X$, $gf(x) := g(f(x))$.

È importante la seguente proprietà .

(1.4) Lemma *Il prodotto di funzioni è* associativo.

Dimostrazione. Date le funzioni $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$ si ha

$$X \xrightarrow{gf} Z \xrightarrow{h} T \qquad \text{e} \qquad X \xrightarrow{f} Y \xrightarrow{hg} T.$$

Ne segue:

$$X \xrightarrow{h(gf)} T \qquad \text{e} \qquad X \xrightarrow{(hg)f} T.$$

Quindi $h(gf)$ e $(hg)f$ hanno lo stesso dominio X e lo stesso codominio T.
Inoltre, per ogni $x \in X$, risulta:

$$h(gf)(x) \;=\; h(gf(x)) \;=\; h(g(f(x))) \;= hg(f(x)) \;=\; (hg)f(x).$$

Si conclude $h(gf) = (hg)f$. ■

(1.5) Lemma *Si considerino le funzioni $X \xrightarrow{f} Y \xrightarrow{g} Z$ e il loro prodotto*

$$X \xrightarrow{gf} Z.$$

1) *se f e g sono iniettive, il prodotto gf è una funzione iniettiva;*

2) *se f e g sono suriettive, il prodotto gf è una funzione suriettiva.*

In particolare, se f e g sono bijettive, gf è una funzione bijettiva.

Dimostrazione.
1) Siano $x_1, x_2 \in X$ tali che $gf(x_1) = gf(x_2)$, ossia $g(f(x_1)) = g(f(x_2))$. La iniettività di g implica allora $f(x_1) = f(x_2)$ e la iniettività di f implica $x_1 = x_2$.

2) Sia $z \in Z$. Poiché g è suriettiva, esiste $y \in Y$ tale che $g(y) = z$. Poiché f è suriettiva, esiste $x \in X$ tale che $g(x) = y$. Si conclude che $gf(x) = g(f(x)) = g(y) = z$. ■

(1.6) Definizione *Per ogni insieme X, la funzione* identica $I_X : X \to X$ *è definita ponendo $I_X(x) = x$, per ogni $x \in X$.*

(1.7) Lemma *Data $X \xrightarrow{f} Y$, consideriamo le funzioni:*

$$X \xrightarrow{I_X} X \xrightarrow{f} Y \xrightarrow{I_Y} Y.$$

Si ha $fI_X = f$, $I_Y f = f$, $I_Y f I_X = f$.

Dimostrazione. Le funzioni f e fI_X hanno entrambe dominio X e codominio Y. Inoltre, per ogni $x \in X$, si ha: $fI_X(x) = f(I_X(x)) = f(x)$. Pertanto $fI_X = f$. Analogamente, le funzioni f e $I_Y f$ hanno entrambe dominio X e codominio Y. Inoltre, per ogni $x \in X$, si ha $I_Y f(x) = I_Y(f(x)) = f(x)$. ■

(1.8) Definizione *Data $X \xrightarrow{f} Y$, supponiamo che esista $Y \xrightarrow{g} X$ tale che*

$$gf = I_X \qquad \text{e} \qquad fg = I_Y.$$

In tal caso diciamo che la funzione g è inversa *di f e scriviamo $g = f^{-1}$.*

Questa notazione è legittimata dal fatto che l'inversa di f, se esiste, è unica. Per la dimostrazione, basata sull'associatività del prodotto, si veda il Lemma 1.5 del Capitolo 2.

(1.9) Lemma *Una funzione $X \xrightarrow{f} Y$ ha inversa se e solo se è bijettiva.*

Dimostrazione.
Supponiamo che f sia bijettiva. Consideriamo la funzione $Y \xrightarrow{g} X$ che, ad ogni elemento y di Y, assegna la sua unica preimmagine x in X. Ossia:

$$g(y) = x \iff f(x) = y.$$

Ne segue che $fg = I_Y$ e $gf = I_X$, da cui $g = f^{-1}$. Infatti per ogni $y \in Y$ e per ogni $x \in X$:

$$fg(y) = f(g(y)) = f(x) = y \qquad \text{e} \qquad gf(x) = g(f(x) = g(y) = x.$$

Viceversa, supponiamo che f abbia inversa f^{-1}.

• f è iniettiva. Infatti, per ogni $x_1, x_2 \in X$: $\quad f(x_1) = f(x_2) \implies$

$$f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \implies \left(f^{-1}f\right)(x_1)) = \left(f^{-1}f\right)(x_2)) \implies I_X(x_1) = I_X(x_2) \implies x_1 = x_2.$$

• f è suriettiva. Infatti ogni $y \in Y$ ha preimmagine $x := f^{-1}(y) \in X$, dato che:

$$f(x) \;=\; f\left(f^{-1}(y)\right) \;=\; I_Y(y) \;=\; y.$$

■

2 Relazioni di equivalenza

Una *relazione* $\sim$ su un insieme X assegna a elementi di X elementi di X. Sia $x \in X$. Per ogni $y \in X$ scriviamo $x \sim y$ se la relazione $\sim$ assegna a x l'elemento y. Scriviamo invece $x \not\sim y$ in caso contrario.
Si noti che ogni funzione è , in particolare, una relazione.

(2.1) Definizione *Una relazione $\sim$ su X si dice di* equivalenza *se, per ogni $x, y, z \in X$:*

1) $x \sim x$ *(proprietà riflessiva);*

2) $x \sim y \implies y \sim x$ *(proprietà simmetrica);*

3) $(x \sim y \text{ e } y \sim z) \implies x \sim z$ *(proprietà transitiva).*

Se $x \sim y$ diciamo che y è *equivalente* a x nella $\sim$.

(2.2) Definizione *Per ogni $x \in X$, la* classe di equivalenza *di x rispetto alla relazione di equivalenza $\sim$ è il sottoinsieme di X costituito dagli elementi equivalenti a x nella $\sim$. Tale sottoinsieme si indica con $[x]$. In simboli:*

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

(2.3) Esempio *La funzione identica I_X è una relazione di equivalenza su X. Per ogni $x \in X$ la sua classe di equivalenza $[x]$ coincide con il singoletto $\{x\}$.*

(2.4) Lemma *Sia $\sim$ una relazione di equivalenza su X. Per ogni $x, y \in X$:*

1) $x \in [x]$;

2) $x \sim y \implies [x] = [y]$.

3) $x \not\sim y \implies [x] \cap [y] = \emptyset$.

Dimostrazione.

1) $x \sim x$ per la proprietà riflessiva. Quindi $x \in [x]$.

2) Sia $x \sim y$. Innanzitutto ne segue $[y] \subseteq [x]$. Infatti, per ogni $z \in [y]$:

$$(x \sim y \text{ e } y \sim z) \implies x \sim z \implies z \in [x].$$

Poichè $x \sim y$ implica $y \sim x$, si ha anche $[x] \subseteq [y]$. Si conclude che $[x] = [y]$.

3) Sia $x \not\sim y$ e supponiamo, per assurdo, che esista $z \in [x] \cap [y]$. Allora:

$$(x \sim z \text{ e } y \sim z) \implies (x \sim z \text{ e } z \sim y) \implies x \sim y.$$

Ma $x \sim y$ è in contrasto con l'ipotesi. ■

(2.5) Corollario *Le classi di equivalenza di una relazione di equivalenza $\sim$ su X costituiscono una* partizione *di X. Ossia ogni elemento $x \in X$ appartiene a* una e una sola *classe di equivalenza.*

Dimostrazione.

$x \in [x]$. Inoltre se $x \in [y]$, per qualche $y \in X$, si ha $x \sim y$ da cui $[x] = [y]$. ■

(2.6) Definizione *Sia $\sim$ una relazione di equivalenza su X.*

1) *L'insieme i cui elementi sono le classi di equivalenza di $\sim$ si dice l'*insieme quoziente *di X rispetto $\sim$ e si indica con $X/\sim$;*

2) *la funzione $\pi : X \to X/\sim$ tale che, per ogni $x \in X$:*

$$\pi(x) := [x]$$

si dice la proiezione canonica.

Essa è suriettiva. È iniettiva solo se $\sim$ coincide con la relazione identica I_X.

3 Relazioni d'ordine

(3.1) Definizione *Una relazione $\leq$ su X si dice d'* ordine *se, per ogni $x, y, z \in X$:*

1) $x \leq x$ *(proprietà riflessiva);*

2) $(x \leq y \text{ e } y \leq x) \implies x = y$ *(proprietà antisimmetrica);*

3) $(x \leq y \text{ e } y \leq z) \implies x \leq z$ *(proprietà transitiva).*

Se valgono i precedenti assiomi, diciamo che $(X, \leq)$ è un insieme *ordinato.*

(3.2) Definizione $(X, \leq)$ *si dice* totalmente ordinato *se, per ogni* $x, y \in X$*, si ha:*

$$x \leq y \quad \text{oppure} \quad y \leq x.$$

(3.3) Esempio *L'usuale relazione di* $\leq$ *sull'insieme* $\mathbb{R}$ *dei numeri reali è d'ordine. L'insieme* $(\mathbb{R}, \leq)$ *è totalmente ordinato.*

(3.4) Definizione *Siano* $(X, \leq)$ *un insieme ordinato e* $\emptyset \neq S \subseteq X$*.*

1) *un elemento* $x \in X$ *si dice* estremo superiore *o* minimo maggiorante *di* S *se:*

i) $s \leq x$ *per ogni* $s \in S$*;*

ii) se $c \in X$ *è tale che* $s \leq c$ *per ogni* $s \in S$*, allora* $x \leq c$*.*

1′) *un elemento* $y \in X$ *si dice* estremo inferiore *o* massimo minorante *di* S *se:*

i′) $y \leq s$ *per ogni* $s \in S$*;*

ii′) se $c \in X$ *è tale che* $c \leq s$ *per ogni* $s \in S$*, allora* $c \leq y$*.*

Può succedere che S non abbia estremo superiore o che non abbia estremo inferiore. Si ha tuttavia il seguente:

(3.5) Lemma *Siano* $(X, \leq)$ *un insieme ordinato e* S *un sottoinsieme non vuoto di* X*.*

1) *L'estremo superiore di* S *in* X*, se esiste, è unico e si indica con* $\sup_X(S)$*;*

2) *l'estremo inferiore di* S *in* X*, se esiste, è unico e si indica con* $\inf_X(S)$*.*

Dimostrazione.
1) Siano x, x' estremi superiori di S in X. Per ogni $s \in S$ si ha $s \leq x'$. Poiché x è minimo maggiorante di S, ne segue $x \leq x'$. Analogamente, per ogni $s \in S$ si ha $s \leq x$. Poiché x' è minimo maggiorante di S, ne segue $x' \leq x$. Per la proprietà simmetrica si conclude $x = x'$.
2) La dimostrazione è analoga. ■

(3.6) Definizione *Sia* S *un sottoinsieme non vuoto di un insieme ordinato* $(X, \leq)$*.*

1) *Se $x = \sup_X(S)$ appartiene a S, si dice che x è il* massimo *di S. Esso è caratterizzato dalle proprietà : $x \in S$ e, per ogni $s \in S$, si ha $s \leq x$.*

1′) *Se $y = \inf_X(S)$ appartiene a S, si dice che y è il* minimo *di S. Esso è caratterizzato dalle proprietà : $y \in S$ e, per ogni $s \in S$, si ha $y \leq s$.*

(3.7) Definizione *Un insieme ordinato $(X, \leq)$ si dice* bene ordinato *se ogni suo sottoinsieme non vuoto ha minimo.*

Ogni insieme bene ordinato è totalmente ordinato. Infatti ogni suo sottoinsieme $S = \{a, b\}$ ha minimo. Detto a, per esempio, il minimo di S si ha $a \leq b$.

(3.8) Esempio *L'insieme $\mathbb{N}$ dei numeri naturali, rispetto all'ordinamento indotto da $\mathbb{R}$, è bene ordinato.*

(3.9) Esempio *Per ogni insieme X, l'insieme $\mathcal{P}(X)$ i cui elementi sono i sottoinsiemi di X è parzialmente ordinato rispetto alla relazione di* inclusione $\subseteq$.

In $(\mathcal{P}(X), \subseteq)$ valgono i seguenti fatti:

1) $\emptyset$ è il minimo di $\mathcal{P}(X)$, X è il massimo di $\mathcal{P}(X)$;

2) per ogni $A, B \in \mathcal{P}(X)$:

- $\sup_{\mathcal{P}(X)}(\{A, B\}) = A \cup B$;
- $\inf_{\mathcal{P}(X)}(\{A, B\}) = A \cap B$;

3) se X ha almeno 2 elementi, $(\mathcal{P}(X), \subseteq)$ non è totalmente ordinato.

4 Equipotenza fra insiemi

(4.1) Definizione *Siano X, Y due insiemi. Si dice che X è equipotente a Y se esiste una applicazione bijettiva $f : X \to Y$. In tal caso si scrive*

$$|X| = |Y|$$

e si dice anche che X e Y hanno la stessa cardinalità .

(4.2) Teorema *Siano X, Y, Z insiemi. Allora:*

1) $|X| = |X|$;

2) $|X| = |Y| \ \Rightarrow \ |Y| = |X|$;

3) $(|X| = |Y| \quad \text{e} \quad |Y| = |Z|) \ \Rightarrow \ |X| = |Z|$.

Dimostrazione.

1) L'aplicazione identica $I_X : X \to X$ è bijettiva.

2) Sia $f : X \to Y$ una applicazione bijettiva. Per il Lemma 1.9 esiste l' inversa $f^{-1} : Y \to X$. Essa è bijettiva per lo stesso Lemma, avendo come inversa la f.

3) Siano $f : X \to Y$ e $g : Y \to Z$ delle applicazioni bijettive. Allora $gf : X \to Z$ è bijettiva per il Lemma 1.5. ■

5 Insiemi infiniti e insiemi finiti

(5.1) Definizione *Un insieme X è* infinito *se è equipotente a un suo sottoinsieme $Y \neq X$. In caso contrario è* finito.

(5.2) Esempio *L'insieme $\mathbb{Z}$ dei numeri interi è infinito.*

Infatti $\mathbb{Z}$ è equipotente al sottoinsieme $2\mathbb{Z}$ dei numeri pari. Per convincersi di ciò basta considerare l'applicazione $f : \mathbb{Z} \to 2\mathbb{Z}$ tale che $f(z) := 2z$ e notare che è bijettiva.

(5.3) Teorema *Ogni numero naturale $n := \{0, 1, \ldots, n-1\}$ è un insieme finito.*

La dimostrazione si ottiene per induzione. I numeri naturali sono, a meno di bijezioni, gli unici insiemi finiti. Infatti si può dimostrare che, per ogni insieme finito X, esiste un numero naturale n tale che X è equipotente a n.

(5.4) Definizione *Se X è equipotente al numero naturale n si dice che X ha* ordine n *(o* cardinalità *n) e si scrive $|X| = n$.*

(5.5) Esempio *$|\{1, 2, \ldots, n\}| = n$. Infatti l'applicazione*

$$\varphi : \{0, 1, \ldots, n-1\} \to \{1, 2, \ldots, n\}$$

tale che $f(i) := i + 1$ è bijettiva.

