

Capitolo 1

Richiami di teoria

1.1 Nozioni fondamentali

1.1.1 Gli insiemi

Il concetto di *insieme* è una nozione primitiva; non tenteremo di definirla e non presenteremo una trattazione assiomatica della teoria degli insiemi. Da un punto di vista ingenuo, che noi adoteremo, un insieme è una collezione di oggetti, i suoi elementi. L'unica proprietà di un insieme X è la possibilità di decidere se un elemento x è o meno appartenente all'insieme X : nel primo caso scriveremo $x \in X$ e diremo che x *appartiene* all'insieme X , se invece x non è un elemento di X scriveremo $x \notin X$, da leggersi x *non appartiene* ad X . In particolare due insiemi X e Y sono *uguali* se e solo se contengono gli stessi elementi. Vi è un solo insieme che non contiene alcun elemento, l'*insieme vuoto*, indicato con \emptyset .

Un insieme X è un *sottoinsieme* di un insieme Y se ogni elemento di X è un elemento di Y , in tale caso scriviamo $X \subseteq Y$; con $X \not\subseteq Y$ intendiamo invece che X non è un sottoinsieme di Y . L'insieme vuoto è un sottoinsieme di ogni insieme X , in simboli $\emptyset \subseteq X$, e ovviamente vale anche $X \subseteq X$. La famiglia di tutti i sottoinsiemi di X si indica con $\mathcal{P}(X)$ ed è detta *insieme delle parti* di X ; due particolari elementi di $\mathcal{P}(X)$ sono quindi \emptyset e X stesso.

Spesso un sottoinsieme X di un insieme Y è definito per mezzo di una proprietà p ; scriveremo

$$X \doteq \{y \in Y \mid p(y)\}$$

per indicare che X è l'insieme di tutti gli elementi di Y per cui la proprietà p è vera.

L'*unione* $X \cup Y$ dei due insiemi X e Y è l'insieme i cui elementi sono tutti e soli gli elementi che appartengono ad X o ad Y : abbiamo cioè

$$x \in X \cup Y \quad \text{se e solo se} \quad x \in X \text{ oppure } x \in Y.$$

Si noti che, a differenza dell'uso nel linguaggio comune della congiunzione “oppure” un elemento dell'unione può appartenere ad entrambi gli insiemi X e Y ; l'alternativa è da intendersi quindi nel senso della congiunzione latina *vel*.

L'intersezione $X \cap Y$ è l'insieme che ha per elementi gli elementi che appartengono ad X e ad Y

$$x \in X \cap Y \quad \text{se e solo se} \quad x \in X \text{ e } x \in Y.$$

L'unione e l'intersezione si possono definire per un numero qualsiasi di insiemi: se \mathcal{F} è una famiglia di insiemi allora

$$x \in \bigcup_{X \in \mathcal{F}} X \quad \text{se e solo se} \quad \text{esiste } X \text{ in } \mathcal{F} \text{ per cui } x \in X$$

e allo stesso modo

$$x \in \bigcap_{X \in \mathcal{F}} X \quad \text{se e solo} \quad \text{per ogni } X \text{ in } \mathcal{F} \text{ si ha } x \in X.$$

Proposizione 1.1 *L'unione e l'intersezione sono distributive una rispetto all'altra: se X, Y e Z sono tre insiemi allora*

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \quad \text{e} \quad X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Due insiemi X, Y che non hanno alcun elemento in comune, cioè tali che $X \cap Y = \emptyset$, si dicono *disgiunti*. Ogni sottoinsieme X di Y è disgiunto dal suo *complementare* $Y \setminus X$ definito come l'insieme degli elementi di Y che non sono in X . Se X e Y sono insiemi disgiunti allora a volte scriviamo $X \sqcup Y$ per l'unione di X e Y e diciamo che l'unione è *disgiunta*.

Le operazioni sugli insiemi hanno un diretto legame con le operazioni logiche sulle proposizioni come chiarito dalla seguente

Proposizione 1.2 *Se $X = \{z \in Z \mid p(z)\}$ e $Y = \{z \in Z \mid q(z)\}$ sono sottoinsiemi di Z allora*

- (i) $X \cup Y = \{z \in Z \mid p(z) \text{ o } q(z)\},$
- (ii) $X \cap Y = \{z \in Z \mid p(z) \text{ e } q(z)\},$
- (iii) $Z \setminus X = \{z \in Z \mid \text{non } p(z)\},$
- (iv) $X \subseteq Y$ se e solo se p implica q .

Proposizione 1.3 *Se X e Y sono sottoinsiemi di un insieme Z allora valgono le Leggi di de Morgan*

$$Z \setminus (X \cup Y) = (Z \setminus X) \cap (Z \setminus Y) \quad \text{e} \quad Z \setminus (X \cap Y) = (Z \setminus X) \cup (Z \setminus Y);$$

cioè il passaggio al complementare scambia l'unione con l'intersezione.

L'insieme delle coppie di elementi (x, y) con x in X e y in Y si indica con $X \times Y$ e si chiama *prodotto cartesiano* di X e Y . La stessa costruzione è possibile con un numero qualsiasi di insiemi: $X_1 \times X_2 \times \cdots \times X_n$ è l'insieme delle n -uple ordinate (x_1, x_2, \dots, x_n) con $x_1 \in X_1, x_2 \in X_2, \dots, x_n \in X_n$. Indichiamo, per brevità, con X^n il prodotto cartesiano di X con se stesso n volte.

1.1.2 Le applicazioni

Un'applicazione da X in Y è una legge che ad ogni elemento di X associa uno e un solo elemento di Y . Ciò può essere formalizzato definendo un'applicazione f da X in Y come un sottoinsieme del prodotto cartesiano $X \times Y$ con la proprietà che per ogni $x \in X$ esiste un unico $y \in Y$ con $(x, y) \in f$; l'insieme X è detto il *dominio* di f e Y è il *codominio* di f . Per indicare che $f \subseteq X \times Y$ è un'applicazione da X in Y scriveremo $f: X \longrightarrow Y$ o anche $X \xrightarrow{f} Y$ e useremo sempre la notazione funzionale scrivendo $f(x) = y$ o $f: x \longmapsto y$ o anche $x \xrightarrow{f} y$ invece di $(x, y) \in f$.

Se $f(x) = y$ allora diremo indifferentemente che y è l'*immagine* di x , che f manda x in y , che ad x corrisponde y e che y viene raggiunto da x tramite f . Il sottoinsieme $\text{Im}(f) = \{f(x) \mid x \in X\} \subseteq Y$ degli elementi di Y raggiunti da qualche elemento x di X tramite f è detto *immagine* di f . Osserviamo che dalla definizione segue che due applicazioni f e g sono uguali se hanno lo stesso dominio e codominio e se $f(x) = g(x)$ per ogni x nel dominio.

Se A è un sottoinsieme di X allora $f(A)$, l'*immagine* di A tramite f , è l'insieme degli elementi $f(a)$ al variare di a in A . Se invece B è un sottoinsieme di Y allora $f^{-1}(B)$, la *controimmagine* di B tramite f , è l'insieme degli x in X tali che $f(x) \in B$. L'immagine e la controimmagine godono di alcune compatibilità con l'unione e l'intersezione come chiarito dalla seguente

Proposizione 1.4 *La controimmagine commuta con l'unione e intersezione*

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), \quad f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$$

mentre l'immagine commuta solo con l'unione

$$f(A \cup B) = f(A) \cup f(B)$$

e vale

$$f(A \cap B) \subseteq f(A) \cap f(B).$$

In generale, però, $f(A \cap B)$ può essere un sottoinsieme proprio di $f(A) \cap f(B)$.

Se $X \xrightarrow{f} Y$ e $Y \xrightarrow{g} Z$ sono due applicazioni, l'applicazione *composta* $g \circ f$ è definita come

$$X \ni x \xrightarrow{g \circ f} g(f(x)) \in Z.$$

Proposizione 1.5 *Per la composizione vale la legge associativa: se f , g e h sono applicazioni per cui sono definite le composizioni $g \circ f$ e $h \circ g$ allora $h \circ (g \circ f) = (h \circ g) \circ f$.*

Un'applicazione per cui elementi distinti di X corrispondono ad elementi distinti di Y è detta *iniettiva*. Per evidenziare che un'applicazione è iniettiva si scrive

$X \hookrightarrow Y$. Un'applicazione per cui ogni y di Y è raggiunto viene detta *suriettiva*; equivalentemente f è suriettiva se $\text{Im}(f) = Y$. Un'applicazione suriettiva si indica con $X \twoheadrightarrow Y$. Se f è iniettiva e suriettiva allora diremo che f è *biiettiva*, ciò è indicato a volte con $f : X \xrightarrow{\sim} Y$.

Proposizione 1.6 *La composizione di applicazioni iniettive è iniettiva e la composizione di applicazioni suriettive è suriettiva. In particolare, la composizione di applicazioni biiettive è biiettiva.*

Se X è un sottoinsieme di Y allora è definita l'applicazione *inclusione* $X \ni x \xrightarrow{i_X} x \in Y$; si tratta chiaramente di un'applicazione iniettiva. In particolare l'inclusione di X in X è detta *identità* e si indica con Id_X , o semplicemente Id quando non vi è ambiguità; essa è un'applicazione biiettiva.

Se X è un sottoinsieme di Y e f è un'applicazione da Y nell'insieme Z , si chiama *restrizione* di f ad X l'applicazione $X \ni x \xrightarrow{f|_X} f(x) \in Z$; chiaramente si ha $f|_X = f \circ i_X$.

Se f è un'applicazione da X in Y allora un'*inversa* per f è un'applicazione $Y \xrightarrow{g} X$ tale che $g \circ f = \text{Id}_X$ e $f \circ g = \text{Id}_Y$. Un'applicazione per cui esiste un'inversa è detta *invertibile*. Non tutte le applicazioni ammettono inversa, abbiamo infatti

Proposizione 1.7 *Un'applicazione è invertibile se e solo se è biiettiva. Inoltre, se un'applicazione è invertibile essa ammette un'unica inversa.*

Per un'applicazione invertibile possiamo quindi definire f^{-1} come l'unica inversa di f .

Se $X \xrightarrow{f} X$ è un'applicazione di X in sé indichiamo con X^f l'insieme dei *punti fissi* per f , cioè $X^f = \{x \in X \mid f(x) = x\}$; useremo anche la notazione $\text{Fix}(f)$ per l'insieme dei punti fissi.

Un'applicazione biiettiva di un insieme X in sé è detta *permutazione* e l'insieme di tutte le permutazioni di X è indicato con $S(X)$. Tale insieme avrà una notevole importanza per il nostro studio dell'Algebra. In generale, l'insieme di tutte le applicazioni $X \longrightarrow Y$ è indicato con Y^X .

Un diagramma di insiemi e applicazioni è detto *commutativo* se tutti i cammini con la stessa partenza e arrivo danno il medesimo risultato per composizione. Ad esempio, il seguente diagramma

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ g \downarrow & & \downarrow h \\ A & \xrightarrow{i} & B \end{array}$$

è commutativo se e solo se $(h \circ f)x = (i \circ g)x$ per ogni elemento x in X .

1.1.3 Le relazioni

Sia X un insieme e R un sottoinsieme del prodotto cartesiano $X \times X$, ad R è associata la *relazione* \sim_R , o semplicemente \sim se non vi è ambiguità, su X definita come: $x \sim_R y$ se e solo se $(x, y) \in R$. Di fondamentale importanza sono le relazioni di equivalenza: una relazione \sim è di *equivalenza* se valgono le seguenti tre proprietà

- (i) proprietà riflessiva: $x \sim x$ per ogni $x \in X$,
- (ii) proprietà simmetrica: se $x \sim y$ allora $y \sim x$,
- (iii) proprietà transitiva: se $x \sim y$ e $y \sim z$ allora $x \sim z$.

Si osservi che la relazione di uguaglianza è una relazione di equivalenza; può essere utile pensare intuitivamente le relazioni di equivalenza come delle versioni “deboli” dell’uguaglianza. Dato un elemento $x \in X$ si chiama *classe di equivalenza* di x l’insieme $\mathcal{C}\ell(x)$ di tutti gli elementi $y \in X$ con $x \sim y$. Due distinte classi di equivalenza non si intersecano e l’unione di tutte le classi di equivalenza è tutto l’insieme X .

Introduciamo ora un nuovo linguaggio strettamente legato alle relazioni. Una *partizione* di un insieme X è una famiglia \mathcal{P} di sottoinsiemi non vuoti di X con le seguenti proprietà

- (i) due distinti insiemi di \mathcal{P} sono disgiunti,
- (ii) l’unione di tutti i sottoinsiemi di \mathcal{P} è X .

Vi è una perfetta corrispondenza tra relazioni di equivalenza e partizioni come chiarito dal seguente

Teorema 1.8 *Se \sim è una relazione di equivalenza su X allora la famiglia delle classi di equivalenza per \sim è una partizione di X . Viceversa se \mathcal{P} è una partizione di X allora la relazione definita da*

$$x \sim y \quad \text{se e solo se} \quad \text{esiste } C \in \mathcal{P} \text{ con } x, y \in C$$

è una relazione di equivalenza su X ; inoltre \sim ha per classi di equivalenza gli insiemi C della partizione \mathcal{P} .

