

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 $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Esempi 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

$$S \times S \rightarrow S$$

avente dominio $S \times S$ e codominio S . Una tale operazione può essere denotata con uno dei simboli $*$, oppure $+$, oppure \cdot , oppure con altri simboli; nel primo caso, scriveremo che essa associa ad una coppia (a, b) l'elemento $a * b$ di S .

Il termine “applicazione” è sinonimo di “funzione”. Un altro termine usato a volte con lo stesso significato è “mappa”.

Esempi 1.1.4. Esempi di operazioni interne.

(i) $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, la somma è un'operazione interna in \mathbb{Z} ;

$(a, b) \rightarrow a + b$; per esempio

$(1, 2) \rightarrow 1 + 2 = 3$.

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

$(x, y) \rightarrow x \cdot y$; per esempio

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

(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 $id_X : X \rightarrow X$, definita da $id_X(x) = x$ per ogni $x \in X$.

Possiamo definire un'operazione interna in F , data dalla *composizione di applicazioni* $\circ : F \times F \rightarrow F$, data da $(f, g) \rightarrow f \circ g$, 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 interna 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 $e * a = a * e = a$; l'elemento e è detto elemento neutro di G ;

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

Se l'operazione è indicata additivamente, ossia con il simbolo $+$, l'elemento neutro è detto "zero" e indicato con il simbolo 0 , mentre il reciproco di a è detto opposto di a e indicato con $-a$.

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

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

Esempi 1.2.3.

1. $(\mathbb{Z}, +)$ è un gruppo abeliano.
2. (\mathbb{Z}, \cdot) non è un gruppo: la proprietà associativa è soddisfatta, 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 non è invertibile in \mathbb{Z} , in quanto si ha $2 \cdot z \neq 1$ per ogni $z \in \mathbb{Z}$.

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. Inoltre, vale la proprietà associativa, l'elemento neutro è l'1, e per ogni $q \in \mathbb{Q} \setminus \{0\}$ esiste $q^{-1} = \frac{1}{q}$ che verifica $q \cdot \frac{1}{q} = \frac{1}{q} \cdot q = 1$.

5. Sia $X \neq \emptyset$ un insieme e sia $B(X) = \{f : X \rightarrow X \mid f \text{ biettiva}\}$ l'insieme delle applicazioni biettive di X in sè; date $f, g \in B(X)$, denotiamo con $f \circ g$ la funzione composta.

Si ha che $(B(X), \circ)$ è un gruppo. Infatti:

- (i) se $f, g : X \rightarrow X$ sono biettive, anche $f \circ g$ lo è, dunque la composizione è un'operazione interna in $B(X)$;
- (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 $id_X : x \rightarrow x$, per ogni $x \in X$, è l'elemento neutro di $B(X)$;
- (iv) ricordiamo che un'applicazione è biettiva se e solo se esiste l'applicazione inversa $f^{-1} : X \rightarrow X$, che verifica

$$f(x) = y \iff f^{-1}(y) = x.$$

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 $B(X)$ non è abeliano se X ha almeno tre elementi.

Per esempio, sia $X = \{1, 2, 3\}$. Consideriamo $f : X \rightarrow X$ data da

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

e $g : X \rightarrow X$ data da

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

Si ha che $f \circ g \neq g \circ f$, 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 $B(X)$ ha sei elementi, corrispondenti alle permutazioni dell'insieme X ; si veda il Capitolo ??.

Esercizi 1.

1. Costruire un esempio in cui $f \circ g \neq g \circ f$ in modo analogo al precedente, per X insieme di n elementi, con $n \geq 3$ qualunque.

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

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

1. l'elemento neutro in G è unico;
2. ogni elemento $g \in G$ ha un unico reciproco.

Dimostrazione. 1. Supponiamo che e, e' siano 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 gli appunti del corso propedeutico.

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:

Definizione 1.3.1. 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 1.3.2 (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 $x \sim z$.

Esempi 1.3.3.

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: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Definizione 1.3.4 (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:

$$x \equiv y \pmod{n} \iff \exists k \in \mathbb{Z} : x - y = kn.$$

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

Proposizione 1.3.5. *La relazione di congruenza modulo n è una relazione d'equivalenza in \mathbb{Z} .*

Dimostrazione. Verifichiamo che sono soddisfatte le tre proprietà richieste:

1. simmetria: $x - x = 0x$ per ogni $x \in \mathbb{Z}$.
2. riflessività: se $x \equiv_n y$, si ha $x - y = kn$ per un opportuno $k \in \mathbb{Z}$. Allora $y - x = (-k)n$.
3. transitività: 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 $x \equiv_n z$. \square

D'ora in poi supporremo sempre $n \geq 2$.

Proposizione 1.3.6. *$x \equiv_n y$ 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 $0 \leq r \leq n - 1$. Quindi $x - y = (qn + r) - (q'n + r) = (q - q')n$ 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 anche $y = qn + r$ 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 . \square

Definizione 1.3.7 (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 dell'insieme $\mathcal{P}(X)$ delle parti di X , cioè l'insieme di tutti i sottoinsiemi di 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 1.3.8 (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 P_i o sono disgiunti o sono uguali.

Proposizione 1.3.9. *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. \square

Esempi 1.3.10.

1. L'insieme quoziente \mathbb{Z}/\equiv_n si denota \mathbb{Z}_n . Affermiamo che tale insieme ha n elementi, uno per ciascuno degli n possibili resti della divisione per n : $0, 1, 2, \dots, n-1$.

Infatti, se x ha resto r nella divisione per n , $x = qn + r$ dunque $x \equiv_n r$. Inoltre, è immediato verificare che le classi $[r]$ per $0 \leq r \leq n-1$ sono a due a due distinte.

Gli elementi di \mathbb{Z}_n si denotano anche $[r]_n$ o \bar{r} . Dunque $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.

Un insieme S si dice **finito** se esiste un numero naturale n tale che S è in biiezione con l'insieme $\{1, 2, 3, \dots, n-1, n\}$. 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

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}.$$

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 per il prodotto;
3. proprietà commutativa: $\bar{x}\bar{y} = \bar{y}\bar{x}$;
4. proprietà distributiva: $(\bar{x} + \bar{y})\bar{z} = \bar{x}\bar{z} + \bar{y}\bar{z}$.

1.5 Campi

Definizione 1.5.1 (Campo). Sia K un insieme dotato di due operazioni, chiamate somma e prodotto e denotate con $+$ 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:
 $(a + b) \cdot c = ac + bc$.

Esempi 1.5.2.

1. Campi numerici: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,
2. $(\mathbb{Z}, +, \cdot)$ non è un campo perché 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 $a + (-1) \cdot a = 0$. \square

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:

$$a - b = a + (-b)$$

$$ab = a \cdot b$$

$$\frac{a}{b} = a/b = ab^{-1}: \text{ quest'ultima notazione ha senso perché il prodotto è commutativo.}$$

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.

$n = 2$

·	1
1	1

$n = 3$

·	1	2
1	1	2
2	2	1

$n = 4$

·	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$n = 5$

·	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 $f : X \rightarrow X$ 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 $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ 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 $\bar{a}\bar{x} = \bar{a}\bar{y}$, 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 \mathbb{Z}_n .

□

Esercizi 2.

1. 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} .