Si noti che, se X è un insieme di ordine n, detta $f : \{1, 2, \ldots, n\} \to X$ una applicazione bijettiva e posto

$$\begin{aligned} f(1) &= x_1 \\ f(2) &= x_2 \\ &\ldots \\ f(n) &= x_n \end{aligned}$$

si ha

$$X = \{x_1, \ldots, x_n\}\,.$$

(5.6) Esempio *Ciascuno dei seguenti insiemi ha ordine* 4*:*

$$4 = \{0, 1, 2, 3\}\,, \quad X := \{x_1, x_2, x_3, x_4\}, \quad A = \{a, b, c, d\}\,.$$

Capitolo II

Monoidi e gruppi

1 Generalità

I gruppi sono strutture algebriche che hanno un ruolo importante in matematica. Per introdurli, ricordiamo che una *operazione binaria* in un insieme S é una funzione

$$\cdot \ : \ S \times S \to S.$$

Per ogni $(s_1, s_2) \in S \times S$, l'immagine di (s_1, s_2) si indica con $s_1 \cdot s_2$ o anche semplicemente con $s_1 \cdot s_2$ e si dice il *prodotto* di s_1 e s_2.

(1.1) Definizione *Un* monoide $(S, \cdot, 1_S)$ *è una struttura algebrica in cui* S *è un insieme,* 1_S *è un elemento di* S *e* $\cdot$ *è una operazione binaria in* S *per cui valgono le proprietà :*

1) $1_S \cdot s = s \cdot 1_S = s$, *per ogni* $s \in S$*:*

2) $(s_1 \cdot s_2) \cdot s_3 = s_1 \cdot (s_2 \cdot s_3)$ *per ogni* $s_1, s_2, s_3 \in S$ (proprietà associativa).

1_S si dice l'*unità* (o l'*elemento neutro*) di S. L'unità è unica. Infatti, sia $u \in S$ tale che $u \cdot s = s \cdot u = s$, per ogni $s \in S$. In particolare, per $s = 1_S$, si ha $u = u \cdot 1_S = 1_S$.

(1.2) Definizione *Un monoide* $(S, \cdot, 1_S)$ *si dice* commutativo *se l' operazione* $\cdot$ *è commutativa, ossia se* $s_1 \cdot s_2 = s_2 \cdot s_1$ *per ogni* $s_1, s_2 \in S$.

(1.3) Esempio $(\mathbb{C}, \cdot, 1)$, *dove* $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ *è l'insieme dei numeri complessi e* $\cdot$ *l'usuale prodotto:*

$$(a + ib) \cdot (c + id) := (ac - bd) + i(ad + bc)$$

è un monoide commutativo.

Dato un insieme X, indichiamo con X^X l'insieme delle funzioni da X a X. Tenendo presente la Definizione 1.3 di prodotto di funzioni, nonchè i Lemmi 1.7 e 1.4 del Capitolo 1), si ha il seguente:

(1.4) Esempio *La struttura* $\left(X^X, \cdot, I_X\right)$*, dove* $\cdot$ *indica il prodotto di funzioni e* I_X *la funzione identica, è un monoide. Se* $|X| > 1$*, tale monoide è non commutativo.*

(1.5) Lemma *Siano* s, s_1, s_2 *elementi di un monoide* $(S, \cdot, 1_S)$ *tali che* $s \cdot s_2 = s_1 \cdot s = 1_S$*. Allora* $s_1 = s_2$*.*

Dimostrazione. $s_1 = s_1 \cdot 1_S = s_1 \cdot (s \cdot s_2) = (s_1 \cdot s) \cdot s_2 = 1_S \cdot s_2 = s_2$. ■

(1.6) Definizione *Un elemento* s *di un monoide* $(S, \cdot, 1_S)$ *ha* inverso *se esiste* $s_1 \in S$ *tale che:*

$$s \cdot s_1 = s_1 \cdot s = 1_S. \tag{1.7}$$

L'elemento s_1 (quando esiste !) è unico per il Lemma 1.5. Esso è detto l'inverso di s e si indica solitamente con s^{-1} anzichè con s_1.
Per la simmetria della (1.7), s è l'inverso di s^{-1}, ossia

$$\left(s^{-1}\right)^{-1} = s. \tag{1.8}$$

Inoltre, se $a, b \in S$ hanno inverso, allora:

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}. \tag{1.9}$$

Bisogna verificare che la (1.7) è soddisfatta ponendo $s = a \cdot b$, $s_1 = b^{-1} \cdot a^{-1}$. Infatti:

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

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

(1.10) Definizione *Un* gruppo $(G, \cdot, 1_G)$ *è un monoide in cui ogni elemento ha inverso.*

(1.11) Definizione *Un gruppo* $(G, \cdot, 1_G)$ *si dice* abeliano *se il prodotto è commutativo, ossia se, per ogni* $a, b \in G$*,* $a \cdot b = b \cdot a$*.*

Nel seguito, per brevità , un gruppo $(G, \cdot, 1_G)$ sarà indicato anche semplicemente con G e il prodotto $a \cdot b$ di due suoi elementi con ab.
Dal fatto che, per definizione, ogni elemento di un gruppo ha inverso, segue la proprietà espressa dal seguente Lemma, di cui si fa spesso uso.

(1.12) Lemma *(*Leggi di cancellazione*) Sia G un gruppo. Per ogni $a, b, c \in G$:*

$$\begin{aligned} ab = ac &\implies b = c \\ ba = ca &\implies b = c. \end{aligned} \tag{1.13}$$

In particolare:

$$\begin{aligned} ab = a &\implies b = 1_G \\ ba = a &\implies b = 1_G. \end{aligned} \tag{1.14}$$

Dimostrazione.
$ab = ac \implies a^{-1}(ab) = a^{-1}(ac) \implies (a^{-1}a)b = (a^{-1}a)c \implies 1_G b = 1_G c \implies b = c.$
In particolare, $ab = a \implies ab = a1_G \implies b = 1_G$.
Le altre implicazioni si dimostrano in modo analogo. ■

(1.15) Definizione *Siano G un gruppo e g un suo elemento. Per ogni $z \in \mathbb{Z}$ si definisce la* potenza *z-esima di g ponendo:*

$$g^0 := 1_G;$$

$$g^z := g^{z-1}g \qquad \text{se} \quad z > 0;$$

$$g^z := \left(g^{-1}\right)^{-z} \quad \text{se} \quad z < 0.$$

Pertanto:

$$g^1 = g,\ g^2 = gg,\ g^3 = ggg,\ \ldots\ ,\ g^{-2} = g^{-1}g^{-1},\ g^{-3} = g^{-1}g^{-1}g^{-1}, \ldots$$

Le parentesi si possono omettere in virtù della proprietà associativa.

(1.16) Teorema (Proprietà delle potenze) *Per ogni $a, b \in G$ e per ogni $z, t \in \mathbb{Z}$ si ha:*
1) $a^z a^t = a^{z+t}$;
2) $(a^z)^t = a^{zt}$;
3) *se $ab = ba$ allora $(ab)^z = a^z b^z$.*

La dimostrazione si ottiene per induzione (si veda, ad esempio, [5, Teorema 4.4.2, pagina 40]).

(1.17) Lemma *Siano $(S, \cdot, 1_S)$ un monoide e S^* l'insieme degli elementi di S che hanno inverso. Allora $(S^*, \cdot, 1_S)$ è un gruppo.*

Dimostrazione. $1_S \in S^*$ dato che $1_S^{-1} = 1_S$. Per ogni $a, b \in S^*$ si ha $a \cdot b \in S^*$, in virtù di (1.9). Quindi $\cdot$ è una operazione binaria in S^*. È associativa in S^*, essendolo in S. Per ogni $s \in S^*$, il suo inverso $s^{-1} \in S^*$ in virtù di (1.8). Pertanto $(S^*, \cdot, 1_S)$ è un gruppo. ∎

(1.18) Esempio *Sia $\mathbb{C}^*$ l'insieme degli elementi del monoide $(\mathbb{C}, \cdot, 1)$ che hanno inverso. Per il Lemma 1.17 si ha che $(C^*, \cdot, 1)$ è un gruppo.*

Si noti che $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Infatti per ogni $a + ib \neq 0 =$, si ha

$$(a + ib)^{-1} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}.$$

Rappresentando i numeri complessi in forma *esponenziale*, ossia ponendo

$$a + ib = \rho e^{i\theta} \qquad \text{dove} \qquad \rho := \sqrt{a^2 + b^2}, \quad \cos\theta := \frac{a}{\rho}, \quad \sin\theta := \frac{b}{\rho}$$

si ha

$$\mathbb{C}^* = \left\{ \rho e^{i\theta} \mid \rho, \theta \in \mathbb{R},\ 0 < \rho,\ 0 \leq \theta < 2\pi \right\}$$

con le identificazioni

$$\rho_1 e^{i\theta_1} = \rho_2 e^{i\theta_2} \iff \begin{cases} \rho_1 = \rho_2, \\ \theta_2 - \theta_1 = 2k\pi,\ k \in \mathbb{Z}. \end{cases}$$

Inoltre:

$$\rho e^{i\theta}\, \sigma e^{i\psi} = \rho\sigma\, e^{i(\theta+\psi)} \qquad \text{e} \qquad \left(\rho e^{i\theta}\right)^{-1} = \frac{1}{\rho}\, e^{-i\theta}.$$

2 Sottogruppi

(2.1) Definizione *Un* sottogruppo *H di un gruppo G è un sottoinsieme H di G per cui valgono i seguenti assiomi:*

1) *$1_G \in H$;*

2) *per ogni $h \in H$ anche l' inverso h^{-1} appartiene a H;*

3) *per ogni $h_1 \in H$, $h_2 \in H$ anche il prodotto $(h_1 h_2)$ appartiene a H.*

Se H è un sottogruppo di G scriviamo $H \leq G$. Chiaramente H è un gruppo rispetto alla stessa operazione definita in G, con unità $1_H = 1_G$.

(2.2) Esempi *Il sottoinsieme $\mathbb{R}^*$ dei numeri reali $\neq 0$ è un sottogruppo di $(\mathbb{C}^*, \cdot, 1)$. Il sottoinsieme $\mathbb{Q}^*$ dei numeri razionali $\neq 0$ è un sottogruppo di $(\mathbb{R}^*, \cdot, 1)$.*

È utile il seguente criterio.

(2.3) Lemma *Sia H un sottoinsieme non vuoto di un gruppo G tale che, per ogni $h_1 \in H$, $h_2 \in H$, si abbia $\left(h_1 h_2^{-1}\right) \in H$. Allora H è un sottogruppo di G.*

Dimostrazione.
1) Poichè H è non vuoto, esiste $h \in H$. Ne segue $hh^{-1} = 1_G \in H$.
2) Da $1_G \in H$ si ha che, per ogni $h \in H$, anche $1_G h^{-1} \in H$. Quindi $h^{-1} \in H$.
3) Per ogni $h_1, h_2 \in H$ si ha $h_2^{-1} \in H$ da cui $h_1 \left(h_2^{-1}\right)^{-1} \in H$. Quindi $(h_1 h_2) \in H$. ■

(2.4) Teorema *L'intersezione $A \cap B$ di due sottogruppi A, B di G è un sottogruppo.*

Dimostrazione.
Per A e B valgono gli assiomi $1), 2), 3)$ della definizione 2.1.
Dobbiamo dimostrare che valgono anche per $A \cap B$.
1) Da $1_G \in A$ e $1_G \in B$ segue $1_G \in A \cap B$.
2) Sia $x \in A \cap B$. Da $x \in A$ si ha $x^{-1} \in A$. Analogamente da $x \in B$ si ha $x^{-1} \in B$.
Si conclude $x^{-1} \in A \cap B$.
3) Siano $x \in A \cap B$, $y \in A \cap B$. Da $x, y \in A$ segue $(xy) \in A$. Analogamente da
$x, y \in B$ segue $(xy) \in B$. Si conclude $(xy) \in A \cap B$. ■

In modo analogo si dimostra che, più in generale, l'intersezione insiemistica di una famiglia non vuota di sottogruppi di G è un sottogruppo.
Fissato $g \in G$, indichiamo con $\langle g \rangle$ l'insieme delle sue potenze, ossia:

$$\langle g \rangle := \{g^z \mid z \in \mathbb{Z}\}. \tag{2.5}$$

(2.6) Lemma *Valgono i seguenti fatti:*
1) *$g \in \langle g \rangle$;*
2) *$\langle g \rangle$ è un sottogruppo di G;*
3) *se H è un sottogruppo di G tale che $g \in H$, allora $\langle g \rangle \leq H$.*

Dimostrazione.
1) $g = g^1 \in \langle g \rangle$.
2) Per ogni $g^h, g^k \in \langle g \rangle$, si ha $g^h \left(g^k\right)^{-1} = g^{h-k} \in \langle g \rangle$.
3) Dimostriamo per induzione che $g^n \in H$ per ogni $n \geq 0$. Ora $g^0 = 1_G \in H$. Per $n > 0$, si ha $g^n = g^{n-1} g$, con $g^{n-1} \in H$ per l'ipotesi induttiva. Pertanto $g^n \in H$ perchè

prodotto di due suoi elementi. Deduciamo ora che $g^k \in H$ per ogni $k < 0$. Infatti $-k > 0$. Quindi, per quanto dimostrato, $g^{-k} \in H$. Si conclude che $g^k = \left(g^{-k}\right)^{-1} \in H$. ■

Il precedente Lemma mostra che $\langle g \rangle$ è l'intersezione di tutti i sottogruppi di G a cui g appartiene, ossia è il *minimo* sottogruppo di G a cui g appartiene.
Ciò giustifica la seguente

(2.7) Definizione $\langle g \rangle$ *si dice il sottogruppo* ciclico *generato da* g.

(2.8) Definizione *Il* periodo $o(g)$ *di un elemento* $g \in G$ *è così definito:*
1) $o(g) := \infty$ *se* $g^k \neq 1_G$ *per ogni intero* $k \neq 0$*;*
2) $o(g) := n > 0$ $(n \in \mathbb{N})$ *se* $g^n = 1_G$ *e* $g^k \neq 1_G$ *per* $0 < k < n$.

Vedremo nel Corollario 7.12 che $o(g)$ coincide con l'ordine del sottogruppo $\langle g \rangle$.
Per questa ragione lo si chiama anche l' *ordine* di g.

(2.9) Esempio *In ogni gruppo* G *si ha* $o(1_G) = 1$.

(2.10) Esempio *Nel gruppo moltiplicativo* $\mathbb{C}^*$ *dei numeri complessi* $\neq 0$ *si ha:*

$$o(-1) = 2, \quad o(2) = \infty, \quad o(7) = \infty, \quad o\left(e^{\frac{2\pi i}{n}}\right) = n.$$

(2.11) Osservazione *Spesso anzichè* $o(g) = \infty$ *si scrive* $o(g) = 0$.

3 Il gruppo simmetrico

Fissato un insieme X, sia $\left(X^X, \cdot, I_X\right)$ il monoide dell funzioni $X \xrightarrow{f} X$ descritto nell'esempio 1.4. L'insieme $\left(X^X\right)^*$ degli elementi invertibili è costituito dalle funzioni bijettive per il Lemma 1.9 del Capitolo 1, e lo si indica con $\mathrm{Sym}(X)$. In virtù del Lemma 1.17 di questo capitolo si ha:

(3.1) Teorema *Per ogni insieme* X*, l'insieme* $\mathrm{Sym}(X)$ *delle funzioni bijettive da* X *a* X *è un gruppo rispetto al prodotto di funzioni. Esso è detto il* gruppo simmetrico *su* X.

Se X è infinito, $\mathrm{Sym}(X)$ è infinito e i suoi elementi si dicono *trasformazioni.*
Se X è finito e $|X| = n$, allora $\mathrm{Sym}(X)$ si indica anche con $\mathrm{Sym}(n)$, e lo si chiama il *gruppo simmetrico* di grado n. I suoi elementi si dicono *permutazioni.*

Ricordiamo che, per ogni numero naturale n, si definisce induttivamente il fattoriale di n mediante $0! := 1$ e, per ogni $n > 0$, $n! := n(n-1)!$. Cosí

$$1! = 1, \quad 2! = 2, \quad 3! = 6, \quad 4! = 24, \quad 5! = 120, \quad ecc\ldots$$

(3.2) Teorema $|\mathrm{Sym}(n)| = n!$.