La famiglia delle classi di equivalenza per una relazione è detta *insieme quoziente*, indicato con X/\sim , inoltre, l’applicazione

$$X \ni x \mapsto \mathcal{C}\ell(x) \in X/\sim$$

che ad un elemento x associa la sua classe di equivalenza è detta *proiezione al quoziente*.

Un’applicazione $X \xrightarrow{f} Y$ è *compatibile* con la relazione di equivalenza \sim su X se $f(x) = f(y)$ ogni volta che $x \sim y$. Se così è, esiste ed è unica un’applicazione \overline{f}

per cui $f = \overline{f}\pi$; in altri termini, \overline{f} rende il seguente diagramma

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \pi \downarrow & \nearrow \overline{f} & \\ X/\sim & & \end{array}$$

commutativo. Ciò si esprime anche dicendo che f passa al quoziente. Definiremo a volte direttamente un'applicazione \overline{f} come $\mathcal{Cl}(x) \mapsto f(x)$; in tal caso bisognerà controllare che la definizione sia *ben posta*, cioè che f sia compatibile con \sim .

Se abbiamo due relazioni \sim e \sim' su un insieme X e succede che $x \sim y$ implichi $x \sim' y$ allora la partizione \mathcal{P} indotta da \sim è *più fine* della partizione \mathcal{P}' indotta da \sim' : cioè per ogni classe $C \in \mathcal{P}$ esiste una classe $C' \in \mathcal{P}'$ tale che $C \subseteq C'$. La corrispondenza $C \mapsto C'$ è un'applicazione suriettiva ϵ che rende commutativo il diagramma

$$\begin{array}{ccc} & X & \\ \pi \swarrow & & \searrow \pi' \\ X/\sim & \xrightarrow{\epsilon} & X/\sim' \end{array}$$

Un *insieme di rappresentanti* \mathcal{R} per una relazione di equivalenza è un sottoinsieme di X con la proprietà che la proiezione ristretta ad \mathcal{R} è una biiezione con X/\sim ; abbiamo cioè scelto per ogni classe di equivalenza un rappresentante in X .

Un'altra importante classe di relazioni che useremo spesso è data dalle relazioni d'ordine: una relazione d'ordine su un insieme X è una relazione \leq con le seguenti proprietà

- (i) proprietà riflessiva: $x \leq x$ per ogni $x \in X$,
- (ii) proprietà antisimmetrica: se $x \leq y$ e $y \leq x$ allora $x = y$,
- (iii) proprietà transitiva: se $x \leq y$ e $y \leq z$ allora $x \leq z$.

Si noti che non chiediamo che tutti gli elementi di X siano tra loro confrontabili, può infatti essere che $x \leq y$ e $y \leq x$ siano entrambe false. Se invece per ogni coppia di elementi $x, y \in X$ si ha $x \leq y$ o $y \leq x$ allora la relazione si dice d'ordine *totale*. A volte, per evidenziare che una relazione d'ordine può non essere di ordine totale diremo che è una relazione d'ordine *parziale*.

Una relazione d'ordine *stretto* è invece una relazione $<$ su X che verifica le proprietà

- (i) proprietà irreflessiva: per nessun $x \in X$ si ha $x < x$,
- (ii) proprietà transitiva: se $x < y$ e $y < z$ allora $x < z$.

Ad ogni relazione d'ordine è associata una relazione d'ordine stretto e viceversa. Infatti se \leq è una relazione d'ordine allora definendo $x < y$ se $x \leq y$ e $x \neq y$, abbiamo una relazione d'ordine stretto e, se $<$ è d'ordine stretto allora definendo

$x \leq y$ se $x < y$ o $x = y$, abbiamo una relazione d'ordine. Questa associazione tra \leq e $<$ verrà assunta tacitamente nel seguito.

1.1.4 Il principio di induzione

Indichiamo l'insieme dei numeri naturali $\{0, 1, 2, \dots\}$ con \mathbb{N} ; nel seguito assumeremo note le proprietà elementari dei naturali e non daremo una loro definizione assiomatica. Ricordiamo solo che una possibile definizione formale è quella di Giuseppe Peano di cui riportiamo, data la sua fondamentale importanza, solo il quinto assioma detto *Principio d'Induzione*.

Assioma 1.9 (Principio di Induzione) *Sia $p(n)$ una proprietà dipendente da un naturale n tale che: $p(0)$ è vera e, per ogni naturale m , si ha che $p(m)$ implica $p(m+1)$. Allora $p(n)$ è vera per ogni n .*

Nell'uso del Principio di Induzione la verifica che $p(0)$ è vera è spesso chiamata *passo base* e la dimostrazione che $p(m)$ implica $p(m+1)$ *passo induttivo*. Il Principio di Induzione può essere enunciato in varie forme equivalenti. Ad esempio

Proposizione 1.10 (Seconda forma del Principio di Induzione) *Sia $p(n)$ una proprietà dipendente da un naturale n tale che: $p(0)$ è vera e, per ogni naturale m , si ha che $p(m+1)$ segue da $p(0), p(1), \dots, p(m-1), p(m)$. Allora $p(n)$ è vera per ogni n .*

Con la seconda forma dell'induzione possiamo assumere la verità di $p(0), p(1), \dots, p(m)$ per dimostrare $p(m+1)$ nel passo induttivo.

Un'ulteriore utile forma equivalente è il cosiddetto *Principio del Minimo* o del *Buon Ordinamento*

Proposizione 1.11 (Principio del Minimo) *Se A è un sottoinsieme non vuoto di \mathbb{N} allora A ammette minimo, esiste cioè un elemento $a \in A$ tale che $a \leq b$ per ogni $b \in A$.*

Chiamiamo *successione* in X una applicazione $\mathbb{N} \rightarrow X$, indichiamo una successione con $(a_n)_n$ invece di $n \mapsto a_n$.

Vogliamo definire una successione $(a_n)_n$ in X fissando il valore iniziale $a_0 = x \in X$ e imponendo che per ogni n , il termine a_{n+1} si possa ricavare in qualche modo dai termini precedenti $a_0, a_1, \dots, a_{n-1}, a_n$. Siano quindi $f_n : X^n \rightarrow X$, con $n \geq 1$, delle applicazioni e richiediamo $a_{n+1} = f_{n+1}(a_0, a_1, \dots, a_{n-1}, a_n)$ per ogni n . In questa situazione diciamo che la successione $(a_n)_n$ è definita per *ricorsione*. La fondatezza di tale modo di procedere è un'altra forma equivalente del Principio d'Induzione.

Proposizione 1.12 (Principio di Definizione Ricorsiva) *Sia X un insieme, x un elemento di X e supponiamo data, per ogni $n \in \mathbb{N}$, un'applicazione $f_n : X^n \rightarrow X$. Allora esiste un'unica successione $(a_n)_n$ per cui $a_0 = x$ e $a_{n+1} = f_{n+1}(a_0, a_1, \dots, a_{n-1}, a_n)$ per ogni $n \in \mathbb{N}$.*

Un esempio di definizione ricorsiva è dato dalla successione $(F_n)_n$ dei numeri di Fibonacci: essi sono definiti da $F_0 = 0$, $F_1 = 1$ e, per ogni $n \geq 1$, $F_{n+1} = F_n + F_{n-1}$. I primi elementi di tale successione sono

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

Questa definizione rientra nello schema della proposizione precedente prendendo $X = \mathbb{N}$, $x = 0$, $f_1(a_0) = 1$ e $f_{n+1}(a_0, a_1, a_2, \dots, a_n) = a_{n-1} + a_n$ per ogni $n \geq 1$.

1.1.5 Le operazioni

Il principale oggetto del nostro studio dell'algebra sono gli insiemi su cui possono essere definite, in modo naturale, delle operazioni con determinate proprietà. Un'operazione su un insieme X è un'applicazione dal prodotto cartesiano $X \times X$ in X . Di solito, per le operazioni non usiamo la notazione funzionale ma, indicata, ad esempio, con \circ un'operazione su X , l'immagine attraverso \circ della coppia (x, y) di elementi X è indicata con $x \circ y$; l'operazione stessa è quindi

$$X \times X \ni (x, y) \mapsto x \circ y \in X.$$

Diciamo anche che $x \circ y$ è la *composizione* di x e y mediante l'operazione \circ .

L'operazione \circ è detta *associativa* se $(x \circ y) \circ z = x \circ (y \circ z)$ per ogni $x, y, z \in X$. Dati n elementi x_1, x_2, \dots, x_n di X , se \circ è un'operazione associativa è possibile definire un significato non ambiguo alla composizione $x_1 \circ x_2 \circ \dots \circ x_n$; infatti possiamo associare tra loro a due a due gli elementi in qualsiasi modo senza cambiare il risultato finale.

Un'operazione \circ è detta *commutativa* se $x \circ y = y \circ x$ per ogni $x, y \in X$. Se un'operazione è commutativa e associativa allora la composizione $x_1 \circ x_2 \circ \dots \circ x_n$ non dipende dall'ordine degli elementi.

Un *elemento neutro* e per un'operazione \circ è un elemento di X per cui $e \circ x = x \circ e = x$ per ogni $x \in X$. È facile provare che se un elemento neutro esiste allora esso è unico.

Se un'operazione \circ ammette un elemento neutro e allora diciamo che un elemento x ha per *inverso sinistro* un elemento y se $y \circ x = e$. Allo stesso modo un *inverso destro* per x è un elemento y per cui $x \circ y = e$ e, infine, un *inverso* è un inverso sinistro che è contemporaneamente un inverso destro.

Se \circ è un'operazione sull'insieme X e Y è un sottoinsieme di X , allora diciamo che Y è *chiuso* rispetto a \circ se per ogni coppia di elementi y_1, y_2 di Y si ha $y_1 \circ y_2 \in Y$. Se Y è chiuso per \circ allora possiamo *restringere* l'operazione

◦ ad un'operazione di Y definendo $Y \times Y \ni (y_1, y_2) \mapsto y_1 \circ y_2 \in Y$. Di solito l'operazione ristretta di Y si indica con lo stesso simbolo dell'operazione di X .

Date due operazioni \circ e $+$ su un insieme X diciamo che \circ è *distributiva* rispetto a $+$ se per ogni $x, y, z \in X$ vale: $(x + y) \circ z = (x \circ z) + (y \circ z)$ e $x \circ (y + z) = (x \circ y) + (x \circ z)$.

1.1.6 I numeri

Nel seguito faremo uso di vari insiemi numerici, soprattutto come esempi di strutture algebriche. Essi sono tutti costruiti a partire dai naturali visti nella Sezione 1.1.4. Così, ad esempio, gli interi \mathbb{Z} sono i “naturali con segno” e possono essere definiti come le coppie in $\mathbb{N} \times \mathbb{N}$ modulo la relazione di equivalenza $(n, m) \sim (h, k)$ se $n + k = m + h$; la classe di equivalenza di (n, m) è l'intero $n - m$. L'addizione e la moltiplicazione con i naturali possono essere estese agli interi. Con i naturali possiamo risolvere l'equazione $x + a = b$ se solo se $a \leq b$, con gli interi invece la stessa equazione è sempre risolubile e si ha la soluzione $b - a$.

In modo analogo si costruisce l'insieme \mathbb{Q} dei numeri razionali come $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ modulo la relazione di equivalenza $(n, m) \sim (h, k)$ se $nk = mh$; la classe di equivalenza di (n, m) è il numero razionale n/m . Anche in questo caso possiamo estendere le operazioni di \mathbb{Z} . Mentre con gli interi l'equazione $ax = b$ è risolubile se e solo se b è un multiplo di a , con i razionali ciò è sempre possibile se $a \neq 0$ e si ha la soluzione b/a .

Esistono però delle equazioni che non hanno alcuna soluzioni in numeri razionali, ad esempio $x^2 - 2 = 0$; si opera un'ulteriore estensione introducendo i numeri reali. La costruzione dell'insieme \mathbb{R} dei numeri reali è però alquanto più complicata. Benché già i greci ne avessero compreso alcune proprietà con ciò che loro chiamavano “teoria dei rapporti delle lunghezze”, solo verso la fine del XIX secolo si arrivò ad una precisa definizione formale. Qui ricordiamo soltanto che si possono seguire varie strade; ad esempio usare le successioni di Cauchy in razionali o le sezioni di Dedekind. In entrambi i casi, si tratta di “completare” \mathbb{Q} aggiungendo quelle quantità che possono essere approximate con numeri razionali ma che non sono in \mathbb{Q} . In \mathbb{R} abbiamo, ad esempio, il numero $\sqrt{2}$ che è una soluzione dell'equazione $x^2 - 2 = 0$ vista prima. Ma non abbiamo ancora finito, infatti l'equazione $x^2 + 1 = 0$ non ha alcuna soluzione in numeri reali; infatti il quadrato di un numero reale è sempre non negativo.