Dimostrazione. Posto $X = \{1, \ldots, n\}$, ogni permutazione $\sigma \in \mathrm{Sym}(n)$ si può rappresentare nella forma:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Chiaramente $\sigma(1)$ è un qualunque elemento di X. Quindi $\sigma(1)$ si può scegliere in n modi. Affinchè σ sia iniettiva, deve essere $\sigma(2) \in X \setminus \{\sigma(1)\}$. Quindi $\sigma(2)$ si può scegliere in $n-1$ modi, ecc.. Infine, notando che una applicazione iniettiva di un insieme finito in sè è suriettiva, si conclude che $\mathrm{Sym}(n)$ ha $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ elementi. ■

Ovviamente questo Teorema ammette una dimostrazione per induzione su n, più rigorosa, ma meno intuitiva.

(3.3) Definizione *Una permutazione* $\gamma \in \mathrm{Sym}(n)$ *si dice un* ciclo di lunghezza r *se esiste* $i \in \{1, \ldots, n\}$ *tale che* $Y = \{i,\ \gamma(i),\ \gamma^2(i), \ldots,\ \gamma^{r-1}(i)\}$ *ha ordine* r *e* $\gamma(j) = j$ *per ogni* $j \notin Y$.

Ossia, posto $x_1 = i$, $x_2 = \gamma(i)$, ecc... si deve avere:

$$\gamma = \begin{pmatrix} x_1 & x_2 & \ldots & x_r & x_{r+1} & \ldots & x_n \\ x_2 & x_3 & \ldots & x_1 & x_{r+1} & \ldots & x_n \end{pmatrix} = (x_1, x_2, \ldots,\ x_r).$$

Per esempio, un ciclo di lunghezza 4 in Sym(8) è :

$$\gamma = \begin{pmatrix} 3 & 7 & 8 & 4 & 1 & 2 & 5 & 6 \\ 7 & 8 & 4 & 3 & 1 & 2 & 5 & 6 \end{pmatrix} = (3, 7, 8, 4).$$

Si noti che $(3,7,8,4) = (7,8,4,3) = (8,4,3,7) = (4,3,7,8)$.
Due permutazioni $\sigma, \tau \in \mathrm{Sym}(X)$ sono *disgiunte* se gli elementi di X spostati dall'una sono fissati dall'altra. Ossia se, per ogni $x \in X$:

$$\sigma(x) \neq x \implies \tau(x) = x.$$

In tal caso si verifica immediatamente che $\sigma\tau = \tau\sigma$. In altre parole due *permutazioni disgiunte commutano.* Evidentemente ogni permutazione *è prodotto di cicli disgiunti.*
Un ciclo di lunghezza r ha periodo r. Il prodotto di due cicli disgiunti di rispettive lunghezze r, s ha periodo il $\mathrm{mcm}\,(r, s)$.

(3.4) Esempio *Nel gruppo simmetrico* Sym(5) *si ha:* $o\,((4,5)) = 2$,

$$o\,((1,2)(4,5)) = 2, \quad o\,((4,5,1)) = 3, \quad o\,((1,2,3,4)) = 4, \quad o\,((1,2)(3,4,5)) = 6.$$

(3.5) Definizione *Uno* scambio *è un ciclo di lunghezza* 2.

Ogni ciclo di lunghezza r è prodotto di $r-1$ scambi. Infatti:

$$(x_1, x_2, \dots, x_r) = (x_1, x_r)\,(x_1, x_{r-1}) \dots (x_1, x_3)\,(x_1, x_2)\,.$$

Per esempio $(1,2,3,4) = (1,4)(1,3)(1,2)$. Ne segue che ogni permutazione σ è *prodotto di scambi* (in generale non disgiunti). Si può dimostrare che il loro numero è sempre pari o sempre dispari. Ha quindi senso la seguente

(3.6) Definizione *Una permutazione σ si dice* pari *se è prodotto di un numero pari di scambi. In caso contrario si dice* dispari.

(3.7) Esempio *La permutazione* $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} = (1,2,3)\,(5,6) = (1,3)\,(1,2)\,(5,6)$ *è dispari.*

(3.8) Esempio *La permutazione* $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 1 & 6 & 4 & 9 & 7 & 5 \end{pmatrix} =$
$(1,3,2,8,7,9,5,6,4) = (1,4)\,(1,6)\,(1,5)\,(1,9)\,(1,7)\,(1,8)\,(1,2)\,(1,3)$ *è pari.*

(3.9) Esempio *La permutazione* $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 9 & 7 & 8 & 5 & 4 & 6 & 3 \end{pmatrix} =$
$(1,2)\,(3,9)\,(4,7)\,(5,8,6) = (1,2)\,(3,9)\,(4,7)\,(5,6)\,(5,8)$ *è dispari.*

4 Il Teorema di Lagrange

(4.1) Definizione *Sia H un sottogruppo di G. Per ogni $a, b \in G$ poniamo:*

$$a \equiv b \pmod{H} \iff ab^{-1} \in H.$$

(4.2) Teorema *La relazione di congruenza modulo un sottogruppo H è di equivalenza in G. Per ogni $g \in G$, la classe di equivalenza di g è l'insieme*

$$Hg := \{hg \mid h \in H\}\,.$$

Dimostrazione. Siano $a, b, c \in G$.
1) $a \equiv a \pmod{H}$ poichè $aa^{-1} = 1_H \in H$.
2) $a \equiv b \pmod{H} \implies b \equiv a \pmod{H}$.
Da $ab^{-1} \in H$ segue $\left(ab^{-1}\right)^{-1} \in H$, ossia $ba^{-1} \in H$.

3) ($a \equiv b \pmod H$ e $b \equiv c \pmod H$) $\implies a \equiv c \pmod H$.
Infatti da $ab^{-1} \in H$ e $bc^{-1} \in H$ segue $\left(ab^{-1}\right)\left(bc^{-1}\right) = ac^{-1} \in H$.
Pertanto la congruenza modulo H è una relazione di equivalenza in G.
Fissato $g \in G$, per ogni $x \in G$ si ha

$$x \equiv g \pmod H \iff xg^{-1} = h \iff x = hg$$

per qualche $h \in H$. Si conclude che la classe di equivalenza di g è Hg. ■

(4.3) Definizione *Hg si dice il* laterale destro *di H individuato da g.*

Tenendo presente il punto 2 del Lemma 2.4 del Capitolo 1, per ogni $a, b \in G$ si ha:

$$Ha = Hb \iff a \equiv b \pmod H \iff ab^{-1} \in H. \tag{4.4}$$

(4.5) Esempio *Sia $H = \langle(1,2)\rangle$ il sottogruppo di* Sym(3) *generato da* $(1,2)$.
Indicando con id la permutazione identica, i suoi laterali destri sono i 3 *sottoinsiemi:*

$$\begin{array}{lcl} H & = & \{id,\ (1,2)\} \\ H(1,3) & = & \{(1,3),\ (1,3,2)\} \\ H(2,3) & = & \{(2,3),\ (1,2,3)\}\,. \end{array}$$

Si noti che

$$\begin{array}{lcl} H = Hid & = & H(1,2) \\ H(1,3) & = & H(1,3,2)\ . \\ H(2,3) & = & H(1,2,3) \end{array}$$

(4.6) Esempio *Sia G il sottogruppo di $\mathbb{C}^*$ generato da $\epsilon := e^{\frac{2\pi i}{8}}$, ossia:*

$$G = \left\{1,\ \epsilon,\ \epsilon^2,\ \epsilon^3,\ \epsilon^4,\ \epsilon^5,\ \epsilon^6,\ \epsilon^7\right\}.$$

Detto H il sottogruppo di G generato da ϵ^2, i laterali destri di H in G sono i 2 *sottoinsiemi:*

$$\begin{array}{lcccccccc} H & = & \left\{\epsilon^0,\ \epsilon^2,\ \epsilon^4,\ \epsilon^6\right\} & = & H\epsilon^2 & = & H\epsilon^4 & = & H\epsilon^6 \\ H\epsilon & = & \left\{\epsilon,\ \epsilon^3,\ \epsilon^5,\ \epsilon^7\right\} & = & H\epsilon^3 & = & H\epsilon^5 & = & H\epsilon^7. \end{array}$$

(4.7) Teorema (di Lagrange) *L'ordine di un sottogruppo H di un gruppo finito G è un divisore dell'ordine di G.*

Dimostrazione. Sia $H = \{h_1, \ldots, h_m\}$. Per ogni $g \in G$, si ha:

$$Hg = \{h_1 g,\ \ldots,\ h_m g\}\,.$$

L' applicazione da H a Hg tale che $h \mapsto hg$ è evidentemente suriettiva. Ma è anche iniettiva dato che, per le leggi di cancellazione, $h_i g = h_j g$ implica $h_i = h_j$. Pertanto $|Hg| = |H| = m$ per ogni $g \in G$. Detti $Hg_1, \ldots, Hg_k$ i laterali destri distinti di H, ogni elemento di G appartiene a uno e uno solo di essi, per il Lemma 2.5. Si conclude:

$$|G| = |Hg_1| + \cdots + |Hg_k| = |H| + \cdots + |H| = |H|k.$$

■

(4.8) Definizione *Il numero* $k = \frac{|G|}{|H|}$ *si dice l'*indice *di* H *in* G.

5 Sottogruppi normali e gruppi quoziente

(5.1) Definizione *Un sottogruppo* N *di* G *si dice* normale *se, per ogni* $g \in G$ *e per ogni* $n \in N$ *si ha* $gng^{-1} \in N$.

(5.2) Esempio *In ogni gruppo* G*, i sottogruppi banali* $\{1_G\}$ *e* G *sono normali.*

(5.3) Esempio *Ogni sottogruppo di un gruppo abeliano è normale.*

(5.4) Esempio *Nel gruppo simmetrico* $\mathrm{Sym}(n)$ *le permutazioni pari costituiscono un sottogruppo normale, detto il gruppo* alterno *di grado* n *e indicato con* $\mathrm{Alt}(n)$.

D'altra parte, il sottogruppo $H = \langle (1,2) \rangle$ di $\mathrm{Sym}(3)$ non è normale perchè , ad esempio $(1,3)(1,2)(1,3)^{-1} = (2,3) \notin H$.

(5.5) Lemma *Sia* N *un sottogruppo normale di* G*. Per ogni* $a, a', b, b' \in G$*:*

$$\begin{cases} a \equiv a' \pmod N \\ b \equiv b' \pmod N \end{cases} \implies (ab) \equiv (a'b') \pmod N. \tag{5.6}$$

Dimostrazione. Sia $aa'^{-1} = n_1 \in N$, $bb'^{-1} = n_2 \in N$. Ne segue:

$$ab\left(a'b'\right)^{-1} = \left(n_1 a'\right)\left(n_2 b'\right)\left(b'^{-1}a'^{-1}\right) = n_1\left(a' n_2 a'^{-1}\right).$$

L'ipotesi che N sia normale implica $\left(a' n_2 a'^{-1}\right) \in N$, da cui $n_1\left(a' n_2 a'^{-1}\right) \in N$.

■

Il precedente Lemma consente di definire un prodotto di laterali, dando luogo a un nuovo gruppo i cui elementi sono i laterali. Si ha infatti:

(5.7) Teorema *Sia N un sottogruppo normale di G. L'insieme $\frac{G}{N}$ dei laterali di N in G è un gruppo rispetto al prodotto definito ponendo, per ogni $a, b \in G$:*

$$(Na)\,(Nb) := N(ab). \tag{5.8}$$

$\frac{G}{N}$ si dice il gruppo quoziente *di G rispetto a N.*

Dimostrazione. Il prodotto di laterali è ben definito in quanto le relazioni (3.3) sono equivalenti a:

$$\begin{cases} Na = Na' \\ Nb = Nb' \end{cases} \quad \Longrightarrow \quad N(ab) = N(a'b').$$

Tale prodotto è associativo, infatti, per ogni $a, b, c \in G$:

$$Na(NbNc) = NaN(bc) = Na(bc) = N(ab)c = N(ab)Nc = (NaNb)Nc.$$

Il laterale $N = N1_G$ è elemento neutro poichè , per ogni $g \in G$:

$$N1_G\,Ng \;=\; N(1_G\,g) \;=\; Ng, \quad Ng\,N1_G \;=\; N(g\,1_G) \;=\; Ng.$$

Infine ogni laterale Ng ha inverso Ng^{-1}. Infatti:

$$Ng\,Ng^{-1} \;=\; Ng\,g^{-1} \;=\; N1_G, \quad Ng^{-1}\,Ng \;=\; Ng^{-1}\,g \;=\; N1_G.$$

■

6 La notazione additiva per i gruppi abeliani

Spesso, per un gruppo abeliano G, è opportuna la notazione *additiva*. In tal caso, l'operazione si chiama *somma* e si indica con il simbolo $+$. L'elemento neutro si chiama *zero* e si indica con 0_G. Per ogni $g \in G$, l' elemento che sommato con g dà 0_G, si chiama l' *opposto* di g e si indica con $-g$. In luogo di $g_1 + (-g_2)$ si scrive $g_1 - g_2$.
Per ogni $g \in G$ e $z \in \mathbb{Z}$, la Definizione 1.15 diventa:

$$0\,g := 0_G;$$

$$z\,g := (z-1)g + g \quad \text{se} \quad z > 0;$$

$$z\,g := (-n)(-g) \qquad \text{se} \quad z < 0.$$

Pertanto:

$1\,g = g,\ \ 2\,g = g + g,\ \ 3\,g = g + g + g,\ \ \ldots\ ,\ \ -2\,g = -g - g,\ \ -3\,g = -g - g - g, \ldots.$
L'elemento zg si dice il *multiplo* z-esimo di g.

Il Teorema 1.16 si enuncia così . Per ogni $a, b \in G$ e per ogni $z, t \in \mathbb{Z}$ si ha:
1) $za + ta = (z + t)a$;
2) $z\,(ta) = (zt)a$;
3) $z\,(a + b) = za + zb$.
Le leggi di cancellazione (1.13) ed (1.14) diventano: per ogni $a, b, c \in G$:

$$a + b = a + c \implies b = c, \quad a + b = a \implies b = 0_G. \tag{6.1}$$

Se H è un sottogruppo di G, il laterale individuato da $g \in G$ si indica con $H + g$. Chiaramente:

$$H + g := \{h + g \ \mid \ h \in H\}\,.$$

Per ogni $a, b \in G$ le relazioni (4.4) diventano:

$$H + a = H + b \iff a \equiv b \pmod{H} \iff (a - b) \in H. \tag{6.2}$$

Infine, in virtù di (5.8), l'insieme $\frac{G}{H}$ dei laterali di H in G è un gruppo rispetto:

$$(H + a) + (H + b) := H + (a + b).$$

(6.3) Esempio *L'insieme* $\mathbb{C}$ *dei numeri complessi, rispetto alla somma usuale:*

$$(a + ib) + (c + id) := (a + c) + i(b + d)$$

è un gruppo abeliano. Lo indichiamo con $(\mathbb{C}, +, 0)$.

Esempi importanti di sottogruppi del gruppo additivo dei numeri complessi sono:
• il sottogruppo $(\mathbb{R}, +, 0)$ dei numeri reali;
• il sottogruppo $(\mathbb{Q}, +, 0)$ dei numeri razionali;
• il sottogruppo $(\mathbb{Z}, +, 0)$ dei numeri interi.
Tali gruppi sono tutti infiniti. D'altra parte, il seguente Lemma fornisce un esempio di gruppo abeliano di ordine n, per ogni $n \geq 1$.

(6.4) Lemma *Sia* $n\mathbb{Z}$ *il sottogruppo di* $(\mathbb{Z}, +, 0)$ *generato da* n.
Il gruppo quoziente $\frac{\mathbb{Z}}{n\mathbb{Z}}$ *è abeliano di ordine* n.

Dimostrazione.

La dimostrazione si basa sul Teorema 2.4 del Capitolo 3.
Sia $n\mathbb{Z}+a$ un laterale di $n\mathbb{Z}$ in $\mathbb{Z}$. Dividendo a per n si ottengono due interi q, r tali che $a = nq + r$, con $0 \leq r \leq (n-1)$. Da $a - r = nq$ segue $a \equiv r \pmod{n\mathbb{Z}}$, ossia $n\mathbb{Z} + a = n\mathbb{Z} + r$.
Sia ora $s \in \mathbb{Z}$, con $0 \leq s \leq n-1$, tale che $n\mathbb{Z} + r = n\mathbb{Z} + s$. Ne segue $r - s = nk$, per un opportuno intero k. Da $r = nk + s = n0 + r$, si deduce $k = 0$, $s = r$ per l'unicità del quoziente e del resto della divisione di r per n.
Quindi, gli elementi distinti di $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sono gli n laterali:

$$n\mathbb{Z} + r, \quad 0 \leq r \leq n-1.$$

La somma, data dalla definizione (5.8), risulta essere:

$$(n\mathbb{Z} + a) + (n\mathbb{Z} + b) := n\mathbb{Z} + (a + b). \tag{6.5}$$

■

Notazioni

• $a \equiv b \pmod{n\mathbb{Z}}$ si abbrevia in $a \equiv b \pmod{n}$.

• Il laterale $n\mathbb{Z}+a$ si indica anche con $[a]_n$ e si dice la *classe di resti modulo n* individuata da a;

• Il gruppo quoziente $\frac{\mathbb{Z}}{n\mathbb{Z}}$ si chiama il *gruppo delle classi di resti modulo n*, si indica con $\mathbb{Z}_n$.

La somma data in (6.5) risulta quindi :

$$[a]_n + [b]_n := [a + b]_n.$$

(6.6) Esempio *La tavola della somma di* $\frac{\mathbb{Z}}{2\mathbb{Z}} = \mathbb{Z}_2$ *è :*

$+$	$2\mathbb{Z}+0$	$2\mathbb{Z}+1$
$2\mathbb{Z}+0$	$2\mathbb{Z}+0$	$2\mathbb{Z}+1$
$2\mathbb{Z}+1$	$2\mathbb{Z}+1$	$2\mathbb{Z}+0$

ossia

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

(6.7) Esempio *La tavola della somma di* $\frac{\mathbb{Z}}{3\mathbb{Z}} = \mathbb{Z}_3$ *è :*

$+$	$3\mathbb{Z}+0$	$3\mathbb{Z}+1$	$3\mathbb{Z}+2$
$3\mathbb{Z}+0$	$3\mathbb{Z}+0$	$3\mathbb{Z}+1$	$3\mathbb{Z}+2$
$3\mathbb{Z}+1$	$3\mathbb{Z}+1$	$3\mathbb{Z}+2$	$3\mathbb{Z}+0$
$3\mathbb{Z}+2$	$3\mathbb{Z}+2$	$3\mathbb{Z}+0$	$3\mathbb{Z}+1$

ossia

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

7 Omomorfismi

(7.1) Definizione *Siano* $(G, \cdot, 1_G)$ *e* $(H, *, 1_H)$ *due gruppi. Un* omomorfismo *da* G *a* H *è una applicazione* $f : G \to H$ *tale che, per ogni* $a, b \in G$*:*

$$f(a \cdot b) = f(a) * f(b). \tag{7.2}$$

Inoltre un omomorfismo $f : G \to H$ si dice:

- un *monomorfismo* se è una applicazione iniettiva;
- un *epimorfismo* se è una applicazione suriettiva;
- un *isomorfismo* se è una applicazione bijettiva.

Un *automorfismo* di G è un isomorfismo $f : G \to G$.

(7.3) Definizione *Siano* A *e* B *due gruppi.*

1) B *è* immagine epimorfa *di* A *se esiste un epimorfismo* $f : A \to B$*.*

2) B *è* isomorfo *ad* A *se esiste un isomorfismo* $f : A \to B$*. In tal caso scriviamo*

$$B \cong A.$$

(7.4) Esercizio *Siano* $\alpha : A \to B$*,* $\beta : B \to C$ *isomorfismi di gruppi. Si dimostri che* $\beta\alpha : A \to C$ *e* $\alpha^{-1} : B \to A$ *sono isomorfismi.*

Ne segue che, se A, B, C sono gruppi qualunque, si ha:

1) $A \cong A$;
2) $A \cong B \implies B \cong A$;
3) $(A \cong B \text{ e } B \cong C) \implies A \cong C$.

Queste proprietà giustificano il fatto che, in algebra, gruppi isomorfi sono identificati.

(7.5) Esempio *Siano* $(\mathbb{R}, +, 0)$ *il gruppo additivo dei numeri reali e* $(\mathbb{R}^+, \cdot, 1)$ *il gruppo moltiplicativo dei numeri reali positivi. L'applicazione* $f : \mathbb{R} \to \mathbb{R}^+$ *tale che*

$$f(x) := e^x$$

è un isomorfismo. Pertanto $(\mathbb{R}, +, 0) \cong (\mathbb{R}^+, \cdot, 1)$.

(7.6) Lemma *Sia* $f : G \to H$ *un omomorfismo di gruppi.*

1) $f(1_G) = 1_H$*;*

2) *per ogni* $g \in G$*:* $f\left(g^{-1}\right) = f(g)^{-1}$*;*

3) Ker $f := \{g \in G \mid f(g) = 1_H\}$ *è un sottogruppo normale di* G*;*

4) $f(G) := \{f(g) \mid g \in G\}$ *è un sottogruppo di* H*;*

5) *per ogni* $a, b \in G$*:* $f(a) = f(b) \iff ab^{-1} \in \text{Ker } f$.

In particolare f *è un monomorfismo se e solo se* Ker $f = \{1_G\}$.

Dimostrazione.

1) Da $1_G = 1_G 1_G$ segue $f(1_G) = f(1_G)f(1_G)$. Quindi $f(1_G) = 1_H$ per le (1.14).

2) $f(g^{-1})f(g) = f(g^{-1}g) = f(1_G) = 1_H$. Pertanto $f\left(g^{-1}\right) = f(g)^{-1}$.

3) $1_G \in \text{Ker } f$ per il punto 1). Per ogni $x, y \in \text{Ker } f$ si ha:

$$f(xy^{-1}) = f(x)f(y^{-1}) = 1_H f(y)^{-1} = 1_H 1_H^{-1} = 1_H.$$

Quindi $xy^{-1} \in \text{Ker } f$, che è pertanto un sottogruppo.

Per ogni $g \in G$ e ogni $x \in \text{Ker } f$ risulta:

$$f\left(gxg^{-1}\right) = f(g)\, f(x)\, f\left(g^{-1}\right) = f(g)\, 1_H f(g)^{-1} = 1_H.$$

Quindi $gxg^{-1} \in \text{Ker } f$ che è pertanto un sottogruppo normale di G.

4) $1_H \in f(G)$ per il punto 1). Per ogni $h_1, h_2 \in f(G)$ esistono $g_1, g_2 \in f(G)$ tali che $f(g_1) = h_1$, $f(g_2) = h_2$. Ne segue

$$h_1 h_2^{-1} = f(g_1)\, f(g_2)^{-1} = f\left(g_1 g_2^{-1}\right) \in f(G).$$

5) $f(a) = f(b) \iff f(a)f(b)^{-1} = 1_H \iff f(ab^{-1}) = 1_H \iff ab^{-1} \in \text{Ker } f$. ∎

(7.7) Teorema (fondamentale sugli omomorfismi).

1) *Siano* N *un sottogruppo normale di* G *e* $\frac{G}{N}$ *il corrispondente gruppo quoziente. La proiezione canonica* $\pi : G \to \frac{G}{N}$ *definita ponendo*

$$\pi(g) := Ng$$

è un epimorfismo. Inoltre $N = \text{Ker } \pi$.

2) *Sia* $f : G \to H$ *un omomorfismo di gruppi e sia* $\pi : G \to \frac{G}{\text{Ker } f}$ *la proiezione canonica. Allora* f *induce un unico isomorfismo* $\overline{f} : \frac{G}{\text{Ker } f} \to f(G)$ *tale che*

$$\overline{f}\pi = f. \tag{7.8}$$

In particolare

$$\frac{G}{\text{Ker } f} \cong f(G). \tag{7.9}$$

Dimostrazione.
1) Per ogni $a, b \in G$ si ha: $\pi(ab) = N(ab) = NaNb = \pi(a)\pi(b)$.
Inoltre $\pi(a) = N1_G \Longleftrightarrow a \in N$. Quindi Ker $\pi = N$.
2) La condizione (7.8) determina $\overline{f}$, dovendo essere $\overline{f}\,((\text{Ker } f)g) = \overline{f}\,(\pi(g)) = f(g)$. Verifichiamo che ponendo, per ogni elemento (Ker f)g di $G/\text{ Ker } f$

$$\overline{f}\,((\text{Ker } f)g) := f(g)$$

si definisce una applicazione. Infatti (Ker f)a = (Ker f)b implica $ab^{-1} \in$ Ker f da cui $f(a) = f(b)$ per il punto 5) del precedente Lemma.
$\overline{f}$ è un omomorfismo in quanto, posto $K =$ Ker f:

$$\overline{f}\,(Ka\ Kb) \ = \ \overline{f}\,(Kab) \ = \ f(ab) \ = \ f(a)f(b) \ = \ \overline{f}\,(Ka)\,\overline{f}\,(Kb)\,.$$

Chiaramente $\overline{f}$ è suriettiva. Dimostriamo che è anche iniettiva.

$$\overline{f}\,((\text{Ker } f)a) = \overline{f}\,((\text{Ker } f)b) \implies f(a) = f(b) \implies ab^{-1} \in \text{Ker } f \implies (\text{Ker } f)\,a = (\text{Ker } f)\,b.$$

Si conclude che $\overline{f}$ è un isomorfismo. Pertanto vale (7.9). ■

(7.10) Esempio *Sia* $\mathrm{GL}_2(\mathbb{C})$ *il gruppo moltiplicativo delle matrici* 2×2*, a elementi complessi, con determinante* $\neq 0$*. (Si veda l'Esempio* 3.1 *del Capitolo* 3*). L' applicazione*

$$\det : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^*$$

che ad ogni matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *assegna il suo determinante* $\det A = ad - bc$*, è un epimorfismo di gruppi, il cui nucleo consiste delle matrici di determinante 1. Tale nucleo è detto il gruppo* speciale lineare *di grado* 2 *su* $\mathbb{C}$*, e indicato con* $\mathrm{SL}_2(\mathbb{C})$*. Ne segue*

$$\frac{\mathrm{GL}_2(\mathbb{C})}{\mathrm{SL}_2(\mathbb{C})} \cong \mathbb{C}^*.$$

Ogni gruppo ciclico è immagine epimorfa del gruppo additivo dei numeri interi. Inoltre, due gruppi ciclici dello stesso ordine sono isomorfi. Vale infatti il seguente:

(7.11) Teorema *Sia* g *un elemento di un gruppo* $(G.\cdot, 1_G)$*, e sia* $\langle g \rangle$ *il sottogruppo ciclico generato da* g*. Indicando al solito con* $(\mathbb{Z}, +, 0)$ *il gruppo additivo dei numeri interi, si ha:*

1) *se* $o(g) = 0$*, allora* $(\mathbb{Z}, +, 0) \cong \langle g \rangle$*;*

2) *se* $o(g) = n > 0$, *allora* $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \langle g \rangle$;

In particolare, se $o(g) = n > 0$, *per ogni* $a, b \in \mathbb{Z}$, *si ha:*

$$g^a = g^b \Longleftrightarrow a \equiv b \pmod{n}.$$

Dimostrazione. L'applicazione $f : \mathbb{Z} \to \langle g \rangle$ tale che $f(z) := g^z$ è un omomorfismo. Infatti $f(z+t) = g^{z+t} = g^z g^t$. Chiaramente $f(\mathbb{Z}) = \langle g \rangle$. Inoltre Ker $f = \{0\}$ se $o(g) = 0$, mentre Ker $f = n\mathbb{Z}$ se $o(g) = n$. Gli isomorfismi dei punti 1) e 2) seguono quindi da (7.9). Infine, tenendo presente il punto 5) del Lemma 7.6,

$$g^a = g^b \Longleftrightarrow f(a) = f(b) \Longleftrightarrow (a-b) \in n\mathbb{Z} \Longleftrightarrow a \equiv b \pmod{n}.$$

■

(7.12) Corollario *Ogni elemento* g *di un gruppo finito* G *ha periodo un divisore di* $|G|$.

Dimostrazione. Per il punto 1) del Teorema 7.11 il periodo $o(g)$ di g non può essere 0. Quindi $o(g) = n > 0$. Per il punto 2) dello stesso Teorema si ha $n = |\mathbb{Z}_n| = |\langle g \rangle|$. Poichè $\langle g \rangle$ è un sottogruppo di G, la tesi segue dal Teorema 4.7 di Lagrange. ■

Dato un gruppo $(G, \cdot, 1_G)$ e fissato $g \in G$, consideriamo l'applicazione $\mu_g : G \to G$ che consiste nella *moltiplicazione a sinistra per* g, ossia tale che, per ogni $x \in G$:

$$\mu_g(x) := gx. \tag{7.13}$$

La μ_g è bijettiva, avendo come inversa la $\mu_{g^{-1}}$. Pertanto μ_g è un elemento del gruppo $\mathrm{Sym}(G)$ delle applicazioni bijettive dell' insieme G in sè .

(7.14) Teorema (di Cayley) *L'applicazione* $\mu : G \to \mathrm{Sym}(G)$ *tale che, per ogni* $g \in G$*:*

$$\mu(g) := \mu_g \tag{7.15}$$

è un monomorfismo da G *al gruppo* $\mathrm{Sym}(G)$. *In particolare* G *è isomorfo al sottogruppo* $\mu(G)$ *di* $\mathrm{Sym}(G)$.

Dimostrazione. Per ogni $g_1, g_2 \in G$ si ha $\mu(g_1 g_2) = \mu(g_1)\,\mu(g_2)$. Infatti, per ogni $x \in G$:

$$\mu_{g_1 g_2}(x) = (g_1 g_2)\, x = g_1 (g_2 x) = g_1 (\mu_{g_2}(x)) = \mu_{g_1} (\mu_{g_2}(x)) = (\mu_{g_1} \mu_{g_2})(x).$$

Quindi μ è un omomorfismo. Infine Ker $f = 1_G$. Infatti $\mu(g) = \mathrm{Id}_G$ se e solo se $gx = x$ per ogni $x \in G$, se e solo se $g = 1_G$. ■

Questo Teorema rende i gruppi, in un certo senso, uniformi. Infatti dice che ogni gruppo G è isomorfo a un gruppo di trasformazioni (o di permutazioni se finito).