Spendiamo ora qualche parola riguardo al passo successivo, i numeri complessi; essi non presentano nessuna seria difficoltà, una volta che siano stati costruiti i numeri reali. Chiamiamo numero complesso ogni coppia (a, b) di numeri reali; come è tradizione indichiamo la coppia (a, b) con $a + ib$, dove i è un simbolo detto *unità immaginaria*, inoltre a è la *parte reale* e b è la *parte immaginaria*. Definiamo la somma e la moltiplicazione per i numeri complessi come

$$\begin{aligned}(a + ib) + (c + id) &= (a + c) + i(b + d) \\ (a + ib)(c + id) &= (ac - bd) + i(ad + bc).\end{aligned}$$

Considerando i numeri complessi del tipo $a + i \cdot 0$, troviamo subito che i numeri reali sono naturalmente un sottoinsieme dei numeri complessi. È inoltre immediato provare che le operazioni così definite sull'insieme \mathbb{C} dei numeri complessi estendono quelle dei numeri reali. Il motivo per cui abbiamo definito la moltiplicazione tra numeri complessi nel modo appena visto è che ora vale: $i^2 = (0 + i \cdot 1)^2 = -1$; anche -1 ha una radice quadrata. Altrimenti detto, l'equazione $x^2 + 1 = 0$ ha le due soluzioni complesse $\pm i$.

Un numero complesso $0 + ib$ viene detto *immaginario puro*. Può risultare utile pensare ai numeri complessi come ai punti di un piano, detto *piano complesso*, in cui l'asse delle ascisse è l'asse dei numeri reali, corrispondente al coefficiente a , e l'asse delle ordinate è l'asse dei numeri immaginari puri, corrispondente al coefficiente b nella scrittura $a + ib$. In questa rappresentazione l'origine degli assi è il numero complesso $0 = 0 + i \cdot 0$, l'elemento neutro per la somma. Quella che abbiamo finora introdotto si chiama *forma algebrica* dei numeri complessi.

Dato un numero complesso $z = a + ib$ chiamiamo $\bar{z} = a - ib$ il *coniugato* di z . Il coniugato di z è il simmetrico di z rispetto alla retta reale. La distanza del punto z dall'origine è $|z| = \sqrt{a^2 + b^2}$ detta *modulo* di z , osserviamo che $|z|^2 = z \cdot \bar{z}$. Da questa identità otteniamo la formula $1/z = \bar{z}/|z|^2$ per l'inverso di un numero complesso non nullo. In particolare, per i numeri complessi di modulo 1, cioè per i punti della circonferenza unitaria nel piano complesso, si ha $z^{-1} = \bar{z}$.

Se $z \neq 0$, indichiamo con θ l'*argomento* di z , cioè l'angolo formato dalla semiretta reale positiva e la congiungente l'origine 0 con il punto z ; allora vale

$$z = |z|(\cos \theta + i \sin \theta).$$

Vi è una fondamentale formula che lega l'esponenziale complesso e le funzioni trigonometriche, è la Formula di Eulero

$$e^{i\theta} = \cos \theta + i \sin \theta;$$

usando questa formula possiamo esprimere un numero complesso z nella sua *forma polare*

$$z = |z|e^{i\theta}.$$

Per $z = 0$ l'argomento θ è indefinito, mentre, se $z \neq 0$, la forma polare è unica a meno di multipli di 2π per θ . Si noti come al variare di θ il numero complesso $|z|e^{i\theta}$ si muova sulla circonferenza di centro 0 e raggio $|z|$. In particolare, grazie alla Formula di Eulero, l'applicazione $\theta \mapsto e^{i\theta}$ parametrizza i punti della circonferenza unitaria.

La forma polare è particolarmente adatta per il calcolo delle potenze di un numero complesso; si ha infatti subito che se $z = |z|e^{i\theta}$ e n è un intero, allora

$$z^n = |z|^n e^{in\theta},$$

o, in altri termini, il modulo di z^n è $|z|^n$ e l'argomento è $n\theta$. Analogamente possiamo calcolare le radici n -esime di z , cioè quei numeri complessi ζ per cui $\zeta^n = z$; esse

sono date da

$$\sqrt[n]{|z|} e^{i \frac{\theta + 2k\pi}{n}}, \quad \text{con } k = 0, 1, 2, \dots, n-1.$$

Si osservi che se $z \neq 0$ abbiamo n radici n -esime distinte. Ponendo $z = 1$, questa formula si specializza al caso, per noi particolarmente interessante, delle *radici n -esime dell'unità*

$$e^{2\pi i k/n} = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad \text{con } k = 0, 1, 2, \dots, n-1.$$

Inoltre, fissando $\zeta_n = e^{2\pi i/n}$, tutte le radici n -esime dell'unità si ottengono come $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$.

Concludiamo questa breve introduzione ai vari tipi di numeri osservando che ogni equazione

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0,$$

con $a_0, a_1, \dots, a_{n-1}, a_n$ complessi e $a_n \neq 0$, ha una soluzione in \mathbb{C} se $n > 0$; non c'è più bisogno di estendere l'insieme dei numeri per risolvere le equazioni. In seguito studieremo in dettaglio le equazioni polinomiali, concentrandoci sul meccanismo di estensione tramite soluzioni che in questa sezione abbiamo più volte incontrato in modo informale.

Osserviamo che le usuali operazioni di addizione e moltiplicazione tra interi, razionali, reali e complessi sono associative e commutative, hanno per elementi neutri 0 e 1 rispettivamente, l'inverso dell'intero a rispetto all'addizione è $-a$ e, infine, la moltiplicazione è distributiva rispetto all'addizione.

1.2 Combinatoria

Un insieme X si dice *finito* se ha un numero finito di elementi, tale numero si chiama la *cardinalità* di X e si indica con $|X|$. Se X non è finito allora diremo che è *infinito* e che la sua cardinalità è infinita. Due insiemi hanno la stessa cardinalità finita se e solo se possono essere messi in biiezione tra loro. In particolare, X è finito di cardinalità n se e solo se esiste una biiezione tra $\{1, 2, \dots, n\}$ e X , possiamo quindi elencare gli elementi di X e scrivere $X = \{x_1, x_2, \dots, x_n\}$.

È possibile definire la cardinalità in maniera più raffinata, distinguendo tra varie cardinalità per gli insiemi infiniti. Ciò esula però dagli scopi di questo volume; qui ci accontenteremo di distinguere tra insiemi finiti e non.

Una prima osservazione sugli insiemi finiti è la seguente

Osservazione 2.1 *Un'applicazione $X \longrightarrow Y$ tra insiemi finiti della stessa cardinalità è iniettiva se e solo se è suriettiva se e solo se è biiettiva.*

Se $X = \{x_1, x_2, \dots, x_n\}$ e $Y = \{y_1, y_2, \dots, y_m\}$ sono due insiemi di cardinalità finita, gli elementi del prodotto cartesiano $X \times Y$ sono (x_i, y_j) con $i = 1, 2, \dots, n$ e $j = 1, 2, \dots, m$. Abbiamo cioè

Osservazione 2.2 *Se X e Y sono insiemi finiti allora si ha*

$$|X \times Y| = |X| \cdot |Y|.$$

Se invece uno dei due insiemi è infinito e l'altro è non vuoto, allora anche il prodotto cartesiano è infinito.

Una applicazione $f : X \longrightarrow Y$ con X di cardinalità n è completamente determinata da una n -upla di elementi di Y , esiste cioè una biiezione tra Y^X e Y^n ; in particolare

Osservazione 2.3 *Se X e Y sono insiemi finiti non entrambi vuoti allora la cardinalità dell'insieme Y^X di tutte le applicazioni da X in Y è data da*

$$|Y^X| = |Y|^{|X|}.$$

Se invece uno dei due insiemi è infinito e l'altro è non vuoto, allora anche Y^X è infinito.

Ad un sottoinsieme A di X possiamo associare la sua *funzione caratteristica* $\chi_A : X \longrightarrow \{0, 1\}$ definita da $\chi_A(x) = 1$ se $x \in A$ e $\chi_A(x) = 0$ se $x \notin A$. I sottoinsiemi di X sono in biiezione con le loro funzioni caratteristiche e quindi

Osservazione 2.4 *Se X è un insieme finito allora la cardinalità dell'insieme delle parti $\mathcal{P}(X)$ è*

$$|\mathcal{P}(X)| = 2^{|X|},$$

se invece X è infinito allora anche $\mathcal{P}(X)$ è infinito.

Il numero delle applicazioni iniettive da un insieme X di n elementi in un insieme Y di m elementi può essere facilmente contato; basta osservare che un'applicazione iniettiva corrisponde ad una scelta ordinata di n elementi distinti di Y .

Osservazione 2.5 *Sia $|X| = n$ e $|Y| = m$. Se $n > m$ allora non ci sono applicazioni iniettive da X in Y , se invece $n \leq m$ allora il numero delle applicazioni iniettive da X in Y è $m(m-1)(m-2) \cdots (m-n+1)$.*

La conclusione di questa osservazione, per $n > m$, è a volta enunciata come segue

Osservazione 2.6 (Principio dei cassetti) *Se n oggetti sono disposti in m cassetti e $n > m$ allora esiste un cassetto che contiene almeno due oggetti.*

Il *fattoriale* $n!$ di un naturale n è definito per ricorrenza come $0! = 1$ e, per ogni $n \geq 0$, $(n+1)! = (n+1) \cdot n!$. Ovviamente, ciò è equivalente a porre $n! = n \cdot (n-1) \cdots 2 \cdot 1$. Grazie all'Osservazione 2.1, un caso particolare della formula appena vista per le funzioni iniettive è

Osservazione 2.7 *Il numero di permutazioni di un insieme con n elementi è $n!$*

Come vedremo in seguito, le permutazioni di un insieme di n elementi sono un oggetto fondamentale della teoria dei gruppi; se $X = \{1, 2, \dots, n\}$ allora l'insieme $S(X)$ delle permutazioni di X viene indicato semplicemente con S_n . Per quanto abbiamo appena visto $|S_n| = n!$

L'insieme delle parti $\mathcal{P}(X)$ di un insieme X con n elementi può essere suddiviso in base alla cardinalità dei sottoinsiemi, cioè

$$\mathcal{P}(X) = \bigsqcup_{k=0}^n \{A \subseteq X \mid |A| = k\}.$$

Inoltre, da quanto richiamato sopra, possiamo subito ricavare che

Osservazione 2.8 *Se $|X| = n$ e $0 \leq k \leq n$, allora il numero di sottoinsiemi di X di cardinalità k è*

$$\frac{n \cdot (n-1) \cdots (n-k+1)}{k!}.$$

Questa conclusione ha un'importanza fondamentale per la combinatoria; se $n \geq 0$ e $0 \leq k \leq n$ definiamo il *coefficiente binomiale* di posto n, k come

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Si noti che, in particolare, $\binom{n}{0} = 1$, e infatti vi è un solo sottoinsieme con 0 elementi in X , cioè l'insieme vuoto, e $\binom{n}{n} = 1$ e infatti vi è un solo sottoinsieme con n elementi in X , cioè X stesso. È a volte utile estendere il significato del simbolo $\binom{n}{k}$ definendolo come 0 per ogni $k < 0$ e $k > n$.

I coefficienti binomiali soddisfano moltissime relazioni tra loro; due delle principali sono le seguenti

Osservazione 2.9 *Per ogni $n \geq 0$ si ha*

$$\binom{n}{n-k} = \binom{n}{k}$$

e vale anche

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

La seconda di queste relazioni può essere usata come definizione ricorsiva dei coefficienti binomiali dopo aver posto $\binom{0}{0} = 1$ e $\binom{0}{k} = 0$ per ogni $k \neq 0$.

Dalla decomposizione di $\mathcal{P}(X)$ in sottoinsiemi per cardinalità abbiamo l'altra relazione

Osservazione 2.10 *Se n è un naturale allora*

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$

È usuale disporre i coefficienti binomiali in un triangolo che ha per righe i vari $\binom{n}{k}$ con n fissato. Le prime sei righe di tale triangolo, detto triangolo di Tartaglia o di Pascal, sono

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

I coefficienti binomiali possono essere usati per sviluppare le potenze di un binomio.

Teorema 2.11 (del Binomio di Newton) *Se a e b sono due numeri e n è un intero non negativo, allora si ha*

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

In realtà lo stesso risultato è valido per a e b in un qualsiasi anello commutativo; si veda in seguito nel capitolo sugli anelli.

Dati due sottoinsiemi X_1 e X_2 di un insieme X con $X = X_1 \cup X_2$ allora

$$|X| = |X_1| + |X_2| - |X_1 \cap X_2|,$$

infatti gli elementi di $X_1 \cap X_2$ appartengono ad entrambi i sottoinsiemi e sono quindi contati due volte in $|X_1| + |X_2|$. La formula appena vista è un caso particolare del seguente

Proposizione 2.12 (Principio di inclusione esclusione) *Se X è un insieme finito e X_1, X_2, \dots, X_k sono suoi sottoinsiemi con $X_1 \cup X_2 \cup \dots \cup X_k = X$ allora si ha*

$$|X| = \sum (-1)^{h+1} |X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_h}|$$

dove la somma è per $h = 1, \dots, k$ e per tutte le h -uple (i_1, i_2, \dots, i_h) con $1 \leq i_1 < i_2 < \dots < i_h \leq n$.

Ad esempio, il caso con $k = 3$ della formula di inclusione esclusione è

$$|X| = |X_1| + |X_2| + |X_3| - |X_1 \cap X_2| - |X_1 \cap X_3| - |X_2 \cap X_3| + |X_1 \cap X_2 \cap X_3|.$$

Se invece assumiamo che $\{X_1, X_2, \dots, X_k\}$ sia una partizione dell'insieme X allora chiaramente

$$|X| = |X_1| + |X_2| + \dots + |X_k|.$$

1.3 I numeri interi

1.3.1 La divisibilità tra interi

L'aritmetica degli interi è fondata sulla *Divisione Euclidea*, richiamata nella seguente

Proposizione 3.1 (Divisione Euclidea) *Dati un intero a e un intero positivo m , esistono e sono unici un intero q , detto quoziente, e un intero non negativo r , detto resto, tali che $a = q \cdot m + r$ e $0 \leq r < m$.*

Se nella Divisione Euclidea succede che $r = 0$ allora $a = q \cdot m$ e scriviamo $m \mid a$: diciamo che a è un *multiplo* di m o che m *divide* a e chiamiamo m un *divisore* di a . Se m invece non divide a scriviamo $m \nmid a$. Solo ± 1 dividono 1 mentre ogni intero non nullo è un divisore di 0.

Se a e b sono due interi non entrambi nulli chiamiamo *massimo comun divisore* di a e b un intero positivo m tale che: m è un divisore di a e di b e, se n è un altro divisore comune di a e b , allora n divide m . È grazie alla Divisione Euclidea che possiamo dimostrare

Proposizione 3.2 *Il massimo comun divisore m di due interi non entrambi nulli esiste ed è unico. Inoltre esistono due interi x e y per cui $m = xa + yb$; tale identità è detta *Identità di Bezout*.*

Nel seguito scriveremo (a, b) per indicare il massimo comun divisore di a e b . Osserviamo che $(a, b) = (|a|, |b|)$, possiamo cioè sempre ricondurci a due interi non negativi. Per il calcolo del massimo comun divisore si può utilizzare

Proposizione 3.3 (Algoritmo di Euclide) *Supponiamo che a e b siano interi non negativi con $a \geq b$ e poniamo $r_0 = a$, $r_1 = b$. Se, per $k \geq 1$, $r_k > 0$ allora definiamo ricorsivamente r_{k+1} come il resto della divisione di r_{k-1} per r_k . Visto che $r_0 > r_1 > r_2 > \dots \geq 0$, in un numero finito di passi, diciamo n , avremo $r_n = 0$. Risulterà allora $(a, b) = r_{n-1}$.*

Questo algoritmo può essere usato per calcolare esplicitamente una soluzione (x, y) dell'Identità di Bezout; basta infatti sostituire le espressioni che definiscono i resti r_k in termini dei resti precedenti fino a giungere alla prima equazione $a = qb + r_1$ per ottenere un'identità contenente solo a , b e l'ultimo resto non nullo $r_{n-1} = (a, b)$.

Due numeri interi si dicono *primi tra loro* se succede che $(a, b) = 1$; ciò vale se e solo se esistono due interi x, y per cui $xa + yb = 1$.

Osservazione 3.4 (Lemma di Euclide) *Se m divide il prodotto di interi $a \cdot b$ e m è primo con a allora m divide b .*

Con il Lemma di Euclide possiamo facilmente trovare tutte le soluzioni dell'Identità di Bezout

Proposizione 3.5 *Siano a, b due interi non entrambi nulli, sia m il loro massimo comun divisore e sia (x_0, y_0) una soluzione dell'Identità di Bezout per a, b . Allora tutte le coppie di interi per cui vale l'Identità di Bezout sono date da*

$$\left(x_0 + k \frac{b}{m}, y_0 - k \frac{a}{m}\right), \quad k \in \mathbb{Z}.$$

Chiamiamo *equazione diofantea lineare* nelle due variabili intere x e y un'equazione del tipo $ax + by = c$ con a, b e c coefficienti interi. In generale ogni equazione con coefficienti interi di cui si cercano le soluzioni intere si chiama equazione diofantea. La soluzione di questo tipo di equazioni è ben diversa dalla soluzione in numeri reali ed è, di solito, molto difficile. Non è lontana dal vero l'affermazione che la matematica attuale è in grado di risolvere solo le equazioni diofantee lineari e quadratiche; già le equazioni cubiche fanno parte dell'intrigato e affascinante mondo in cui vivono anche le curve ellittiche.

Nell'Esercizio Preliminare 7, per il caso di equazioni lineari si utilizza l'Identità di Bezout per provare

Proposizione 3.6 *L'equazione diofantea $ax + by = c$ ha soluzione se e solo se il massimo comun divisore $m = (a, b)$ divide il termine noto c . In tal caso, detta (x_0, y_0) una soluzione, tutte le soluzioni sono date da*

$$\left(x_0 + k \frac{b}{m}, y_0 - k \frac{a}{m}\right), \quad k \in \mathbb{Z}.$$

Vediamo ora la definizione fondamentale dell'aritmetica degli interi. Un numero intero positivo p è detto *primo* se ha solo i due distinti divisori positivi 1 e p . Si noti che 1 non è quindi un numero primo. Se n è un intero allora il massimo comun divisore (p, n) può essere solo p , nel caso p divida n , o 1, nel caso p non divida n . Da ciò segue subito

Osservazione 3.7 *Se un primo p divide il prodotto $a \cdot b$ e p non divide a allora p divide b .*

È un classico risultato dell'aritmetica greca che ogni intero si fattorizzi in primi in modo essenzialmente unico, vale cioè

Teorema 3.8 (Fondamentale dell’Aritmetica) *Se n è un intero positivo allora esistono, unici a meno dell’ordine, numeri primi p_1, p_2, \dots, p_r tali che $n = p_1 p_2 \cdots p_r$.*

Se p è un primo e n è un intero, diciamo che una potenza p^e divide esattamente n se p^e divide n e p^{e+1} non divide n . In altre parole, p^e divide esattamente n se e solo se il primo p appare nella fattorizzazione di n con esponente e .

Dati due interi non entrambi nulli a e b definiamo il loro *minimo comune multiplo*, indicato con $[a, b]$, come un multiplo comune positivo che è diviso da ogni altro multiplo comune. Analogamente al massimo comun divisore, il minimo comune multiplo esiste ed è unico; vale inoltre $(a, b)[a, b] = ab$. La definizione di minimo comune multiplo è duale a quella di massimo comune divisore; così, spesso, le loro proprietà sono simili.

1.3.2 Le congruenze

Nel suo libro “Disquisitiones Arithmeticae” del 1801, Carl Friedrich Gauss introdusse quella che si è dimostrata essere una delle più importanti relazioni tra numeri interi per l’aritmetica elementare: diciamo che l’intero a è *congruo* all’intero b modulo n , e scriviamo $a \equiv b \pmod{n}$, se $a - b$ è un multiplo di n . È facile provare che la relazione di congruenza è una relazione di equivalenza.

La classe di equivalenza dell’intero a , cioè l’insieme di tutti gli interi congrui ad a , è indicata con $[a]_n$ ed è chiaramente l’insieme $\{a + kn \mid k \in \mathbb{Z}\}$. In altri termini, $[a]_n$ è l’insieme degli interi che hanno lo stesso resto di a quando divisi per n . Se il modulo n è chiaro dal contesto, indicheremo la classe $[a]_n$ anche con \bar{a} .

Come per tutte le relazioni di equivalenza, le classi di congruenza modulo n formano una partizione di \mathbb{Z} . Come insieme di rappresentanti possiamo prendere $\{0, 1, 2, \dots, n-1\}$, essi saranno detti *residui modulo n* ; in particolare le classi di equivalenza sono in numero di n . Ovviamente, qualsiasi insieme di n interi che hanno resti distinti quando divisi per n , è un sistema di rappresentanti per le classi di congruenza modulo n . Si noti che n interi consecutivi formano sempre un sistema di rappresentanti.

L’insieme quoziente di \mathbb{Z} per la relazione di congruenza modulo n è indicato con $\mathbb{Z}/n\mathbb{Z}$. Vedremo in seguito, quando studieremo i gruppi, il perché di questa particolare notazione, per ora essa ci ricorda che nel quoziente “identifichiamo” tra di loro gli interi che differiscono per un multiplo di n , cioè per un elemento di $n\mathbb{Z}$.

Vediamo alcune proprietà della congruenza modulo n .

Proposizione 3.9 *Siano a e b due interi con $a \equiv b \pmod{n}$. Allora valgono*

- (i) $(a, n) = (b, n)$,
- (ii) se $m \mid n$ allora $a \equiv b \pmod{m}$,
- (iii) se si ha anche $a \equiv b \pmod{m}$ allora $a \equiv b \pmod{[n, m]}$,

Un modo equivalente di enunciare la seconda proprietà è: se n è un multiplo di m allora le classi di congruenza modulo n sono una partizione più fine delle classi

di congruenza modulo m . Infatti

$$[a]_m = \bigsqcup_{h=0,1,\dots,\frac{n}{m}-1} [a + mh]_n.$$

Osserviamo quindi che se n è un multiplo di m è definita una mappa $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ che manda la classe $[a]_n$ in $[a]_m$, essa rende commutativo il diagramma

$$\begin{array}{ccc} & a & \\ \swarrow & & \searrow \\ [a]_n & \xrightarrow{\quad} & [a]_m \end{array}$$

come già osservato nella sezione sulle relazioni.

La relazione di congruenza modulo n è compatibile con l'addizione e la moltiplicazione di interi.

Proposizione 3.10 *Se a, b, a' e b' sono quattro interi e vale $a \equiv b \pmod{n}$, $a' \equiv b' \pmod{n}$ allora $a + a' \equiv b + b' \pmod{n}$ e $a \cdot a' \equiv b \cdot b' \pmod{n}$.*

In particolare, se $a \equiv b \pmod{n}$ e k è un intero, allora $ka \equiv kb \pmod{n}$. Osserviamo esplicitamente che l'inverso di quanto appena notato è in generale falso: $2 \cdot 2 \equiv 2 \cdot 0 \pmod{4}$ mentre $2 \not\equiv 0 \pmod{4}$. Un parziale inverso è

Proposizione 3.11 *Se a, b e k sono interi e $k \neq 0$ allora*

$$ka \equiv kb \pmod{n} \quad \text{implica} \quad a \equiv b \pmod{\frac{n}{(n,k)}}.$$

In particolare, se il fattore k è primo con il modulo n , allora

$$ka \equiv kb \pmod{n} \quad \text{se e solo se} \quad a \equiv b \pmod{n}.$$

Quindi, continuando l'esempio di prima, da $2 \cdot 2 \equiv 2 \cdot 0 \pmod{4}$ ricaviamo correttamente $2 \equiv 0 \pmod{2}$ visto che $4/(4, 2) = 2$.

Quanto richiamato finora, benché elementare, ha delle applicazioni già non del tutto ovvie all'aritmetica. Per esempio, usando la rappresentazione in base 10 di un intero e come modulo 3 è possibile ricavare il ben noto criterio di divisibilità per 3, basta infatti osservare che $10 \equiv 1 \pmod{3}$. Allo stesso modo si ricavano i criteri per 2, 4, 5, 9, 11 e 25; è anche possibile ottenere criteri, sempre più complicati, per 7 e per 13.

Un primo risultato non banale sulle classi di resto modulo un primo è il seguente

Teorema 3.12 (del Binomio Ingenuo) *Se p è un numero primo allora, per ogni coppia di interi a e b vale*

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

La dimostrazione di questo teorema segue facilmente una volta osservato che i coefficienti binomiali $\binom{p}{h}$ con p primo e $1 \leq h \leq p-1$ sono tutti divisibili per p .

Usando il Teorema del Binomio Ingenuo è possibile provare per induzione

Teorema 3.13 (di Fermat) *Se p è un numero primo allora*

$$a^p \equiv a \pmod{p}$$

per ogni intero a .

Abbiamo, come facile corollario di questo teorema, uno dei primi risultati non banali sui numeri primi della storia della matematica dopo Euclide

Corollario 3.14 (Piccolo Teorema di Fermat) *Se p è un primo e a è un intero primo con p , allora $a^{p-1} \equiv 1 \pmod{p}$.*

La soluzione di una congruenza lineare, cioè di un'equazione in x del tipo $ax \equiv b \pmod{n}$ con a e b interi, si riconduce immediatamente all'equazione diofantea lineare $ax + ny = b$ in x e y . Da ciò si ricava subito

Proposizione 3.15 *La congruenza lineare $ax \equiv b \pmod{n}$ ha soluzione se e solo se $m = (a, n)$ divide b . In tal caso, detta x_0 una soluzione, tutte le soluzioni sono date da*

$$\left[x_0 + k \frac{n}{m} \right]_n \quad \text{per } k = 0, 1, \dots, m-1;$$

in particolare vi sono m soluzioni modulo n .