(7.16) Esempio *Sia* $G = \{1, i, -1, -i\}$ *il sottogruppo di* $\mathbb{C}^*$ *generato da* $i = e^{i\pi/2}$. $\mu(G)$ *è il sottogruppo di* $\mathrm{Sym}(G)$ *costituito dalle permutazioni:*

$$\begin{array}{rcc} \mu_1 & = & \mathrm{Id} \\ \mu_i & = & (1, i, -1, -i) \\ \mu_{-1} & = & (1, -1)(i, -i) \\ \mu_{-i} & = & (1, -i, -1, i) \end{array}$$

Il monomorfismo $\mu : G \to \mathrm{Sym}(G)$ *è il seguente:*

$$\begin{array}{rcc} 1 & \mapsto & \mathrm{Id} \\ i & \mapsto & (1, i, -1, -i) \\ -1 & \mapsto & (1, -1)(i, -i) \\ -i & \mapsto & (1, -i, -1, i) \end{array}$$

Capitolo III

Anelli

1 Generalità

(1.1) Definizione *Un anello* $(A, +, \cdot, 0_A, 1_A)$ *è una struttura algebrica in cui* A *è un insieme,* 0_A*,* 1_A *sono elementi di* A *e* $+$*,* $\cdot$ *sono operazioni binarie in* A*, per cui valgono le seguenti proprietà :*

1) $(A, +, 0_A)$ *è un gruppo abeliano;*

2) $(A, \cdot, 1_A)$ *è un monoide;*

3) *per ogni* $a, b, c \in A$*:*

4) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(proprietà distributiva sinistra);*

5) $(a + b) \cdot c = a \cdot c + b \cdot c$ *(proprietà distributiva destra).*

Le operazioni $+$ e $\cdot$ si dicono, rispettivamente, la somma e il prodotto. L'elemento neutro rispetto alla somma, 0_A, si dice lo zero. L'elemento neutro rispetto al prodotto, 1_A, si dice l'unitá. Scriveremo ab anziché $a \cdot b$.

(1.2) Definizione *L'anello* A *è* commutativo *se il prodotto è commutativo, ossia se* $ab = ba$ *per ogni* $a, b \in A$*.*

(1.3) Lemma *Sia* A *un anello. Per ogni* $a, b \in A$ *e per ogni* $z \in \mathbb{Z}$ *si ha:*

1) $a0_A = 0_A = 0_A a$*;*

2) $(-a)b = -(ab) = a(-b)$*;*

3) $(za)b = z(ab) = a(zb)$*.*

Dimostrazione.

1) $a0_A + a0_A = a(0_A + 0_A) = a0_A$. Quindi $a0_A + a0_A = a0_A$ implica $a0_A = 0_A$ per le leggi di cancellazione della somma nel gruppo $(A, +, 0_A)$ (si veda (6.1) del Capitolo 2). Analogamente si prova $0_A a = 0_A$.

2) $(-a)b + ab = (-a + a)b = 0_A b = 0_A$. Da $(-a)b + ab = 0_A$ segue $(-a)b = -(ab)$.
Analogamente si prova che $a(-b) = -(ab)$.
3) Per $z \geq 0$ ragioniamo per induzione.
Se $z = 0$ si ha $(0a)b = 0_A b = 0_A = 0(ab)$.
Se $z > 0$, per l'ipotesi induttiva $((z-1)a)b = (z-1)(ab)$. Quindi:

$$(za)b \;=\; ((z-1)a + a)\, b \;=\; ((z-1)a)b + (ab) \;=\; (z-1)(ab) + (ab) \;=\; z(ab).$$

Sia ora $z < 0$. Essendo $-z > 0$, per quanto appena provato si ha: $(-za)b = -z(ab)$.
Passando agli opposti: $-\left((-za)b\right) = z(ab)$. Per il punto 2), si conclude $(za)b = z(ab)$. ■

Dal punto 1) segue che se un anello A ha almeno due elementi, allora $0_A \neq 1_A$.

(1.4) Definizione *Un elemento $a \in A$ si dice un divisore dello zero se $a \neq 0_A$ ed esiste $b \in A,\ b \neq 0_A$, tale che $ab = 0_A$ oppure $ba = 0_A$.*

Pertanto A è *privo di divisori dello zero* se, per ogni $a, b \in A$:

$$ab = 0_A \;\Rightarrow\; (a = 0_A \text{ oppure } b = 0_A).$$

(1.5) Teorema *In un anello A, privo di divisori dello zero, valgono le* leggi di cancellazione del prodotto. *Ossia, per ogni $a, x, y \in A$:*
1) $(a \neq 0_A \text{ e } ax = ay) \;\Rightarrow\; x = y$;
2) $(a \neq 0_A \text{ e } xa = ya) \;\Rightarrow\; x = y$.
In particolare $(a \neq 0_A \text{ e } ax = a) \;\Rightarrow\; x = 1_A$.

Dimostrazione.
1) $ax = ay \;\Rightarrow\; ax - ay = 0_A \Rightarrow\; a(x-y) = 0_A$. Essendo $a \neq 0_A$, si ha $x - y = 0_A$. La 2) si dimostra in modo analogo. Ponendo $y = 1_A$ nella 1) si ha l'ultima osservazione. ■

(1.6) Definizione *Per ogni $a \in A$, si dice* caratteristica *di a e la si indica con* $\mathrm{char}(a)$, *il periodo di a come elemento del gruppo additivo $(A, +, 0_A)$.*

Chiaramente l'unico elemento di A che ha caratteristica 1 é 0_A.

(1.7) Teorema *In un anello A, privo di divisori dello zero, tutti gli elementi diversi da zero hanno la stessa caratteristica, detta la* caratteristica di A. *Essa é 0 oppure un numero primo p.*

Dimostrazione. Siano $a, b \in A$, con $a \neq 0_A$, $b \neq 0_A$. Per ogni $k \in \mathbb{Z}$:

$$ka = 0_A \iff (ka)b = a(kb) = 0_A \iff kb = 0_A.$$

Ne segue che $\text{char}(a) = \text{char}(b)$. Nel caso in cui $\text{char}(a) = p > 0$, resta da dimostrare che p è un numero primo. Per assurdo sia $p = nm$ una fattorizzazione in cui $1 < m < p$. Posto $b = ma$, si ha $b \neq 0_A$, quindi $\text{char}(b) = p$. D'altra parte:

$$nb = n(ma) = (nm)a = pa = 0_A$$

in contrasto con $1 < n < p$. Si conclude che p é primo. ■

(1.8) Definizione *Diciamo che $a \in A$ è* unitario*, se ha inverso moltiplicativo, ossia se esiste $b \in A$ tale che $ab = ba = 1_A$. In tal caso si scrive $b = a^{-1}$.*

Indichiamo con A^* l'insieme degli elementi unitari di A. In virtù del Lemma 1.17 del Capitolo 2, A^* è un gruppo rispetto al prodotto dell'anello A.

(1.9) Definizione *Un* campo $\mathbb{K}$ *è un anello commutativo in cui ogni elemento diverso da zero è invertibile.*

(1.10) Esempio *L'insieme $\mathbb{C}$ dei numeri complessi è un campo rispetto alle usuali operazioni di somma e prodotto. Esso ha caratteristica* 0*.*

Importanti esempi di sottocampi di $\mathbb{C}$ sono:
• Il campo $\mathbb{R}$ dei numeri reali.
• Il campo $\mathbb{Q}$ dei numeri razionali.

(1.11) Esercizio *Si dimostri che un campo non ha divisori dello zero.*

2 L'anello $\mathbb{Z}$ dei numeri interi

L'insieme $\mathbb{Z}$ dei numeri interi, rispetto alle usuali operazioni di somma e prodotto, è un anello commutativo, privo di divisori dello zero. Cioè è un dominio di integrità .
Ricordiamo che, per ogni $z \in \mathbb{Z}$, il modulo $|z|$ di z è definito mediante:

$$|z| := \begin{cases} z & \text{se} \quad z \geq 0 \\ -z & \text{se} \quad z < 0 \end{cases} .$$

Per ogni $a, b, c \in \mathbb{Z}$ si ha:

$$|a| = 1 \iff a \in \{1, -1\}\,; \tag{2.1}$$

$$|bc| = |b|\,|c|; \tag{2.2}$$

$$(0 \le a < c \ \text{ e } \ 0 \le b < c) \implies |a-b| < c. \tag{2.3}$$

In virtù di (2.1) e di (2.2), gli elementi invertibili dell'anello $\mathbb{Z}$ sono ± 1, ossia

$$\mathbb{Z}^* = \{1, -1\}\,.$$

(2.4) Teorema *Siano $a, b \in \mathbb{Z}$, con $b \neq 0$. Esistono e sono unici $q, r \in \mathbb{Z}$ tali che:*
1) *a=bq+r;*
2) $0 \le r < |b|$.

Dimostrazione. Dimostriamo innanzitutto l'esistenza di q e di r.
Caso $a \ge 0$. Induzione su a.
Se $a < |b|$, i numeri $q = 0$, $r = a$ soddisfano le condizioni 1) e 2).
Se $a \ge |b|$, si ha $0 \le a - |b| < a$. Per induzione, esistono $q', r \in \mathbb{Z}$ tali che:

$$1')\quad a - |b| = bq' + r, \qquad 2)\quad 0 \le r < |b|.$$

Dalla 1′) segue

$$a \;=\; bq' + r + |b| \;=\; b(q' + \epsilon) + r$$

dove $\epsilon = \pm 1$. Pertanto i numeri $q := q' + \epsilon$ e r soddisfano le condizioni 1) e 2).
Caso $a < 0$. Per quanto dimostrato, esistono $q', r' \in \mathbb{Z}$ tali che:

$$1'')\quad -a = bq' + r', \qquad 2'')\quad 0 \le r' < |b|.$$

Se $r' = 0$, i numeri $q = -q'$, $r = 0$ soddisfano 1) e 2). Se $r' > 0$, dalla 1″) segue

$$a \;=\; b(-q') - |b| + |b| - r' \;=\; b(-q' + \epsilon) \;+\; \left(|b| - r'\right).$$

I numeri $q = -q' + \epsilon$, $r = |b| - r'$ soddisfano 1) e 2).

Mostriamo infine l'unicità di q e di r. Siano $q,\ \overline{q},\ r,\ \overline{r} \in \mathbb{Z}$ tali che:

$$a \;=\; bq + r \;=\; b\overline{q} + \overline{r}, \quad 0 \;\le\; r,\ \overline{r} \;<\; |b|.$$

Ne segue $b(q - \overline{q}) = \overline{r} - r$ e, in virtù di (2.3), $|\overline{r} - r| < |b|$. Pertanto:

$$0 \;\le\; |b(q - \overline{q})| \;=\; |\overline{r} - r| \;< |b|. \tag{2.5}$$

Se fosse $(q-\overline{q}) \neq 0$, si avrebbe $|q-\overline{q}| \geq 1$ da cui $|b(q-\overline{q})| \geq |b|$, in contrasto con (2.5). Si conclude $q-\overline{q}=0$, $r-\overline{r}=0$. ■

(2.6) Definizione *Nelle notazioni del Teorema* (2.4) *i numeri* q *ed* r *si chiamano il* quoziente *e il* resto *della divisione di* a *per* b. *Si dice inoltre che* b divide a, *e si scrive* $b \mid a$, *se* $r=0$.

3 Altri esempi di anelli

(3.1) Esempio *Sia* R *un anello commutativo. L'insieme* $\mathrm{Mat_2(R)}$ *delle matrici quadrate* 2×2 *a elementi in* R *è un anello rispetto alla somma definita componente per componente e al prodotto righe per colonne. Precisamente:*

$$\mathrm{Mat_2(R)} = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mid \mathrm{a_{ij}} \in \mathrm{R} \right\}.$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}.$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}.$$

Si noti che, ponendo $0=0_R$, $1=1_R$, *si ha:*

$$0_{\mathrm{Mat_2(R)}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad 1_{\mathrm{Mat_2(R)}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Tale anello è non commutativo e ha divisori dello zero. Infatti, ad esempio, posto:

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

si ha:

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

Il gruppo $\mathrm{Mat_2(R)^*}$ *degli elementi invertibili di* $\mathrm{Mat_2(R)}$ *si indica anche con* $\mathrm{GL_2}(R)$ *e lo si chiama il* gruppo generale lineare *di grado* 2 *su* R.
Se $R=\mathbb{K}$ *è un campo, si verifica facilmente che* $\mathrm{GL_2}(\mathbb{K})$ *è costituito dalle matrici con determinante* $\neq 0_{\mathbb{K}}$. *Si noti che:*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{-1} = \frac{1}{a_{11}a_{22}-a_{12}a_{21}} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

(3.2) Esercizio *Fissato $n \in \mathbb{N}$, si dimostri che, per ogni $a, a', b, b' \in \mathbb{Z}$:*

$$\left\{ \begin{array}{ll} a \equiv a' & (\mathrm{mod}\ n) \\ b \equiv b' & (\mathrm{mod}\ n) \end{array} \right. \quad \Longrightarrow \quad (ab) \equiv (a'b') \pmod{n}. \tag{3.3}$$

Tenendo presente il Lemma 6.4 del Capitolo 2 e l'esercizio precedente, si dimostra facilmente il seguente:

(3.4) Lemma *Per ogni $n \geq 2$ l'insieme $\mathbb{Z}_n$ delle classi di resti modulo n è un anello commutativo rispetto alle operazioni:*

$$[a]_n + [b]_n := [a+b]_n, \quad [a]_n[b]_n := [ab]_n.$$

(3.5) Esempio *L'anello $\mathbb{Z}_7$ è un campo, infatti:*

$[a]_7$	$([a]_7)^{-1}$
$[1]_7$	$[1]_7$
$[2]_7$	$[4]_7$
$[3]_7$	$[5]_7$
$[-3]_7$	$[-5]_7$
$[-2]_7$	$[-4]_7$
$[-1]_7$	$[-1]_7$

(3.6) Esempio *L'anello $\mathbb{Z}_6$ ha divisori dello zero. Infatti $[2]_6[3]_6 = [0]_6$.*

4 Potenza del binomio

Per ogni numero naturale n si definisce induttivamente il fattoriale nel modo seguente. $0! := 1$ e, per n positivo, $n! := (n-1)!\, n$. Equivalentemente

$$n! := \prod_{i=1}^{n} i.$$

Esso concide con l'ordine del gruppo simmetrico $\mathrm{Sym}(n)$: infatti le applicazioni bijettive di un insieme di n elementi sono $n!$.

Per ogni $n, k \in \mathbb{N}$, con $0 \leq k \leq n$, si definisce il *coefficiente binomiale*

$$\left(\begin{array}{c} n \\ k \end{array} \right) := \frac{n!}{(n-k)!\, k!}$$

Esso è sempre un intero. La dimostrazione di tale fatto si ottiene, per induzione, dal Lemma 4.1. Oppure anche notando che $\left(\begin{array}{c} n \\ k \end{array} \right)$ rappresenta il numero dei sottoinsiemi di ordine k di un insieme di ordine n.

(4.1) Lemma

1) *per* $0 \leq k \leq n$: $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$;

2) $\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = 1$;

3) *per* $1 \leq k \leq n-1$: $\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right)$.

Dimostrazione.