Per la soluzioni dei sistemi di equazioni lineari è fondamentale il seguente teorema

Teorema 3.16 (Cinese dei Resti) *Se n_1, n_2, \dots, n_r sono r interi non nulli a due a due primi tra loro e a_1, a_2, \dots, a_r sono interi, allora il sistema di congruenze*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

ha una e una sola soluzione modulo $n_1 n_2 \cdots n_r$.

Alla fine della prossima sezione vedremo come calcolare una soluzione di un sistema lineare di congruenze come nel teorema appena visto.

1.3.3 L'aritmetica modulare

Le proprietà di compatibilità della relazione di congruenza modulo un intero non nullo n viste nella sezione precedente ci permettono di definire due operazioni sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ delle classi di resto modulo n .

Definiamo l'addizione $+$ e la moltiplicazione \cdot delle due classi di resto $[a]_n$ e $[b]_n$ come

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

Queste definizioni sono ben poste: esse non dipendono dai rappresentanti a e b in \mathbb{Z} scelti per le classi $[a]_n$ e $[b]_n$ ma solo dalle classi; ciò è una diretta conseguenza della Proposizione 3.10.

Dalle corrispondenti proprietà degli interi seguono le conclusioni del seguente

Teorema 3.17 (i) *Le operazioni $+$ e \cdot sono associative, vale cioè*

$$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n), \quad ([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

per ogni $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$.

(ii) *Le operazioni $+$ e \cdot sono commutative, vale cioè*

$$[a]_n + [b]_n = [b]_n + [a]_n, \quad [a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

per ogni $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$.

(iii) *La classe $[0]_n$ è l'elemento neutro per l'addizione e la classe $[1]_n$ è l'elemento neutro per la moltiplicazione. Inoltre l'elemento $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ ha per inverso rispetto $+$ l'elemento $[-a]_n$.*

(iv) *L'operazione \cdot è distributiva rispetto all'operazione $+$, vale cioè*

$$[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$$

per ogni $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$.

A differenza dell'addizione non tutte le classi di resto hanno un inverso rispetto alla moltiplicazione: ad esempio $[2]_4$ non ha un inverso in $\mathbb{Z}/4\mathbb{Z}$. Le classi $[a]_n$ per cui un inverso moltiplicativo esiste sono dette *invertibili*: $[a]_n$ è quindi invertibile se esiste una classe $[b]_n$ per cui $[a]_n[b]_n = [1]_n$. L'insieme delle classi invertibili modulo n si indica con $(\mathbb{Z}/n\mathbb{Z})^*$.

Dal criterio di risolubilità per le congruenze lineari troviamo che la classe $[a]_n$ è invertibile se e solo se $(a, n) = 1$. È quindi chiaro che il prodotto di due classi invertibili è ancora una classe invertibile; in altri termini, la moltiplicazione induce per restrizione un'operazione, indicata ancora con \cdot , su $(\mathbb{Z}/n\mathbb{Z})^*$. Nel caso particolare di modulo p un numero primo si ha $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$, cioè ogni classe non nulla è invertibile modulo un primo.

Per calcolare l'inverso della classe $[a]_n$ si può usare l'Identità di Bezout. Infatti da $(a, n) = 1$ segue che esistono interi b e c , calcolabili con l'Algoritmo di Euclide,

per cui $ab + nc = 1$; ma allora, passando alle classi modulo n , otteniamo $ab \equiv 1 \pmod{n}$, cioè $[b]_n$ è l'inverso di $[a]_n$.

Possiamo enunciare il Teorema Cinese dei Resti sui sistemi di congruenze lineari, in modo equivalente, come una proprietà delle classi di resto

Teorema 3.18 *Se n e m sono due interi non nulli primi tra loro allora l'applicazione*

$$\mathbb{Z}/mn\mathbb{Z} \ni [a]_{nm} \mapsto ([a]_n, [a]_m) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

è biiettiva.

Un immediato corollario è il seguente

Corollario 3.19 *Siano m e n due interi non nulli primi tra loro, la classe $[a]_{nm}$ è invertibile se e solo se $[a]_n$ e $[a]_m$ sono invertibili, inoltre l'applicazione $[a]_{nm} \mapsto ([a]_n, [a]_m)$ è una biiezione tra $(\mathbb{Z}/nm\mathbb{Z})^*$ e $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.*

La funzione di Eulero $n \mapsto \phi(n)$ associa ad un intero positivo n il numero $\phi(n)$ di interi tra 1 e n primi con n ; questa funzione ha un ruolo importante nell'aritmetica modulare. Per quanto visto $\phi(n)$ è anche uguale al numero di elementi invertibili modulo n , cioè $\phi(n)$ è la cardinalità di $(\mathbb{Z}/n\mathbb{Z})^*$. Abbiamo ad esempio $\phi(p) = p - 1$.

Una funzione f su \mathbb{N} è detta *moltiplicativa* se, per ogni coppia di naturali n e m primi tra loro, si ha $f(nm) = f(n)f(m)$. Il corollario precedente permette di concludere allora che la funzione di Eulero è moltiplicativa. Contando i numeri da 1 a p^e non divisibili per p è chiaro che $\phi(p^e) = (p - 1)p^{e-1}$, per ogni intero $e \geq 1$. Abbiamo così provato la seguente formula

Osservazione 3.20 *Se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ è la fattorizzazione di n in primi con $p_i \neq p_j$ per $i \neq j$ e $e_i \geq 1$ per ogni i , allora*

$$\phi(n) = \prod_{i=1}^r (p_i - 1) p_i^{e_i - 1}.$$

Il Corollario 3.14 può essere anche espresso come $a^{\phi(p)} \equiv 1 \pmod{p}$ se p è primo e a non è divisibile per p . In questa forma esso può essere generalizzato in

Teorema 3.21 (di Eulero) *Se a è un intero primo con il modulo n allora $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Terminiamo questa parte sulle congruenze illustrando in dettaglio alcuni metodi per risolvere i sistemi di congruenze lineari con moduli coprimi, come nel Teorema Cinese dei Resti. Consideriamo il sistema di due congruenze

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

con n_1 e n_2 primi tra loro. Risolvere il sistema è equivalente a trovare due interi u e v per cui $x = a_1 + un_1$ e $x = a_2 + vn_2$. In altri termini, u e v sono soluzioni dell'equazione diofantea lineare

$$n_1u - n_2v = a_2 - a_1.$$

Questo tipo di equazioni è risolto in dettaglio nell'Esercizio Preliminare 7. Trovati u e v , abbiamo che la soluzione del sistema è la classe di resto di $x_0 = a_1 + un_1 = a_2 + vn_2$ modulo n_1n_2 . Come sappiamo essa è l'unica soluzione modulo n_1n_2 o, equivalentemente, tutte le soluzioni intere sono date da $x_0 + hn_1n_2$ al variare di h in \mathbb{Z} .

Passiamo ora a sistemi con un numero r qualsiasi di congruenze lineari

$$\begin{cases} x \equiv a_1 & (\text{mod } n_1) \\ x \equiv a_2 & (\text{mod } n_2) \\ x \equiv a_3 & (\text{mod } n_3) \\ \vdots \\ x \equiv a_r & (\text{mod } n_r) \end{cases}$$

con n_1, n_2, \dots, n_r a due a due primi tra loro. Possiamo usare il metodo sopra descritto per trovare l'unica soluzione x_0 modulo n_1n_2 del sottosistema delle prime due congruenze e considerare il sistema equivalente

$$\begin{cases} x \equiv x_0 & (\text{mod } n_1n_2) \\ x \equiv a_3 & (\text{mod } n_3) \\ \vdots \\ x \equiv a_r & (\text{mod } n_r) \end{cases}$$

che ha ora $r - 1$ congruenze. Continuando a risolvere le prime due congruenze, troviamo via via sistemi equivalenti con meno congruenze fino alla soluzione del sistema dato.

Vediamo ora un altro metodo per risolvere l'iniziale sistema di r congruenze lineari. Sappiamo che esso ammette una sola soluzione modulo $n_1n_2 \cdots n_r$. Per calcolarla cerchiamo prima dei numeri interi x_1, x_2, \dots, x_r per cui, per ogni $i = 1, 2, \dots, r$, si ha $x_i \equiv 0 \pmod{n_j}$ per ogni $j \neq i$ e $x_i \equiv 1 \pmod{n_i}$. In altri termini, x_1, x_2, \dots, x_r sono soluzioni dei sistemi

$$\begin{cases} x_1 \equiv 1 & (\text{mod } n_1) \\ x_1 \equiv 0 & (\text{mod } n_2) \\ \vdots \\ x_1 \equiv 0 & (\text{mod } n_r) \end{cases} \quad \begin{cases} x_2 \equiv 0 & (\text{mod } n_1) \\ x_2 \equiv 1 & (\text{mod } n_2) \\ \vdots \\ x_2 \equiv 0 & (\text{mod } n_r) \end{cases} \quad \cdots \quad \begin{cases} x_r \equiv 0 & (\text{mod } n_1) \\ x_r \equiv 0 & (\text{mod } n_2) \\ \vdots \\ x_r \equiv 1 & (\text{mod } n_r). \end{cases}$$

Una volta risolti questi sistemi è chiaro che la soluzione del sistema originario è

$$x_0 \equiv a_1x_1 + a_2x_2 + \dots + a_rx_r \pmod{n_1n_2 \cdots n_r}.$$

Per trovare l'intero x_1 , e analogamente x_2, \dots, x_r , basta osservare che necessariamente $x_1 = y_1 n_2 \cdots n_r$ per qualche intero y_1 . Inoltre, $n_2 \cdots n_r$ è una classe invertibile modulo n_1 , date le ipotesi sui moduli n_1, n_2, \dots, n_r ; y_1 si ottiene quindi risolvendo $y_1(n_2 \cdots n_r) \equiv 1 \pmod{n_1}$ o, equivalentemente, $y_1 \equiv (n_2 \cdots n_r)^{-1} \pmod{n_1}$. Questa congruenza è, come sopra, equivalente ad un'equazione diofantea lineare e può quindi essere esplicitamente risolta.

Questo secondo metodo per il calcolo delle soluzioni del sistema attraverso le soluzioni ausiliarie x_1, x_2, \dots, x_r , può essere utile quando si debbano risolvere più sistemi di congruenze con moduli n_1, n_2, \dots, n_r fissati ma termini noti a_1, a_2, \dots, a_r che cambiamo di sistema in sistema; ciò capita spesso negli esercizi.

Le osservazioni qui viste sul calcolo esplicito delle soluzioni di un sistema di congruenze lineari verranno ripetutamente usate, solitamente senza menzione esplicita, nelle soluzioni degli esercizi presentati.

1.4 I gruppi

1.4.1 Definizione e prime proprietà

Una delle strutture fondamentali dell'algebra è quella di gruppo; essa è abbastanza semplice da essere definita in poche righe ma, nello stesso tempo, ha un'importanza cruciale. Le strutture più complesse che vedremo in seguito saranno tutte basate sui gruppi.

Un insieme non vuoto G con un'operazione \cdot si dice *gruppo* se

- (i) l'operazione \cdot è associativa,
- (ii) in G esiste un elemento e , detto *elemento neutro*, per cui $g \cdot e = g = e \cdot g$ per ogni g in G ,
- (iii) per ogni elemento g di G esiste un elemento h , detto *inverso* di g , tale che $g \cdot h = e = h \cdot g$.

Nel seguito diremo che (G, \cdot) è un gruppo per indicare che \cdot è un'operazione su G che rende tale insieme un gruppo; se l'operazione è chiara dal contesto diremo semplicemente che G è un gruppo. A volte il simbolo \cdot dell'operazione di un gruppo verrà ommesso anche nelle composizioni e scriveremo gh per indicare la composizione $g \cdot h$ di g e h in G .

Gli esempi di gruppo sono innumerevoli: l'insieme \mathbb{Z} dei numeri interi con l'operazione di addizione; l'insieme \mathbb{Q}^* dei numeri razionali non nulli con l'operazione di moltiplicazione; l'insieme \mathbb{R}^* dei numeri reali non nulli, come anche l'insieme \mathbb{C}^* dei numeri complessi non nulli, con l'operazione di prodotto; l'insieme S_n delle permutazioni di n elementi con l'operazione di composizione.

È molto facile provare che in un gruppo esiste un solo elemento neutro. Altrettanto ovvio è che dato un elemento g in un gruppo, esiste un unico inverso di g ; esso è indicato con g^{-1} .

In generale se n è un intero positivo e g un elemento di un gruppo, definiamo g^n come la composizione di g con se stesso n volte e poniamo, inoltre, $g^{-n} = (g^n)^{-1}$.

In questo modo valgono le usuali regole per le potenze: $g^n \cdot g^m = g^{n+m}$ e $(g^n)^m = g^{nm}$ per ogni coppia di naturali n e m .