1) $\left(\begin{array}{c} n \\ n-k \end{array} \right) := \frac{n!}{(n-(n-k))!\,(n-k)!} = \frac{n!}{(n-k)!\,k!} := \left(\begin{array}{c} n \\ k \end{array} \right)$

2) $\left(\begin{array}{c} n \\ 0 \end{array} \right) := \frac{n!}{(n)!\,0!} = 1.$

3) $\left(\begin{array}{c} n-1 \\ k-1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right) = \frac{(n-1)!}{(n-1-(k-1))!\,(k-1)!} + \frac{(n-1)!}{(n-1-k)!\,k!} =$

$\frac{(n-1)!}{(n-k)!\,(k-1)!} + \frac{(n-1)!}{(n-1-k)!\,k!} = \frac{(n-1)!\,k+(n-1)!\,(n-k)}{(n-k)!\,k!} = \frac{(n-1)!\,(k+n-k)!}{(n-k)!\,k!} = \left(\begin{array}{c} n \\ k \end{array} \right)$. ■

Da questo Lemma si ricava il triangolo di Tartaglia , utile per il calcolo dei coefficienti binomiali:

$$\begin{array}{ccccccccccc}
 & & & & \left(\begin{array}{c} 0 \\ 0 \end{array} \right) & & & & & & \\
 & & & \left(\begin{array}{c} 1 \\ 0 \end{array} \right) & & & \left(\begin{array}{c} 1 \\ 1 \end{array} \right) & & & & \\
 & & \left(\begin{array}{c} 2 \\ 0 \end{array} \right) & & & \left(\begin{array}{c} 2 \\ 1 \end{array} \right) & & & \left(\begin{array}{c} 2 \\ 2 \end{array} \right) & & \\
 & \left(\begin{array}{c} 3 \\ 0 \end{array} \right) & & & \left(\begin{array}{c} 3 \\ 1 \end{array} \right) & & & \left(\begin{array}{c} 3 \\ 2 \end{array} \right) & & & \left(\begin{array}{c} 3 \\ 3 \end{array} \right) & \\
\ldots & & & & \ldots & & & & & & \ldots
\end{array}$$

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & & 1 & & & & \\
 & & 1 & & 2 & & & 1 & & & \\
 & 1 & & 3 & & & 3 & & 1 & & \\
1 & & 4 & & & 6 & & & 4 & & 1 \\
 & 5 & & & 10 & & & 10 & & 5 & \\
\ldots & & & & \ldots & & & & & \ldots & 1
\end{array}$$

(4.2) Lemma *Siano* $a, b \in A$. *Se* $ab = ba$, *allora:*

$$(a+b)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^k.$$

Così $(a+b)^2 = a^2 + 2ab + b^2$, $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, ...

Dimostrazione.

Induzione su n.

Per $n = 0$, $(a+b)^0 := 1_A = \binom{0}{0} a^0 b^0$. Per $n > 0$: $(a+b)^n =$

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

$$\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k}\ b^k\ +\ \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k}\ b^{k+1} =$$

$$a^n\ +\ \sum_{k=1}^{n-1} \binom{n-1}{k} a^{n-k}\ b^k\ +\ \sum_{k=0}^{n-2} \binom{n-1}{k} a^{n-1-k}\ b^{k+1}\ + b^n =$$

ponendo $h = k + 1$

$$a^n\ +\ \sum_{k=1}^{n-1} \binom{n-1}{k} a^{n-k}\ b^k\ +\ \sum_{h=1}^{n-1} \binom{n-1}{h-1} a^{n-h}\ b^h\ + b^n =$$

chiamando di nuovo k l'indice variabile h

$$a^n\ +\ \sum_{k=1}^{n-1} \left(\binom{n-1}{k} + \binom{n-1}{k-1} \right) a^{n-k}\ b^k\ +\ b^n =$$

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

■

5 Anelli di polinomi

Sia R un anello commutativo. L'insieme $R[x]$ dei polinomi a coefficienti in R, nella indeterminata x, è un anello commutativo rispetto alla somma e al prodotto di polinomi. Ricordiamo che se

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad b(x) = b_0 + b_1 x + \cdots + b_m x^m \tag{5.1}$$

si ha

$$a(x) + b(x)\ :=\ (a_0 + b_0) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + \ldots$$

$$a(x)\, b(x)\ :=\ (a_0 b_0) + (a_1 b_0 + a_0 b_1)\, x + \cdots + a_n b_m x^{n+m}.$$

L'elemento neutro rispetto alla somma è il polinomio nullo, che indicheremo con $\underline{0}$. L'elemento neutro rispetto al prodotto è il polinomio $1_{\mathbb{K}}x^0$.

(5.2) Definizione *Il* grado $\deg a(x)$ *è definito mediante:*

1) $\deg a(x) := -\infty$, *se* $a(x) = \underline{0}$;

2) $\deg a(x) := n \geq 0$, *se* $a(x) = a_0 + a_1x + \cdots + a_nx^n$ *con* $a_n \neq 0$.

Conviene porre, per ogni numero naturale $n \geq 0$:

$$-\infty < n, \quad -\infty + n = -\infty.$$

Due polinomi sono *uguali* se hanno tutti i coefficienti ordinatamente uguali.
In particolare polinomi uguali hanno lo stesso grado.

(5.3) Lemma *Siano* $a(x), b(x) \in R[x]$ *e supponiamo* $m := \deg b(x) \leq n := \deg a(x)$.

1) $\deg(a(x) + b(x)) \leq n$;

2) $\deg(a(x)b(x)) \leq n + m$;

3) *se* R *è privo di divisori dello zero,* $\deg(a(x)b(x)) = n + m$.

Dimostrazione.
L'asserto è ovvio se $a(x)$ o $b(x)$ sono nulli. Altrimenti siano $a(x), b(x)$ come in (5.1).
1) Scrivendo $b(x) = \sum_{i=0}^{n} b_jx^j$ dove $b_{m+1} = \cdots = b_n = 0$ se $n > m$, si ha:
$a(x) + b(x) = \sum_{i=0}^{n}(a_i + b_i)x^i = (a_0 + b_0)x^0 + \cdots + (a_n + b_n)x^n$.
Esso ha quindi grado n se $b_n \neq -a_n$ ha grado $\leq n - 1$ se $b_n = -a_n$.
2) Scrivendo $a(x) = \sum_{j=0}^{n+m} a_jx^j$, dove $a_j = 0$ per $j > n$ e
$b(x) = \sum_{j=0}^{n+m} b_jx^j$ dove $b_j = 0$ se $j > m$, si ha:
$a(x)b(x) = \sum_{j=0}^{n+m} \left(\sum_{h=0}^{j} a_hb_{j-h}\right) x^j = c_0x^0 + \cdots + c_{n+m}x^{n+m}$.
3) Il coefficiente $c_{n+m} := \sum_{h=0}^{n+m} a_hb_{j-h}$ di $a(x)b(x)$ coincide con a_nb_m. Infatti per $h < n$ si ha $n + m - h > m$ da cui $b_m = 0$ e per $h > n$ si ha $a_h = 0$.
Se R è privo di divisori dello zero da $a_n \neq 0$ e $b_m \neq 0$ segue $a_nb_m \neq 0$. ∎

(5.4) Esercizio *Dimostrare che* $R[x]$ *è privo di divisori dello zero se e solo se* R *è privo di divisori dello zero.*

(5.5) Esercizio *Sia* $\mathbb{K}$ *un campo. Dimostrare che* $\mathbb{K}[x]$ *è privo di divisori dello zero e che gli elementi invertibili di* $\mathbb{K}[x]$ *sono i polinomi di grado 0.*

(5.6) Teorema *Siano $a(x), b(x) \in \mathbb{K}[x]$ con $b(x) \neq \underline{0}$. Allora esistono e sono unici $q(x)$, $r(x) \in \mathbb{K}[x]$ tali che:*
1) $a(x) = b(x)q(x) + r(x)$,
2) $\deg(r(x)) < \deg(b(x))$.

Dimostrazione.
Posto $\deg a(x) = n$, $\deg b(x) = m \geq 0$, dimostriamo l'esistenza di $q(x)$ e $r(x)$ per induzione su n. Se $m > n$ (in particolare nel caso $n = -\infty$), i polinomi $q(x) = \underline{0}$ e $r(x) = a(x)$ soddisfano 1) e 2). Sia quindi $n \geq m$.
Detti a_n e b_m i coefficienti direttivi di $a(x)$ e $b(x)$ rispettivamente, definiamo:

$$a_1(x) \ := \ a(x) \ - \ a_n b_m^{-1} x^{n-m}\, b(x). \tag{5.7}$$

Poichè $\deg a_1(x) < n$, per induzione esistono $q_1(x), r(x) \in \mathbb{K}[x]$ tali che:
$a_1(x) = b(x)q_1(x) + r(x)$,
$\deg(r(x)) < deg(b(x))$.
Ricavando $a(x)$ da (5.7), si conclude che $r(x)$ e $q(x) := a_n b_m^{-1} x^{n-m} + q_1(x) \in \mathbb{K}[x]$ soddisfano la 1) e la 2). Quanto alla loro unicità , siano $\overline{q}(x), \overline{r}(x) \in \mathbb{K}[x]$ tali che:
$1')$ $a(x) = b(x)\overline{q}(x) + \overline{r}(x)$,
$2')$ $\deg(\overline{r}(x)) < deg(b(x))$.
Sottraendo $1')$ da 1) si ottiene:

$$b(x)\,(q(x) - \overline{q}(x)) \ = \ \overline{r}(x) - r(x) \tag{5.8}$$

dove possiamo supporre $\deg \overline{r}(x) \leq \deg r(x)$. Ne segue:

$$\deg\,(b(x)) + \deg\,(q(x) - \overline{q}(x)) \ = \ \deg\,(\overline{r}(x) - r(x)) \ \leq \ \deg\,(r(x)) \ < \ \deg\,(b(x))\,.$$

Deve quindi essere $\deg\,(q(x) - \overline{q}(x)) = -\infty$, ossia $q(x) - \overline{q}(x) = \underline{0}$. Sostituendo questa condizione in (5.8) si ha anche $r(x) - \overline{r}(x) = \underline{0}$. ∎

(5.9) Definizione *Nelle notazioni del Teorema* (5.6) *i polinomi $q(x)$ ed $r(x)$ si chiamano il* quoziente *e il* resto *della divisione di $a(x)$ per $b(x)$. Si dice inoltre che $b(x)$* divide *$a(x)$, e si scrive $b(x) \mid a(x)$, se $r(x) = \underline{0}$.*

Ogni polinomio $f(x) = r_0 x^0 + \cdots + r_n x^n \in R[x]$, dove R è un anello commutativo, dà luogo alla *funzione polinomiale* $f : R \to R$ definita ponendo, per ogni $\alpha \in R$:

$$f(\alpha) \ := \ r_0 \alpha^0 + \cdots + r_n \alpha^n.$$

Chiaramente, se $\deg f(x) \leq 0$, la funzione f è *costante*. Menzioniamo il fatto che, a volte, polinomi distinti danno luogo alla stessa funzione polinomiale.

(5.10) Definizione *Un elemento $\alpha \in \mathbb{K}$ è* radice *di $f(x) \in \mathbb{K}[x]$ se $f(\alpha) = 0_{\mathbb{K}}$.*

(5.11) Teorema (di Ruffini) *Sia $f(x) \in \mathbb{K}[x]$, dove $\mathbb{K}$ è un campo. Un elemento $\alpha \in \mathbb{K}$ è radice di $f(x)$ se e solo se $(x - \alpha)$ divide $f(x)$.*

Dimostrazione.
Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $f(x)$ per $(x-\alpha)$. Poichè $(x-\alpha)$ ha grado 1, deve essere $\deg(r(x)) \leq 0$, ossia $r(x) = kx^0$.
Da $f(x) = (x - \alpha)\, q(x) + kx^0$ segue

$$f(\alpha) \;=\; (\alpha - \alpha)\, q(\alpha) + k\alpha^0 \;=\; 0_{\mathbb{K}}\, q(\alpha) + k\, 1_{\mathbb{K}} \;=\; k.$$

Si conclude

$$f(\alpha) = 0_{\mathbb{K}} \iff k = 0_{\mathbb{K}} \iff r(x) = \underline{0} \iff (x - \alpha) \mid f(x).$$

■

Capitolo IV

Dominii euclidei

1 Dominii di integrità

(1.1) Definizione *Un anello R si dice un* dominio di integrità *se è commutativo e privo di divisori dello zero.*

Chiaramente ogni sottoanello di un campo è un dominio di integrità . Viceversa si può dimostrare che ogni dominio di integrità R è isomorfo a un sottoanello di un campo (si veda, ad esempio, [5, Teorema 5.5.3, pagina 71]). In questo paragrafo R indicherà un dominio di integrità : per il Teorema 1.5 del Capitolo 3, in R valgono le leggi di cancellazione. Al solito R^* indica l'insieme degli elementi invertibili di R. Ricordiamo che $\mathbb{Z}^* = \{1, -1\}$ e, se $\mathbb{K}$ è un campo, $\mathbb{K}[x]^* = \{\text{polinomi di grado } 0\}$.

(1.2) Definizione *Dati $a, b \in R$, diciamo che b* divide *a, e scriviamo $b \mid a$, se esiste $q \in R$ tale che $a = bq$.*

Se $b \neq 0$, allora q è unico. Infatti $bq = b\overline{q} \Longrightarrow q = \overline{q}$ per le leggi di cancellazione.

(1.3) Lemma *Siano $a_1, a_2, b \in R$.*
$(b \mid a_1 \text{ e } b \mid a_2) \implies b \mid (a_1x + a_2y)$ per ogni $x, y \in R$.

In particolare $(b \mid a_1 \text{ e } b \mid a_2) \Longrightarrow b \mid (a_1 \pm a_2)$. *Dimostrazione.*
Siano $q_1, q_2 \in R$ tali che $a_1 = bq_1$ e $a_2 = bq_2$. Ne segue

$$a_1x + a_2y = bq_1x + bq_2y = b(q_1x + q_2y).$$

Poiché $(q_1x + q_2y) \in R$ si conclude che $b \mid (a_1x + a_2y)$. ■

(1.4) Lemma *Siano a, b, c non nulli in R.*

1) $a \mid a$;

2) $(a \mid b \text{ e } b \mid a) \iff b = a\lambda$ *con* $\lambda \in R^*$;

3) $(a \mid b \text{ e } b \mid c) \implies a \mid c$.

Dimostrazione.

1) $a = a1_R$.

2) Supponiamo che $a \mid b$ e $b \mid a$. Per ipotesi $a = b\mu$, $b = a\lambda$ con $\mu, \lambda \in R$.
Da $b = a\lambda = b(\mu\lambda)$ segue $1_R = \mu\lambda$, ossia $\mu = \lambda^{-1}$. Pertanto $\lambda \in R^*$.
Viceversa, da $b = a\lambda$ con $\lambda \in R^*$ segue $a = b\lambda^{-1}$, ossia $a \mid b$ e $b \mid a$.

3) Da $b = aq_1$ e $c = bq_2$ con q_1 e $q_2 \in R$ segue $c = a(q_1q_2)$ con $(q_1q_2) \in R$. ■

(1.5) Definizione *Siano $a, b, d, m \in R$.*

1) d *è un* Massimo Comun Divisore *di a e b, in simboli $d = \mathrm{MCD}(a, b)$, se:*

(i) $d \mid a$ *e* $d \mid b$;

(ii) *per ogni* $c \in R$: $(c \mid a \text{ e } c \mid b) \implies c \mid d$.

$1')$ m *è un* minimo comune multiplo *di a e b, in simboli $m = \mathrm{mcm}(a, b)$, se:*

(i') $a \mid m$ *e* $b \mid m$;

(ii') *per ogni* $c \in R$: $(a \mid c \text{ e } b \mid c) \implies m \mid c$.

In R non è garantita l'esistenza di un MCD (a, b). D'altra parte, quando un MCD (a, b) esiste, anche tutti i suoi multipli secondo elementi invertibili (e solo quelli) sono MCD (a, b), come precisato nell' esercizio 1.6. Idem per mcm (a, b),

(1.6) Esercizio *Siano $a, b, d, d' \in R$, con $a \neq 0$, e sia $d = \mathrm{MCD}(a, b)$. Si dimostri che*

$$d' = \mathrm{MCD}(a, b) \qquad \iff \qquad d' = d\lambda \text{ con } \lambda \in R^*.$$

In particolare, un MCD(a, b) è invertibile se e solo se $1_R = \mathrm{MCD}(a, b)$.

(1.7) Esercizio *Siano $a, b, m, m' \in R$, con $a \neq 0$, e sia $m = \mathrm{mcm}(a, b)$. Si dimostri che*

$$m' = \mathrm{mcm}(a, b) \qquad \iff \qquad m' = m\lambda \text{ con } \lambda \in R^*.$$

(1.8) Esercizio *Sia $d = \mathrm{MCD}(a, b)$ e sia $\lambda \in R^*$. Si dimostri che:*

$$d = \mathrm{MCD}(a\lambda, b).$$

(1.9) Esercizio *Si dimostri che* $\mathrm{MCD}\,(a,b) = b$ *se e solo se* $b \mid a$.

(1.10) Lemma *Siano* $a, b \in R$ *e* $d = \mathrm{MCD}\,(a,b) \neq 0$. *Posto*

$$a = d\overline{a}, \quad b = d\overline{b} \tag{1.11}$$

si ha che $\overline{a}$ *e* $\overline{b}$ *sono* coprimi, *ossia* $\mathrm{MCD}\,(\overline{a},\overline{b}) = 1_R$.

Dimostrazione. Sia $\lambda \in R$ un divisore comune di $\overline{a}$ e $\overline{b}$. Ne segue che $d\lambda$ è un divisore comune di a e b. Pertanto $(d\lambda) \mid d$ per definizione di $\mathrm{MCD}\,(a,b)$. Sia $\mu \in R$ tale che $d = (d\lambda)\mu$. Da $d = d(\lambda\mu)$ segue $\lambda\mu = 1_R$, ossia $\lambda \in R^*$. ■

(1.12) Lemma *Siano* $a, b, q, r, d \in R$ *e si supponga* $a = bq + r$.

$$d = \mathrm{MCD}\,(b,r) \implies d = \mathrm{MCD}\,(a,b).$$

Dimostrazione.
• $(d \mid b \text{ e } d \mid r) \Longrightarrow d \mid (bq + r) = a$. Pertanto d è un divisore comune di a e b.
• Sia $c \in R$ tale che $c \mid a$ e $c \mid b$. Ne segue che $c \mid (a - bq) = r$. Da $c \mid b$ e $c \mid r$ e dall'ipotesi $d = \mathrm{MCD}\,(b,r)$ si deduce che $c \mid d$. ■

(1.13) Definizione *Sia* p *un elemento non nullo e non invertibile di* R.

1) p *è* primo *se, per ogni* $a, b \in R$:

$$p \mid (ab) \implies (p \mid a \text{ oppure } p \mid b)$$

2) p *è* irriducibile *se ha solo divisori banali, ossia se, per ogni* $a, b \in R$:

$$p = ab \implies (a \in R^* \text{ oppure } b \in R^*)\,.$$

(1.14) Esercizio *Sia* p *primo. Si dimostri che* $p\lambda$ *è primo per ogni* $\lambda \in R^*$.

(1.15) Esercizio *Sia* p *irriducibile. Si dimostri che* $p\lambda$ *è irriducibile per ogni* $\lambda \in R^*$.

(1.16) Lemma *Se* p *è* primo *e divide* $(a_1 a_2 \dots a_n)$, *allora divide almeno un* a_i.

Dimostrazione.

Poichè $p \mid a_1(a_2 \dots a_n)$, o divide a_1 o divide $(a_2 \dots a_n)$. Nel secondo caso, per induzione su n, p divide almeno un a_i, $i > 1$. ■

(1.17) Lemma *Ogni elemento primo di R è irriducibile.*

Dimostrazione.
Consideriamo una fattorizzazione $p = ab$ con $a, b \in R$. Poichè p divide se stesso, divide a oppure b, per definizione di elemento primo. Supponiamo, ad esempio, che p divida a, ossia $a = pq$, con $q \in R$. Da $p = p(qb)$ si deduce $1_R = qb$, da cui $b \in R^*$. Concludiamo che la fattorizzazione $p = ab$ è banale. ■

Un *dominio fattoriale* è un dominio di integrità in cui ogni elemento, non nullo e non invertibile, può essere scritto in modo essenzialmente unico come prodotto di un numero finito di elementi irriducibili. In modo più formale:

(1.18) Definizione *Un* dominio fattoriale *è un dominio di integrità R in cui:*

1) *ogni elemento non nullo e non invertibile $a \in R$ si scrive nella forma:*

$$a = p_1 \cdots p_n \tag{1.19}$$

dove $n \geq 1$ dipende da a, e i fattori p_j $(1 \leq j \leq n)$ sono elementi irriducibili di R;

2) *se $q_1, \dots, q_m$ sono irriducibili in R tali che:*

$$a = p_1 \dots p_n = q_1 \dots q_m \tag{1.20}$$

allora $n = m$ e, per un opportuno ordinamento dei fattori

$$q_j = p_j \lambda_j, \quad \text{con } \lambda_j \in R^*, \quad 1 \leq j \leq n.$$

2 Dominii euclidei

(2.1) Definizione *Sia $\varphi : D \setminus \{0_D\} \to \mathbb{N}$ una funzione. Il dominio di integrità D si dice un* dominio euclideo *rispetto a φ quando, per ogni $a, b \in D \setminus \{0_D\}$, si ha che:*

1) *se b divide a, allora $\varphi(b) \leq \varphi(a)$;*

2) *esistono $q, r \in D$ tali che $a = bq + r$ con $r = 0_D$ oppure $\varphi(r) < \varphi(b)$.*

(2.2) Osservazione *Dall'assioma* 1) *segue* $\varphi(1_D) \leq \varphi(d)$ *per ogni* $d \in D \setminus \{0_D\}$.

(2.3) Esempi

• *Ogni campo* $\mathbb{K}$ *è un dominio euclideo ponendo* $\varphi(k) := 1$ *per ogni* $k \in \mathbb{K} \setminus \{0_\mathbb{K}\}$.

• *In virtù del Teorema* 2.4 *del Capitolo* 3, *l'anello* $\mathbb{Z}$ *dei numeri interi è un dominio euclideo ponendo, per ogni* $z \in \mathbb{Z} \setminus \{0\}$,

$$\varphi(z) := |z|.$$

• *In virtù del Teorema* 5.6 *del Capitolo* 3, *l'anello* $\mathbb{K}[x]$ *dei polinomi a coefficienti in un campo* $\mathbb{K}$ *è un dominio euclideo ponendo, per ogni* $f(x) \in \mathbb{K}[x] \setminus \{\underline{0}\}$*:*

$$\varphi(f(x)) := \deg(f(x)).$$

(2.4) Lemma *Sia* D *un dominio euclideo rispetto* φ *e siano* $a, b, c, u \in D \setminus \{0_D\}$.
Se $a = bc$ *e* $c \notin D^*$, *allora* $\varphi(b) < \varphi(a)$. *In particolare, se* $\varphi(1_D) = \varphi(u)$, *allora* $u \in D^*$.

Dimostrazione. Siano $\overline{q}, \overline{r} \in D$ tali che $b = a\overline{q} + \overline{r}$ con $\overline{r} = 0_D$ oppure $\varphi(\overline{r}) < \varphi(a)$. Se fosse $\overline{r} = 0_D$, si avrebbe $a = a\overline{q}c$ da cui, semplificando per a, si otterrebbe $c \in D^*$, contro l'ipotesi. Pertanto $\varphi(\overline{r}) < \varphi(a)$. Da $\overline{r} = b - a\overline{q}$ e dall'ipotesi che b divide a, segue che b divide $\overline{r}$. Si conclude $\varphi(b) \leq \varphi(\overline{r}) < \varphi(a)$.
Infine sia $\varphi(1_D) = \varphi(u)$. Consideriamo l'identità $u = 1_D u$. Se u non appartenesse a D^*, si avrebbe la contraddizione $\varphi(1_D) < \varphi(u)$. Si conclude che $u \in D^*$. ■

Il seguente Teorema non solo dimostra l'esistenza del MCD di due elementi di un dominio euclideo, ma fornisce anche un metodo per calcolarlo, tramite una sequenza di divisioni. Per tale ragione esso è noto come l'algoritmo *delle divisioni successive*.

(2.5) Teorema *Sia* D *un dominio euclideo rispetto* $\varphi : D \setminus \{0_D\} \to \mathbb{N}$.
Per ogni $a, b \in D$, *esiste* $d = \mathrm{MCD}(a, b)$ *ed esistono* $x, y \in D$ *tali che*

$$d = ax + by. \tag{2.6}$$

Dimostrazione.
Se b divide a (in particolare se $a = 0$), l'asserto è vero. Infatti $b = \mathrm{MCD}(a, b)$, per definizione stessa di MCD. Inoltre $b = a0_D + b1_D$, ossia vale (2.6) con $x = 0_D$, $y = 1_D$. Notando che $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$ possiamo quindi supporre $a \neq 0$, $b \neq 0$, $\varphi(a) \geq \varphi(b)$ e ragionare per induzione su $\varphi(b)$.

Se $\varphi(b) = \varphi(1_D)$ si ha $b \in D^*$ per il Lemma 2.4, da cui $b \mid a$ (essendo $a = b(b^{-1}a)$) e l'asserto è vero per quanto osservato all'inizio.
Supponiamo quindi $\varphi(b) > \varphi(1_D)$. Per definizione di dominio euclideo esistono $q, r \in D$ tali che $a = bq + r$ con $r = 0$ oppure $\varphi(r) < \varphi(b)$. Se $r = 0$, ancora una volta $b \mid a$ e l'asserto è vero. Altrimenti, per l'ipotesi induttiva, esiste $d = \text{MCD}\,(b, r)$ ed esistono $x_1,\ y_1 \in D$ tali che $d = bx_1 + ry_1$. Per il Lemma 1.12 di questo Capitolo, si ha $d = \text{MCD}\,(a, b)$. Inoltre, sostituendo $r = a - bq$ in $d = bx_1 + ry_1$, si ottiene $d = ay_1 + b(x_1 - qy_1)$. Basta quindi porre $x = y_1$, $y = x_1 - qy_1$ per ottenere (2.6). ■

(2.7) Corollario *Siano $a, b, c \in D$. Se $a \mid (bc)$ e $\text{MCD}\,(a, b) = 1$, allora $a \mid c$.*

Dimostrazione. Sia $q \in D$ tale che $bc = aq$ e siano $x, y \in D$ tali che $1 = ax + by$.
Ne segue:

$$c = (ax + by)c = a(xc) + (bc)y = a(xc) + (aq)y = a(xc + qy).$$

Si conclude che $a \mid c$. ■

(2.8) Corollario *Dati $a, b \in D$, esiste $\text{mcm}\,(a, b)$. Inoltre*

$$\text{mcm}\,(a, b)\ \text{MCD}\,(a, b) = ab.$$

Dimostrazione. Sia $d = \text{MCD}\,(a, b)$.
Se $d = 0$, allora $a = b = 0$. Ne segue $\text{mcm}\,(a, b) = 0$ e l'asserto è vero.
Se $d \neq 0$, posto $a = d\overline{a}$, $b = d\overline{b}$, $m := a\overline{b}$, dimostriamo che $m = \text{mcm}\,(a, b)$.
Chiaramente $a \mid m = a\overline{b}$, e da $a\overline{b} = \overline{a}b$ segue che $b \mid m$.
Sia $c \in D$ tale che $a|c$ e $b|c$.

$$c = aq_1 = bq_2 \quad \Longrightarrow \quad d\overline{a}q_1 = d\overline{b}q_2 \quad \Longrightarrow \quad \overline{a}q_1 = \overline{b}q_2.$$

Quindi $\overline{a} \mid \left(\overline{b}q_2\right)$ con $q_2 \in D$. Poichè $\text{MCD}\,(\overline{a}, \overline{b}) = 1_D$ per il Lemma 1.10, si ottiene che $\overline{a} \mid q_2$ per il Corollario 2.7. Posto $q_2 = \overline{a}q$, si conclude $c = bq_2 = b\overline{a}q = mq$, ossia $m|c$. ■

3 Fattorialità dei dominii euclidei

(3.1) Lemma *In un dominio euclideo D un elemento p è primo se e solo se è irriducibile.*

Dimostrazione.
Se p è primo, è irriducibile per il Lemma 1.17. Viceversa, supponiamo p irriducibile e dimostriamo che è primo. Siano quindi $a, b \in D$ tali che p divide (ab). Posto $d = \mathrm{MCD}\,(p, a)$, si ha $p = d\overline{p}$ con $d \in D^*$ oppure $\overline{p} \in D^*$, per definizione di elemento irriducibile. Supponiamo $d \in D^*$. Da $p \,|\, (ab)$ e $\mathrm{MCD}\,(p, a) \in D^*$ si ottiene che $p \,|\, b$ per il Corollario 2.7. Supponiamo quindi che $\overline{p} \in D^*$. Allora $p \,|\, d$ e, poichè $d \,|\, a$, si conclude che $p \,|\, a$. ■

(3.2) Teorema *Sia D un dominio euclideo rispetto φ. Allora D è fattoriale.*

Dimostrazione.
Chiamiamo S il sottoinsieme degli elementi non nulli e non unitari di D. Dimostriamo che, per ogni $a \in S$, valgono (1.19) e (1.20) ragionando per induzione su $\varphi(a)$.
Se D è un campo, $S = \emptyset$ e non c'è nulla da dimostrare. Altrimenti $S \neq \emptyset$ ed esiste il minimo valore n_0, assunto da φ in S. Se $\varphi(a) = n_0$, allora a è irriducibile. Infatti da $a = bc$, con $b \in D \setminus D^*$, $c \in D \setminus D^*$, seguirebbe che $b \in S$ e che $\varphi(b) < \varphi(a)$ per il Lemma 2.4, in contrasto con $\varphi(a) = n_0$.
Caso 1 a irriducibile (in particolare $\varphi(a) = n_0$).
In tal caso vale la (1.19) con $a = p_1$, $n = 1$. Inoltre $p_1 = q_1(\cdots q_m)$ come in (1.20), implica $m = 1$. Infatti, se fosse $m > 1$, uno dei fattori irriducibili q_j dovrebbe appartenere a D^*, per l' irriducibilità di p_1. Ma $q_j \notin D^*$, per definizione di elemento irriducibile.
Caso 2 a riducibile.
Detta $a = bc$ una fattorizzazione non banale di a (ossia $b \in D \setminus D^*$, $c \in D \setminus D^*$), segue da 2.4 che $\varphi(b) < \varphi(a)$ e che $\varphi(c) < \varphi(a)$. Per induzione $b = p_1 \cdots p_k$, $c = p_{k+1} \cdots p_n$ dove i fattori p_j sono irriducibili in D. Ne segue che $a = p_1 \cdots p_n$ soddisfa (1.19).
Supponiamo ora che sia $a = p_1 \cdots p_n = q_1 \cdots q_m$ come in (1.20). Chiaramente p_1 divide il prodotto $(q_1 \ldots q_m)$. Essendo irriducibile, è anche primo. Pertanto p_1 divide almeno uno dei fattori q_j. Dopo un eventuale riordinamento, possiamo supporre $q_1 = p_1\lambda_1$, con $\lambda_1 \in D^*$ (essendo anche q_1 irriducibile). Sostituendo in (1.20) e semplificando per p_1:

$$p_2 \cdots p_n = (\lambda_1 q_2) \cdots q_m.$$

Notiamo che $\varphi(p_2 \dots p_n) < \varphi(p_1 p_2 \dots p_n)$ per il Lemma 2.4. Inoltre $\lambda_1 q_2$ è irriducibile. Applicando l'ipotesi induttiva a si ha quindi $n-1 = m-1$, da cui $n = m$ e

$$\begin{cases} \lambda_1 q_2 = \mu_2 p_2 \\ q_3 = \lambda_3 p_3 \\ \dots \\ q_n = \lambda_n p_n \end{cases} \qquad \mu_2,\ \lambda_3,\ \dots,\ \lambda_n \in D^*.$$

Notando che $q_2 = \left(\mu_2^{-1}\lambda_1\right) p_2$ e che $\mu_2^{-1}\lambda_1 := \lambda_2 \in D^*$, la dimostrazione è completa. ■

In particolare $\mathbb{Z}$ e $\mathbb{K}[x]$ sono dominii fattoriali. Nel caso di $\mathbb{Z}$ il precedente risultato si chiama il *Teorema fondamentale dell'aritmetica.*

4 Fattorizzazioni di polinomi e radici

(4.1) Lemma *Sia* $f(x) \in \mathbb{K}[x]$.