Se g e h sono due elementi di un gruppo, diciamo che essi *commutano* se $gh = hg$. Inoltre, se succede che l'operazione di un gruppo G è commutativa, se cioè vale $gh = hg$ per ogni g e h in G , o in altri termini se ogni coppia di elementi commuta, diciamo che il gruppo è *commutativo* o *abeliano*. È usuale indicare l'operazione di un gruppo abeliano con $+$, si dice allora che il gruppo è *denotato additivamente*. In un gruppo denotato additivamente scriviamo $-g$ per l'inverso di un elemento g e ng per g^n . Abbiamo ovviamente $(n+m)g = ng + mg$ e $(nm)g = n(mg)$ per ogni coppia di naturali n e m .

L'*ordine* di un gruppo G è la cardinalità dell'insieme G , esso si indica con $|G|$; l'ordine è quindi il numero di elementi di G se G è finito altrimenti l'ordine è infinito. Invece, l'*ordine* di un elemento g è il minimo intero positivo n , se esiste, per cui $g^n = e$; se invece $g^n \neq e$ per ogni n positivo allora diciamo che g ha ordine *infinito*. Indichiamo l'ordine di g con $\text{ord}(g)$.

Si osservi che l'insieme $\mathbb{Z}/n\mathbb{Z}$ delle classi di congruenza modulo un naturale non nullo n è un gruppo con l'operazione $+$ di addizione tra classi, come segue subito dal Teorema 3.17. È chiaro che si tratta di un gruppo abeliano di ordine n . Anche l'insieme $(\mathbb{Z}/n\mathbb{Z})^*$ delle classi invertibili modulo n è un gruppo abeliano con l'operazione \cdot di moltiplicazione tra classi; il suo ordine è $\phi(n)$.

La nostra prima osservazione teorica sui gruppi è la seguente. Dalla definizione di gruppo segue subito che valgono le seguenti leggi

Osservazione 4.1 (Leggi di Cancellazione) *Se in un gruppo G si ha $gh = gk$ allora $h = k$; allo stesso modo se vale $hg = kg$ allora $h = k$.*

1.4.2 Sottogruppi

Un sottoinsieme H di un gruppo G si dice *sottogruppo* se l'operazione \cdot di G può essere ristretta ad un'operazione di H e, con questa operazione, H è un gruppo. Scriviamo $H \leq G$ per indicare che H è un sottogruppo di G . Per verificare che un sottoinsieme non vuoto H è un sottogruppo basta controllare che dati comunque due elementi h e k in H si ha $h \cdot k \in H$ e che, per ogni elemento h di H , vale $h^{-1} \in H$.

Ad esempio, il sottoinsieme $2\mathbb{Z}$ dei numeri pari è un sottogruppo di \mathbb{Z} , come lo è il sottoinsieme $n\mathbb{Z}$ dei multipli di un fissato naturale n . Il sottoinsieme $\{\pm 1\}$ è un sottogruppo di \mathbb{Q}^* che, a sua volta, è un sottogruppo di \mathbb{R}^* . Il sottoinsieme delle permutazioni che fissano 1 è un sottogruppo di S_n .

Il sottoinsieme $\{e\}$ è sempre un sottogruppo di un gruppo G , come anche G è un sottogruppo di G ; questi due sottogruppi sono detti *banali* e i sottogruppi non banali sono anche detti *propri*.

Dato un gruppo G il sottoinsieme $Z(G)$ di tutti gli elementi z di G per cui $zg = gz$ per ogni g di G , si chiama *centro* di G ; un elemento z è nel centro se commuta con tutti gli elementi del gruppo.

Osservazione 4.2 *Il centro $Z(G)$ è un sottogruppo di G .*

Ritroveremo spesso in seguito il centro in varie questioni, esso misura quanto un gruppo è non abeliano: infatti G è abeliano se e solo se $Z(G) = G$.

Osserviamo che l'intersezione di sottogruppi è ancora un sottogruppo; ciò non è invece vero in generale per l'unione. Dato un sottoinsieme X di un gruppo G , indichiamo con $\langle X \rangle$ il sottogruppo *generato* da X in G : esso è definito come l'intersezione di tutti i sottogruppi di G che contengono X . Si osservi che esiste sempre almeno un tale sottogruppo, infatti G contiene X . Diciamo che X è un *insieme di generatori* per il gruppo $\langle X \rangle$. Il sottogruppo $\langle X \rangle$ generato da X in G può essere caratterizzato come il più piccolo sottogruppo di G che contiene X .

In particolare un gruppo G si dice *ciclico* se esiste un elemento g in G per cui $G = \langle g \rangle$; l'elemento g è un generatore per G . Se G è ciclico allora è chiaramente abeliano. Inoltre se g ha ordine finito n allora $G = \{e, g, g^2, \dots, g^{n-1}\}$ e quindi il gruppo ciclico generato da g ha ordine n . Lo stesso vale se g ha ordine infinito, in tal caso si avrà $G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$.

Ad esempio, \mathbb{Z} è un gruppo ciclico infinito, infatti $\mathbb{Z} = \langle 1 \rangle$. Anche $n\mathbb{Z} = \langle n \rangle$ è un gruppo ciclico infinito e $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$ è un gruppo ciclico di ordine n .

Usando la Divisione Euclidea possiamo subito dimostrare che

Osservazione 4.3 *Un sottogruppo di un gruppo ciclico è ancora ciclico.*

Da questa osservazione abbiamo la descrizione dei sottogruppi di \mathbb{Z}

Corollario 4.4 *Se H è un sottogruppo di \mathbb{Z} allora $H = n\mathbb{Z}$ per qualche intero non negativo n .*

Non solo, come richiamato sopra $\mathbb{Z}/n\mathbb{Z}$ è un gruppo ciclico, esso è anche il prototipo di ogni gruppo ciclico finito, come vedremo in seguito. Studiamo quindi i suoi sottogruppi cominciando con l'osservare che dalle proprietà delle congruenze segue

Osservazione 4.5 *Per ogni intero a l'ordine di $[a]_n$ in $\mathbb{Z}/n\mathbb{Z}$ è*

$$\text{ord}([a]_n) = \frac{n}{(a, n)}.$$

Come possiamo vedere subito dalla formula, abbiamo sempre che $\text{ord}([a]_n)$ divide $n = |\mathbb{Z}/n\mathbb{Z}|$; questo non è un caso come avremo modo di vedere nella successiva sezione. Altre importanti conseguenze sono

Osservazione 4.6 *Per ogni divisore d dell'ordine n ci sono $\phi(d)$ elementi di ordine d in $\mathbb{Z}/n\mathbb{Z}$ e, inoltre, vi è un solo sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ di ordine d ; esso è generato dalla classe $[n/d]_n$. Infine, questi sottogruppi esauriscono la classe dei sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.*

Abbiamo un'ulteriore interessante conseguenza suddividendo gli elementi di $\mathbb{Z}/n\mathbb{Z}$ per ordine. Risulta infatti

Osservazione 4.7 *Se n è un naturale non nullo allora $\sum_{d|n} \phi(d) = n$.*

1.4.3 Prodotto di sottogruppi

Se H e K sono sottoinsiemi di un gruppo G definiamo HK come l'insieme di tutti i prodotti hk al variare di h in H e k in K . Anche se H e K sono sottogruppi non è detto che HK sia un sottogruppo di G . Sicuramente se G è abeliano allora HK è un sottogruppo; in generale si ha

Proposizione 4.8 *Il prodotto HK di due sottogruppi H e K è un sottogruppo se e solo se $HK = KH$.*

In generale però, anche se HK non è un sottogruppo, possiamo dire qualcosa sulla sua cardinalità. Si trova subito infatti che ogni elemento di HK può essere espresso come hk per $|H \cap K|$ coppie (h, k) in $H \times K$. Abbiamo quindi

Osservazione 4.9 *Siano H e K due sottogruppi finiti di un gruppo G , allora $|HK| = |H||K|/|H \cap K|$.*

1.4.4 Classi laterali di un sottogruppo

Se H è un sottogruppo di G definiamo una relazione \sim_H in G nel seguente modo: $g \sim_H k$ se e solo se $g^{-1}k \in H$; diciamo che g è *congruo* a k modulo H o, anche, che g e k sono *congruenti* modulo H . È facile provare che \sim_H è una relazione di equivalenza. Si noti che, in particolare, se n è un naturale non nullo, per il sottogruppo $n\mathbb{Z}$ del gruppo \mathbb{Z} ritroviamo la relazione di congruenza per gli interi definita in precedenza.

Le classi di equivalenza di \sim_H si chiamano *laterali sinistri* di H in G ; questo nome è giustificato dall'essere la classe di equivalenza di g il sottoinsieme $gH = \{gh \mid h \in H\}$. Possiamo chiaramente definire una versione destra ponendo $g \sim_H k$ se e solo se $gk^{-1} \in H$; per questa nuova relazione le classi di equivalenza saranno i *laterali destri* $Hg = \{hg \mid h \in H\}$. È chiaro che in un gruppo abeliano non vi è alcuna differenza tra le due relazioni, un sottoinsieme è un laterale destro se e solo se è un laterale sinistro.

L'insieme quoziente rispetto alla relazione \sim_H si indica con G/H , se invece usiamo \sim_H allora scriviamo $H \backslash G$ per il quoziente. Si noti che $gH \mapsto Hg$ è una corrispondenza biunivoca tra G/H e $H \backslash G$.

Definiamo l'*indice* $[G : H]$ del sottogruppo H di G come la cardinalità dell'insieme quoziente G/H . Per quanto osservato questa è anche la cardinalità di $H \backslash G$. Useremo l'indice di un sottogruppo quasi esclusivamente quando esso è finito.

Vogliamo ora ricavare un'importante proprietà dei sottogruppi di un gruppo finito. La mappa $h \mapsto gh$ definisce una biiezione tra H e il laterale sinistro gH ; in particolare ogni laterale ha la stessa cardinalità di H . Visto che \sim_H induce una partizione di G ricaviamo subito

Teorema 4.10 (di Lagrange) *L'ordine di un sottogruppo di un gruppo finito divide l'ordine del gruppo.*

E come corollario abbiamo

Corollario 4.11 *L'ordine di un elemento di un gruppo finito divide l'ordine del gruppo. In particolare se il gruppo finito G ha ordine n e g è un suo elemento allora $g^n = e$.*

Da questo risultato possiamo ricavare il Teorema di Eulero 3.21: basta infatti osservare che $(\mathbb{Z}/n\mathbb{Z})^*$ ha ordine $\phi(n)$.

Un'altra immediata conseguenza riguarda i gruppi di ordine un primo. Se g è un elemento diverso dall'elemento neutro di un gruppo G di ordine primo p , allora l'ordine di g , dovendo dividere p , non può che essere p . Abbiamo così

Corollario 4.12 *Un gruppo di ordine primo è ciclico.*

Infine, per un gruppo finito G e un suo sottogruppo H , troviamo che $[G : H] = |G|/|H|$; in particolare anche l'indice di un sottogruppo è un divisore dell'ordine del gruppo.

1.4.5 Sottogruppi normali

Abbiamo osservato sopra che in un gruppo abeliano i laterali destri di un sottogruppo coincidono con i laterali sinistri. Questa è una proprietà fondamentale e i sottogruppi per cui questo vale hanno un'estrema importanza; è stato Évariste Galois a capirlo per primo.

Sia G un gruppo e h un suo elemento, ogni elemento del tipo ghg^{-1} si dice *coniugato* di h . Se H è un sottoinsieme di G allora gHg^{-1} è l'insieme di tutti gli elementi ghg^{-1} al variare di h in H . Un sottogruppo H si dice *normale* se $gHg^{-1} = H$ per ogni g in G . È chiaro che in un gruppo abeliano ogni sottogruppo è normale visto che $ghg^{-1} = h$ per ogni h e g . Notiamo che possiamo riscrivere la condizione di normalità come $gH = Hg$; troviamo quindi che un sottogruppo è normale se e solo se ogni laterale destro è un laterale sinistro.

Chiaramente i sottogruppo banali $\{e\}$ e G sono normali. Come altro esempio di sottogruppo normale possiamo considerare il centro: infatti $gZ(G) = Z(G)g$ visto che gli elementi di $Z(G)$ commutano con tutti gli elementi di G e, quindi, in particolare con l'elemento g .

Osserviamo inoltre che se H è un sottogruppo normale allora, per ogni coppia g_1, g_2 di elementi di G abbiamo $g_1Hg_2H = g_1g_2HH = g_1g_2H$, cioè il prodotto di due laterali sinistri, come sottoinsiemi di G , è ancora un laterale sinistro.

Ciò suggerisce la possibilità di definire un'operazione sul quoziente G/H ponendo $(g_1H) \cdot (g_2H) = (g_1g_2)H$. L'operazione tra le classi g_1H, g_2H dipende solo

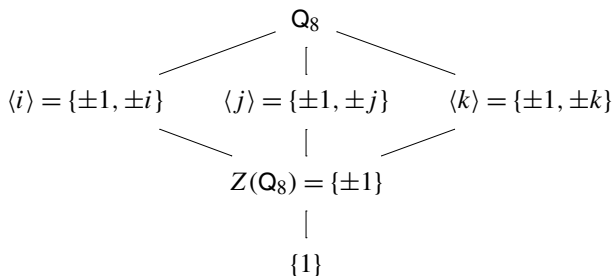
dalle classi e non dai rispettivi rappresentanti g_1 e g_2 scelti; infatti richiedere che questa definizione sia ben posta è esattamente equivalente ad avere H normale in G . Molto di più è vero

Teorema 4.13 *Se H è un sottogruppo normale di G allora l'operazione $g_1H \cdot g_2H = (g_1g_2)H$ definisce una struttura di gruppo sull'insieme quoziente G/H . L'ordine di questo gruppo è $[G : H]$.*

Diciamo che la struttura di gruppo del quoziente G/H è *indotta* dalla struttura di G . Se ritorniamo a considerare il gruppo abeliano \mathbb{Z} e il suo sottogruppo, chiaramente normale, $n\mathbb{Z}$, vediamo che l'operazione di addizione definita sulle classi di congruenza è la struttura indotta sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ dall'addizione di \mathbb{Z} . Questo motiva la scelta della notazione $\mathbb{Z}/n\mathbb{Z}$ per le classi di resto.

Poter costruire un gruppo sull'insieme quoziente è una procedura estremamente importante. In G/H ci dimentichiamo di alcune informazioni, per così dire, visto che identifichiamo gli elementi di G che differiscono per elementi di H ; ma d'altra parte G/H può essere più “semplice” di G . Inoltre, ed è questo il punto, potremmo essere in grado di ricavare alcune informazioni su G dalla conoscenza di G/H .

Abbiamo visto che tutti i sottogruppi di un gruppo abeliano sono normali; non è però vero il viceversa. Infatti, come esempio di sottogruppo non abeliano con tutti i sottogruppi normali, possiamo considerare il gruppo Q_8 delle *unità dei quaternioni*; esso è definito come segue. Gli elementi di Q_8 sono $\pm 1, \pm i, \pm j$ e $\pm k$ in cui 1 è l'elemento neutro, la moltiplicazione per -1 cambia segno agli elementi, $i^2 = j^2 = k^2 = -1$ e $ij = k = -ji, jk = i = -kj$ e $ki = j = -ik$. È facile provare che i sottogruppi di Q_8 sono i seguenti



dove due sottogruppi sono collegati se quello più in basso è un sottogruppo di quello più in alto.

La normalità dei sottogruppi di Q_8 segue da principi generali; notiamo infatti che in questo caso un sottogruppo proprio H o ha indice 2 o è il centro. Ma, come già osservato, il centro è normale ed è, inoltre, sempre vero che

Osservazione 4.14 *Un sottogruppo di indice 2 è normale.*

1.4.6 Il gruppo simmetrico

Fissato un naturale n , l'insieme S_n di tutte le permutazioni di $\{1, 2, \dots, n\}$ è un gruppo con la composizione di applicazioni, esso è detto *gruppo simmetrico* su n elementi. Sappiamo infatti che la composizione di applicazioni biettive è ancora un'applicazione biettiva, che l'applicazione identità è l'elemento neutro per la composizione e che ogni applicazione biettiva è invertibile. Abbiamo anche visto che S_n ha $n!$ elementi.

Se $\sigma \in S_n$ è una permutazione e i_1, i_2, \dots, i_n sono tali che $\sigma(k) = i_k$ per ogni $k = 1, 2, \dots, n$, allora indichiamo la permutazione σ nel seguente modo

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Dati k_1, k_2, \dots, k_ℓ interi distinti nell'insieme $\{1, 2, \dots, n\}$ la permutazione σ per cui

$$\sigma(k_t) = k_{t+1}, \text{ per ogni } t = 1, 2, \dots, \ell - 1,$$

$$\sigma(k_\ell) = k_1,$$

$$\sigma(j) = j \text{ per ogni } j \in \{1, 2, \dots, n\} \setminus \{k_1, k_2, \dots, k_\ell\}$$

è detta *ciclo di lunghezza ℓ* o anche ℓ -ciclo. Indicheremo il ciclo σ appena definito come $(k_1, k_2, \dots, k_\ell)$.

Osserviamo che l'ordine di un ciclo è dato dalla sua lunghezza. Ad esempio, se $n \geq 3$, allora il ciclo $(1, 2, 3)$ in S_n ha ordine 3. Un ciclo (i, j) di lunghezza 2 è detto *trasposizione*: esso scambia i e j e non permuta nessun altro numero in $\{1, 2, \dots, n\}$.

Il gruppo simmetrico S_n è *non* abeliano per ogni $n \geq 3$. Infatti si ha, ad esempio,

$$(123)(12) = (13) \neq (23) = (12)(123).$$

Come si vedrà nel seguito dello studio dell'algebra, non solo i gruppi simmetrici sono non abeliani, ma, anzi, essi sono sufficientemente complicati da contenere ogni gruppo finito come sottogruppo.

1.4.7 Omomorfismi di gruppi

Introduciamo ora gli omomorfismi, applicazioni che rispettano la struttura di gruppo; con gli omomorfismi possiamo confrontare i gruppi mettendoli in relazione tra loro. Come vedremo, questo modo di procedere sarà particolarmente fecondo.

Siano G, H due gruppi con rispettive operazioni \cdot e \circ . Un'applicazione $f: G \rightarrow H$ tra due gruppi si dice *omomorfismo* se $f(g_1 \cdot g_2) = f(g_1) \circ f(g_2)$ per ogni coppia di elementi g_1, g_2 di G .

È immediato dalla definizione che un omomorfismo manda l'elemento neutro di G nell'elemento neutro di H , cioè $f(e_G) = e_H$; inoltre $f(g^{-1}) = f(g)^{-1}$ e

$\text{ord}(f(g)) \mid \text{ord}(g)$. I sottogruppi vengono mandati in sottogruppi come chiarito dalla seguente proposizione

Proposizione 4.15 Sia $G \xrightarrow{f} H$ un omomorfismo di gruppi. Se G' è un sottogruppo di G , allora $f(G')$ è un sottogruppo di H e se H' è un sottogruppo di H , $f^{-1}(H')$ è un sottogruppo di G .

In particolare, l'immagine $f(G)$ di f è un sottogruppo di H ; essa viene detta *immagine omomorfa* di G . L'immagine inversa del sottogruppo banale $\{e_H\}$ di H ha un'importanza fondamentale, essa è il *nucleo* di f , indicato con $\text{Ker}(f)$; in altri termini

$$\text{Ker}(f) = \{g \in G \mid f(g) = e_H\}.$$

Il nucleo misura quanto un omomorfismo non è iniettivo, abbiamo infatti

Proposizione 4.16 Il nucleo di un omomorfismo è un sottogruppo normale di G . Inoltre, per ogni h in $\text{Im}(f)$ si ha $f^{-1}(h) = g \text{Ker}(f)$ con g un qualsiasi elemento di $f^{-1}(h)$. In particolare, f è iniettivo se e solo se $\text{Ker}(f)$ è banale.

Non solo il nucleo di un omomorfismo è un sottogruppo normale, ma ogni sottogruppo normale è il nucleo di un omomorfismo: infatti, se H è normale in G , allora H è il nucleo dell'omomorfismo di proiezione al quoziente $G \rightarrow G/H$. Riportiamo questa osservazione nella seguente

Proposizione 4.17 Un sottogruppo di un gruppo è normale se e solo se è il nucleo di un omomorfismo.

Il risultato fondamentale sugli omomorfismi di gruppi è il seguente

Teorema 4.18 (di Omomorfismo) Se $G \xrightarrow{f} H$ è un omomorfismo e $G \xrightarrow{\pi} G/\text{Ker}(f)$ è l'omomorfismo quoziente, allora esiste un omomorfismo, necessariamente iniettivo, \overline{f} che rende commutativo il diagramma

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow \overline{f} & \\ G/\text{Ker}(f) & & \end{array}$$

Un omomorfismo biiettivo si chiama *isomorfismo*; se esiste un isomorfismo tra G e H diciamo che i due gruppi sono *isomorfi* e scriviamo $G \simeq H$. In particolare, dal teorema precedente abbiamo

Corollario 4.19 Se f è suriettivo, \overline{f} è un isomorfismo tra $G/\text{Ker}(f)$ e H .

Questo corollario ci permette di concludere che le immagini omomorfe del gruppo G sono tutte quozienti di G e possono quindi essere costruite usando solo G . Inoltre ogni omomorfismo $f : G \rightarrow H$ può essere fattorizzato nel seguente modo: l'omomorfismo di proiezione $\pi : G \rightarrow G/\text{Ker}(f)$, seguito dall'isomorfismo $\bar{f} : G/\text{Ker}(f) \rightarrow \text{Im}(f)$ e infine dall'inclusione $\text{Im}(f) \hookrightarrow H$; abbiamo cioè il diagramma commutativo

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & & \uparrow i \\ G/\text{Ker}(f) & \xrightarrow[\sim]{\bar{f}} & \text{Im}(f) \end{array}$$

Sia G un gruppo, chiamiamo *automorfismo* ogni isomorfismo di G con se stesso e indichiamo con $\text{Aut}(G)$ l'insieme degli automorfismi di G . È chiaro che l'identità è un automorfismo, che la composizione di due automorfismi è ancora un automorfismo e che l'inverso di un automorfismo è un automorfismo, quindi $\text{Aut}(G)$ è un gruppo con la composizione di applicazioni.

L'omomorfismo di passaggio al quoziente π associato ad un sottogruppo normale H di G ci permette di precisare il contenuto della Proposizione 4.15.

Proposizione 4.20 *L'insieme dei sottogruppi di G/H è in corrispondenza biunivoca con l'insieme dei sottogruppi di G che contengono H . In particolare le applicazioni $K' \mapsto \pi^{-1}(K')$ e $G' \mapsto \pi(G')$ realizzano questa corrispondenza. Inoltre a sottogruppi normali di G/H corrispondono sottogruppi normali di G .*

Possiamo ora dedurre facilmente la struttura dei gruppi ciclici. Basta infatti osservare che se $G = \langle g \rangle$ è un gruppo ciclico allora $\mathbb{Z} \ni k \mapsto g^k \in G$ è un omomorfismo suriettivo. Applicando quanto visto a questo omomorfismo abbiamo

Teorema 4.21 (di Struttura dei Gruppi Ciclici) *Sia G un gruppo ciclico, se G è infinito allora $G \simeq \mathbb{Z}$ mentre, se $|G|$ ha ordine finito n allora $G \simeq \mathbb{Z}/n\mathbb{Z}$. Inoltre se $G = \langle g \rangle$ è infinito, i suoi sottogruppi sono $\langle g^k \rangle$ al variare di k tra gli interi positivi. Mentre se $|G| = n < \infty$, allora G ha un solo sottogruppo di ordine d per ogni divisore d di n .*

Si noti che la seconda parte sui sottogruppi nel caso di ordine finito è una conseguenza della corrispondenza tra sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ e sottogruppi di \mathbb{Z} che contengono $n\mathbb{Z}$; abbiamo cioè un'altra dimostrazione dell'Osservazione 4.6.

Sappiamo che, per gruppi finiti, l'ordine di un elemento divide l'ordine di un gruppo. Non è però vero che, in generale, per ogni divisore d dell'ordine di G esista un elemento di ordine d in G . Nel caso particolare di un divisore primo, ciò è vero e, per i gruppi abeliani, può essere dimostrato, ad esempio, usando il Teorema di Omomorfismo e una facile induzione.

Teorema 4.22 (di Cauchy) *Sia G è un gruppo finito e p un primo che divide l'ordine di G , allora in G esiste un elemento di ordine p .*

Anche l'ordine di un sottogruppo divide l'ordine di un gruppo; ma, come per gli elementi, non è vero che per ogni divisore dell'ordine di un gruppo esiste un sottogruppo di ordine il divisore. Sappiamo, invece, che un gruppo ciclico ha esattamente un sottogruppo per ogni divisore dell'ordine; questa situazione è molto speciale e anzi

Osservazione 4.23 *Se G è un gruppo finito con esattamente un sottogruppo di ordine d per ogni divisore d di $|G|$, allora G è ciclico.*

1.4.8 Prodotto diretto di gruppi

Dati due gruppi G e H con rispettive operazioni \cdot e \circ , possiamo definire un'operazione sul prodotto cartesiano $G \times H$ ponendo $(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$ per ogni $g_1, g_2 \in G$ e $h_1, h_2 \in H$. È molto facile provare che con questa operazione $G \times H$ è un gruppo, detto il *prodotto diretto* dei gruppi G e H .

Come vedremo le proprietà del prodotto diretto $G \times H$ sono in semplice relazione con le proprietà dei gruppi G e H . Troveremo spesso che un gruppo, definito in un qualche modo, risulta essere isomorfo al prodotto diretto di altri gruppi, ricaveremo così dai fattori le proprietà del gruppo a cui siamo interessati.