1) *Se* $\deg f(x) = 1$, *allora* $f(x)$ *è irriducibile in* $\mathbb{K}[x]$ *e ha una radice in* $\mathbb{K}$;

2) *se* $\deg f(x) \geq 2$ *e* $f(x)$ *ha una radice* $\alpha \in \mathbb{K}$, *allora* $f(x)$ *è riducibile in* $\mathbb{K}[x]$;

3) *se* $\deg f(x) \in \{2, 3\}$, *e* $f(x)$ *non ha radici in* $\mathbb{K}$, *allora è irriducibile in* $\mathbb{K}[x]$.

Dimostrazione.
1) Sia $f(x) = a(x)b(x)$ una fattorizzazione di $f(x)$ in $\mathbb{K}[x]$, dove possiamo supporre $\deg a(x) \geq \deg b(x)$. Da $1 = \deg f(x) = \deg a(x) + \deg b(x)$ segue $\deg a(x) = 1$, $\deg b(x) = 0$. Ne segue che $b(x)$ è invertibile. Pertanto $f(x)$ è irriducibile. Posto $f(x) = k_0 + k_1 x$ l'elemento $-k_0 k_1^{-1} \in \mathbb{K}$ è radice di $f(x)$.
2) Per il Teorema di Ruffini, $f(x)$ è divisibile per $x - \alpha$. Pertanto $f(x) = (x-\alpha)q(x)$, con $q(x) \in \mathbb{K}[x]$. E tale fattorizzazione è non banale, dato che $\deg(x-\alpha) = 1$ e $\deg q(x) = \deg f(x) - 1 \geq 1$.
3) Se $f(x)$ fosse riducibile in $\mathbb{K}[x]$, ammetterebbe una fattorizzazione $f(x) = a(x)\, b(x)$ con $a(x),\ b(x) \in \mathbb{K}[x]$ tali che $1 \leq \deg a(x) \leq \deg b(x)$. La condizione

$$\deg a(x) + \deg b(x) = \deg f(x) \leq 3$$

implica $\deg a(x) = 1$. Per il punto 1), $a(x)$ ha una radice $\alpha \in \mathbb{K}$. Da $f(\alpha) = a(\alpha)\, b(\alpha) = 0_K\, b(\alpha) = 0_K$, si ha che α è radice di $f(x)$, in contrasto con l'ipotesi. ■

(4.2) Definizione *Sia* $r \in \mathbb{N}$. *Un elemento* $\alpha \in \mathbb{K}$ *è* radice *di* $f(x)$ *di molteplicità* r *se* $(x-\alpha)^r$ *divide* $f(x)$, *ma* $(x-\alpha)^{r+1}$ *non divide* $f(x)$.

(4.3) Teorema *Sia* $\underline{0} \neq f(x) \in \mathbb{K}[x]$. *La somma delle molteplicità delle radici di* $f(x)$ *non supera* $\deg f(x)$.

Dimostrazione. Se $f(x)$ non ha radici in $\mathbb{K}$, la somma delle molteplicità delle sue radici è $0 \leq \deg f(x)$. Altrimenti siano $\alpha_1, \ \ldots, \ \alpha_k$ le radici distinte di $f(x)$ in $\mathbb{K}$, con rispettive molteplicità $r_1, \ \ldots, \ r_k$. Per definizione $(x-\alpha_j)^{r_j} \mid f(x)$, per ogni $j = 1, \ldots, k$. Detto $m(x)$ il minimo comune multiplo di $(x-\alpha_1)^{r_1}, \ldots, (x-\alpha_k)^{r_k}$ si ha che $m(x) \mid f(x)$ per definizione di mcm. Essendo $x - \alpha_i$ irriducibile, dal teorema di fattorizzazione unica segue che gli unici divisori di $(x-\alpha_i)^{r_i}$ sono della forma $\lambda\,(x-\alpha_i)^r$ con $r \leq r_i$. Se ne deduce che i polinomi $(x-\alpha_1)^{r_1}, \ \cdots, \ (x-\alpha_k)^{r_k}$ sono a due a due coprimi. Pertanto:

$$m(x) = \prod_{j=1}^{k} (x-\alpha_j)^{r_j} \ = \ (x-\alpha_1)^{r_1} \cdots (x-\alpha_k)^{r_k}\,.$$

Da $m(x)$ divide $f(x)$ abbiamo $f(x) = m(x)q(x)$. Concludiamo:

$$\deg f(x) \ = \ \deg m(x) + \deg q(x) \ \geq \ \deg m(x) \ = \ r_1 + \ \ldots \ + r_k.$$

■

(4.4) Definizione *Un campo* $\mathbb{K}$ *si dice* algebricamente chiuso *se, per ogni polinomio non nullo* $f(x) \in \mathbb{K}[x]$, *la somma delle molteplicità delle sue radici è uguale a* $\deg f(x)$.

In altre parole $\mathbb{K}$ è algebricamente chiuso se ogni $f(x) \in \mathbb{K}[x]$, di grado ≥ 1, si scrive come prodotto di polinomi di grado 1, ossia nella forma

$$f(x) = (x-\alpha_1)^{r_1} \cdots (x-\alpha_m)^{r_m}$$

con $\alpha_i \in \mathbb{K}$. Equivalentemente $\mathbb{K}$ è algebricamente chiuso se gli unici polinomi irriducibili di $\mathbb{K}[x]$ sono quelli di grado 1.

(4.5) Teorema (fondamentale dell'algebra) *Il campo complesso* $\mathbb{C}$ *è algebricamente chiuso.*

Esistono varie dimostrazioni di questo importante risultato. Di solito almeno una di queste è presentata nei corsi di Analisi Matematica.
Il campo reale $\mathbb{R}$ non è algebricamente chiuso. Per esempio $x^2 + 1$ non ha radici in $\mathbb{R}$. Infatti, per ogni $\alpha \in \mathbb{R}$, si ha $\alpha^2 \geq 0$ da cui $\alpha^2 + 1 \geq 1$. Come conseguenza del Teorema fondamentale dell'algebra, vale tuttavia il risultato espresso dal Corollario 4.7, la cui dimostrazione utilizza l'automorfismo $\alpha \mapsto \overline{\alpha}$ di $\mathbb{C}$.

(4.6) Definizione *Per ogni* $\alpha \in \mathbb{C}$ *il suo* complesso coniugato $\overline{\alpha}$ *è così definito. Se* $\alpha = a + ib$ *con* $a, b \in \mathbb{R}$, $i^2 = -1$, *si ha*

$$\overline{\alpha} := a - ib.$$

È facile verificare le seguenti proprietà : per ogni $\alpha, \beta \in \mathbb{C}$:

1) $\overline{\alpha} = \alpha \iff \alpha \in \mathbb{R}$;

2) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$

3) $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.

4) $\alpha + \overline{\alpha} \in \mathbb{R}$, $\alpha\overline{\alpha} \in \mathbb{R}$.

(4.7) Corollario *Ogni polinomio* $f(x) \in \mathbb{R}[x]$, *di grado* ≥ 3, *è riducibile in* $\mathbb{R}[x]$.

Dimostrazione. Sia α una radice di $f(x)$ in $\mathbb{C}$.
Se $\alpha \in \mathbb{R}$, $f(x)$ è riducibile per il punto 2) del Lemma 4.1.
Se $\alpha \notin \mathbb{R}$, allora anche $\overline{\alpha} \neq \alpha$ è radice di $f(x)$. Infatti, posto $f(x) = \sum_{j=0}^{n} r_j\, x^j$,
da $r_j \in \mathbb{R}$ per ogni $j \geq 0$, e da $0 = f(\alpha) = \sum_{j=0}^{n} r_j\, \alpha^j$ segue:

$$0 \;=\; \overline{r_0 + r_1\alpha + \cdots + r_n\alpha^n} \;=\; r_0 + r_1\overline{\alpha} + \ldots r_n\overline{\alpha}^n.$$

Pertanto $f(x)$ è divisibile per

$$(x - \alpha)(x - \overline{\alpha}) \;=\; x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} \;\in \mathbb{R}[x].$$

Di nuovo $f(x)$ è riducibile. ■

In contrasto con il precedente risultato, in $\mathbb{Q}[x]$ ci sono polinomi irriducibili di qualsiasi grado $n \geq 1$. Ad esempio, per ogni primo p, il polinomio $x^n - p$ è irriducibile in $\mathbb{Q}[x]$. Vale infatti il seguente:

(4.8) Teorema (Criterio di Eisenstein) *Dato* $f(x) = z_0 + z_1x + \ldots z_nx^n \in \mathbb{Z}[x]$ *di grado* $n \geq 1$, *si supponga che sia* $\mathrm{MCD}\,(z_0, z_1, \ldots, z_n) = 1$ *e che esista un primo* p *tale che:*

$$p \mid z_j,\ 0 \leq j \leq n-1, \quad p^2 \not| z_0.$$

Allora $f(x)$ *è irriducibile in* $\mathbb{Q}[x]$.

5 Equazioni diofantee

(5.1) Definizione *Dati $a, b, c \in D$, consideriamo l' equazione diofantea*

$$ax + by = c. \tag{5.2}$$

Si dice soluzione della (5.2) *ogni coppia ordinata $(x_0, y_0) \in D^2$ tale che $ax_0 + by_0 = c$.*

(5.3) Teorema *In un dominio euclideo D, l'equazione diofantea* (5.2) *ha soluzioni se e solo se $d := \mathrm{MCD}\,(a, b)$ divide c. Inoltre, se $(x_0, y_0) \in D^2$ è una soluzione, tutte e sole le altre soluzioni sono quelle della forma:*

$$\big(x_0 + \overline{b}k,\ y_0 - \overline{a}k\big) \quad \text{con } k \in D. \tag{5.4}$$

Dimostrazione.
Supponiamo che (5.2) abbia una soluzione $(x_0, y_0) \in D^2$. Poiché $d \,|\, a$ e $d \,|\, b$ si ha che $d \,|\, (ax_0 + by_0) = c$. Viceversa supponiamo che $d \,|\, c$. Siano $\overline{x},\ \overline{y} \in D$ tali che

$$\overline{x}a + \overline{y}b = d$$

e sia $\overline{c} \in D$ tale che $c = d\overline{c}$. Moltiplicando la precedente relazione per $\overline{c}$ si ha:

$$(\overline{c}\,\overline{x})a + (\overline{c}\,\overline{y})b = \overline{c}\,d = c.$$

Posto $x_0 := \overline{c}\,\overline{x}$, $y_0 := \overline{c}\,\overline{y}$ si conclude che $(x_0, y_0) \in D^2$ è una soluzione di (5.2).
Studiamo ora le altre soluzioni. Da $ax_0 + by_0 = c$ segue subito che, per ogni $k \in D$,

$$a(x_0 + \overline{b}k) + b(y_0 - \overline{a}k) = c.$$

Quindi tutte le coppie in (5.4) sono soluzioni. Infine sia $(x_1,\ y_1) \in D^2$ una soluzione. Ne segue $a(x_1 - x_0) = b(y_0 - y_1)$ da cui, nelle notazioni del Lemma 1.10:

$$d\overline{a}(x_1 - x_0) = d\overline{b}(y_0 - y_1). \tag{5.5}$$

Semplificando per d e tenendo conto che $\mathrm{MCD}\,(\overline{a}, \overline{b}) = 1$ si ha che esistono $h, k \in D$ tali che $y_0 - y_1 = \overline{a}h$ e $x_1 - x_0 = \overline{b}k$. Infine, sostituendo tali valori di $y_0 - y_1$ e $x_1 - x_0$ in (5.5) si ottiene $k = h$. Si conclude $x_1 = x_0 + \overline{b}k$, $y_1 = y_0 - \overline{a}k$. ■

(5.6) Corollario *Per ogni primo p l'anello $\mathbb{Z}_p$ delle classi di resti modulo p é un campo.*

Dimostrazione. Dobbiamo verificare che ogni classe $[a]_p \in \mathbb{Z}_p$ diversa dalla classe nulla ha inversa. Ora $[a]_p \neq [0]_p$ implica che p non divide a. Essendo p primo si ha allora $\mathrm{MCD}(a,p) = 1$. Ne segue che l'equazione diofantea $ax + py = 1$ ha soluzione, ossia esistono $b, c \in \mathbb{Z}$ tali che $ab+pc = 1$. In particolare $ab \equiv 1 \pmod{p}$, da cui $[a]_p[b]_p = [1]_p$. Si conclude che $[b]_p = [a]_p^{-1}$. ■

(5.7) Teorema *(di Fermat) Siano a un intero, p un primo. Si ha:*

1) *se p non divide a, allora $a^{p-1} \equiv 1 \pmod{p}$;*

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

Dimostrazione.
1) Il gruppo moltiplicativo $\mathbb{Z}_p{}^*$ degli elementi non nulli del campo $\mathbb{Z}_p$ ha ordine $p-1$. Per il Teorema di Lagrange ogni suo elemento $[a]_p$ ha periodo un divisore $m = m(a)$ di $p-1$. Posto $p-1 = mq$, $q \in \mathbb{Z}$, si ha:

$$([a]_p)^{p-1} = ([a]_p)^{mq} = ([a]_p)^m)^q = ([1]_p)^q = [1]_p.$$

Si conclude $a^{p-1} \equiv 1 \pmod{p}$.
2) Se p non divide a, da $a^{p-1} \equiv 1 \pmod{p}$ si ottiene, moltiplicando per a, $a^p \equiv a \pmod{p}$. Se p divide a, a maggior ragione p divide a^p, quindi $a^p \equiv 0 \pmod{p}$ e $a \equiv 0 \pmod{p}$. ■

Bibliografia

[1] L. Childs, Algebra , Traduzione di C.Traverso, ETS Editrice, 1983.

[2] B.Hartley, T.O.Hawkes, Rings, Modules and Linear Algebra, Chapman and Hall, 1970.

[3] N.Jacobson, Basic Algebra I, W.H.Freeman and company, San Francisco,1974.

[4] S.Lang, Undergraduate Algebra, Second Edition, Springer, 1990.

[5] M.Chiara Tamburini, Appunti di Algebra, Pubblicazioni ISU, 1990.

Elenco dei simboli

Indice analitico