L'insieme $G \times H$ ha cardinalità il prodotto delle cardinalità di G e di H : se G e H hanno ordine finito allora $G \times H$ ha ordine $|G| \cdot |H|$ mentre, se anche uno solo dei due gruppi è infinito allora anche $G \times H$ è infinito. Per gli ordine degli elementi abbiamo la seguente

Osservazione 4.24 *Se gli elementi $g \in G$ e $h \in H$ hanno ordini finiti rispettivamente m e n , allora l'ordine dell'elemento (g, h) in $G \times H$ è il minimo comune multiplo di m e n .*

Anche il centro di $G \times H$ è semplicemente descritto, si verifica subito infatti che $Z(G \times H) = Z(G) \times Z(H)$. In particolare

Osservazione 4.25 *Il gruppo $G \times H$ è abeliano se e solo se G e H sono entrambi abeliani.*

Se G' è un sottogruppo di G e H' un sottogruppo di H , il gruppo $G' \times H'$ è in modo naturale un sottogruppo di $G \times H$; ma si noti che *non* tutti i sottogruppi di $G \times H$ sono prodotti diretti di sottogruppi. Ad esempio il sottogruppo diagonale $\{(g, g) \mid g \in G\}$ non è prodotto diretto di sottogruppi non appena G ha più di un elemento.

Vediamo ora un'applicazione dell'osservazione precedente sull'ordine degli elementi di un prodotto. Troviamo subito

Osservazione 4.26 *Un prodotto diretto di gruppi ciclici finiti, di ordini m e n rispettivamente, è ciclico se e solo se m e n sono primi tra loro.*

In particolare per i gruppi ciclici delle classi di resto $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$ abbiamo che l'omomorfismo

$$\mathbb{Z}/mn\mathbb{Z} \ni [a]_{mn} \longmapsto ([a]_m, [a]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

è un isomorfismo se e solo se m e n sono primi tra loro. Inoltre possiamo restringere questo omomorfismo a $(\mathbb{Z}/mn\mathbb{Z})^*$ e ottenere un omomorfismo tra le strutture moltiplicative

$$(\mathbb{Z}/mn\mathbb{Z})^* \ni [a]_{mn} \longmapsto ([a]_m, [a]_n) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*;$$

anche in questo caso abbiamo un isomorfismo se e solo se m e n sono primi tra loro. Si noti che, in questo modo, abbiamo precisato il contenuto del Teorema 3.18 e del relativo Corollario 3.19.

1.5 Gli anelli

1.5.1 Definizione e prime proprietà

Gli anelli sono insiemi con due operazioni le cui proprietà sono modellate su quelle dell'addizione e della moltiplicazione tra interi: un insieme A con due operazioni $+$ e \cdot si dice *anello* se

- (i) A è un gruppo abeliano con l'operazione $+$,
- (ii) l'operazione \cdot è associativa,
- (iii) l'operazione \cdot è distributiva rispetto a $+$.

Chiamiamo l'operazione $+$ *addizione* e l'operazione \cdot *moltiplicazione*. L'elemento neutro per l'addizione è indicato con 0 , chiamato *zero* dell'anello A . Si noti, invece, che non è detto che esista un elemento neutro per \cdot , se ciò accade allora diciamo che l'anello è *con unità* o *unitario*, l'unità è allora unica e verrà indicata con 1 , detta *uno* dell'anello. Si noti che può ben succedere che $0 = 1$, ma allora è facile provare che $A = \{0\}$, tale anello si chiama l'anello *nullo*. Se la moltiplicazione è un'operazione commutativa per A allora l'anello si dice *commutativo*.

Le elementari regole di calcolo degli interi continuano a valere in un anello qualsiasi, abbiamo infatti

Osservazione 5.1 *Sia A un anello, allora per ogni a e b in A si ha: $a0 = 0a = 0$, $a(-b) = (-a)b = -(ab)$, $(-a)(-b) = ab$. Se inoltre, A è unitario allora $(-1)a = -a$ e $(-1)(-1) = 1$.*

Il primo esempio di anello è ovviamente \mathbb{Z} , un anello commutativo unitario. Grazie al Teorema 3.17 anche le classi di resto $\mathbb{Z}/n\mathbb{Z}$ modulo un intero positivo n sono un anello commutativo unitario, $0 + n\mathbb{Z}$ è lo zero e $1 + n\mathbb{Z}$ è l'uno.

Un elemento a di un anello A è detto *divisore dello zero* se esiste un elemento $b \neq 0$ in A per cui $ab = 0$. Indichiamo l'insieme dei divisori dello zero dell'anello A con $D(A)$. Ovviamente zero è un divisore dello zero in ogni anello non nullo. Un anello che non ha divisori dello zero oltre a 0 è detto *dominio d'integrità*. Gli interi sono un dominio di integrità mentre $\mathbb{Z}/n\mathbb{Z}$ è un dominio di integrità se e solo se n è un primo. Infatti, grazie alla Proposizione 3.11 i divisori di zero sono le classi $a + n\mathbb{Z}$ con $(a, n) \neq 1$.

Un elemento a di un anello è *nilpotente* se esiste un intero positivo k per cui $a^k = 0$. Ad esempio, se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ è la fattorizzazione di n in primi distinti, allora una classe \bar{a} in $\mathbb{Z}/n\mathbb{Z}$ è nilpotente se e solo se $p_1 p_2 \cdots p_r$ divide a in \mathbb{Z} ; si veda l'Esercizio Preliminare 14.

Useremo spesso in seguito il contenuto della seguente osservazione, di fatto equivalente alla definizione di dominio di integrità.

Osservazione 5.2 (Legge dell'Annullamento del Prodotto) *Siano a, b due elementi di un dominio di integrità, se $ab = 0$ allora $a = 0$ o $b = 0$.*

Un elemento a di un anello unitario A è *invertibile* se esiste un elemento $b \in A$ per cui $ab = ba = 1$; indichiamo con A^* l'insieme degli elementi invertibili di A . Per l'anello \mathbb{Z} abbiamo $\mathbb{Z}^* = \{1, -1\}$; anche \mathbb{Q} , \mathbb{R} e \mathbb{C} sono anelli commutativi unitari e si ha $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ e $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. È una conseguenza immediata della Proposizione 3.15 che la classe $a + n\mathbb{Z}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se solo se $(a, n) = 1$.

Osservazione 5.3 *Se A è unitario allora l'insieme A^* degli elementi invertibili è un gruppo con la moltiplicazione, abeliano se A è commutativo. Inoltre, in ogni caso, $A^* \cap D(A) = \emptyset$.*

Per un anello finito vale di più

Osservazione 5.4 *Se A è un anello unitario finito allora $A = A^* \sqcup D(A)$; cioè ogni elemento è o invertibile o un divisore di zero.*

Se \mathbb{K} è un anello commutativo non nullo con unità per cui tutti gli elementi non nulli sono invertibili, diciamo che \mathbb{K} è un *campo*. In altre parole, $\mathbb{K} \neq \{0\}$ è un campo se e solo se $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$; inoltre, in tal caso, questo insieme è un gruppo abeliano con l'operazione di moltiplicazione. Osserviamo che ogni campo è un dominio di integrità e quindi nei campi vale la Legge dell'Annullamento del Prodotto. Esempi di campi sono \mathbb{Q} , \mathbb{R} e \mathbb{C} . Possiamo però anche costruire campi con un numero finito di elementi, infatti, se p è un numero primo allora $\mathbb{Z}/p\mathbb{Z}$ è un campo in quanto, come osservato in precedenza, ogni classe non nulla è invertibile modulo p .

In un anello commutativo il calcolo delle potenze di un binomio è simile a quello per i binomi di numeri.

Osservazione 5.5 (Binomio di Newton) *Se a e b sono due elementi di un anello commutativo A , allora per ogni intero positivo n vale*

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

1.5.2 Sottoanelli, ideali e quozienti

Un sottoinsieme B di un anello A è detto *sottoanello* se le operazioni $+$ e \cdot possono essere ristrette a B e se con queste operazioni ristrette B è un anello. È chiaro che per controllare che un sottoinsieme non vuoto B è un sottoanello basta controllare che $b_1 + b_2$ e $b_1 \cdot b_2$ siano elementi di B per ogni b_1 e b_2 di B e che $-b \in B$ per ogni $b \in B$. Equivalentemente un sottoinsieme B è un sottoanello se è un sottogruppo per l'addizione e se è chiuso per la moltiplicazione.

Sia ora A' un anello contenente l'anello A e sia X un sottoinsieme di A' . È chiaro che l'intersezione di un numero qualunque di sottoanelli di A' è ancora un sottoanello. Possiamo quindi definire l'anello *generato* da X su A come l'intersezione di tutti i sottoanelli di A' che contengono $A \cup X$; indichiamo tale anello con $A[X]$, esso è il più piccolo sottoanello di A' che contiene $A \cup X$. Per un anello commutativo A è facile provare che $A[X]$ è l'insieme di tutte le somme

$$a_1 y_1 + a_2 y_2 + \cdots + a_k y_k$$

al variare di k nei naturali, a_1, a_2, \dots, a_k in A e y_1, y_2, \dots, y_r tra i possibili prodotti di elementi di X . Se l'insieme X è finito, diciamo $X = \{x_1, x_2, \dots, x_r\}$, scriviamo $A[x_1, x_2, \dots, x_r]$ per $A[X]$. In particolare se $X = \{x\}$ e A è commutativo, allora $A[x]$ è l'insieme di tutte le somme

$$\sum_{h=0}^k a_h x^h$$

al variare di k nei naturali e a_0, a_1, \dots, a_k in A .

Un *omomorfismo* di anelli è un'applicazione $A \xrightarrow{f} B$ tra due anelli A e B con la proprietà: $f(a_1 + a_2) = f(a_1) + f(a_2)$ e $f(a_1 a_2) = f(a_1) f(a_2)$ per ogni $a_1, a_2 \in A$. Inoltre, se A e B sono unitari allora richiediamo che un omomorfismo f mandi l'unità 1_A di A nell'unità 1_B di B , cioè $f(1_A) = 1_B$. Un *isomorfismo* di anelli è un omomorfismo biiettivo di anelli; come per i gruppi scriviamo $A \simeq B$ se esiste un isomorfismo da A in B e diciamo che A e B sono *isomorfi*.

Se A è un anello commutativo unitario allora vi è un solo modo di estendere l'assegnazione $\mathbb{Z} \ni 1 \mapsto 1_A \in A$ ad un omomorfismo di anelli. In particolare possiamo pensare ai numeri interi come ad elementi di A ; si noti però che questo omomorfismo non è iniettivo in generale.

Un omomorfismo di anelli è anche un omomorfismo tra i gruppi additivi $(A, +)$ e $(B, +)$. Possiamo quindi definire il *nucleo* $\text{Ker}(f)$ di un omomorfismo di anelli f come il nucleo dell'omomorfismo tra i gruppi additivi, cioè $\text{Ker}(f)$ è l'insieme degli elementi di A che vengono mandati in 0_B da f

$$\text{Ker}(f) = \{a \in A \mid f(a) = 0_B\}.$$

Non solo $\text{Ker}(f)$ è un sottoanello di A , ma vale anche $a_1 \cdot a_2 \in \text{Ker}(f)$ se a_1 o a_2 sono in $\text{Ker}(f)$, diciamo che $\text{Ker}(f)$ *assorbe* rispetto alla moltiplicazione. In generale, un qualsiasi sottogruppo additivo I di A che assorba rispetto alla moltiplicazione è detto *ideale*.

Un ideale è per un anello quello che un sottogruppo normale è per un gruppo. Infatti, essendo $(A, +)$ un gruppo abeliano, un ideale I è un sottogruppo normale rispetto a $+$. Inoltre se consideriamo l'insieme quoziente A/I delle classi laterali $a + I$ dell'ideale I rispetto all'addizione, al variare di a in A ,

$$A/I = \{a + I \mid a \in A\},$$

esso non solo è un gruppo abeliano con l'addizione delle classi indotta da $+$ in A , ma, ponendo $(a_1 + I) \cdot (a_2 + I) = a_1 a_2 + I$ definiamo una moltiplicazione che rende A/I un anello. In altre parole, se I è un ideale di A allora le operazioni $+$ e \cdot di A passano all'insieme quoziente A/I e rendono tale insieme un anello. Abbiamo che l'applicazione di passaggio al quoziente

$$A \ni a \longmapsto a + I \in A/I$$

è un omomorfismo suriettivo. Quindi, analogamente ai gruppi, gli ideali sono esattamente i nuclei degli omomorfismi.

Vediamo ora un'altra definizione che, nel seguito, si dimostrerà estremamente importante: un ideale $M \neq A$ è detto *massimale* se non è contenuto propriamente in nessun ideale diverso da A .

Sia A un anello e X un suo sottoinsieme. Definiamo l'ideale *generato* da X come l'intersezione di tutti gli ideali di A che contengono X , indichiamo tale ideale con (X) , esso è il più piccolo ideale di A che contiene X . Per un anello commutativo A , l'ideale X è l'insieme di tutte le somme

$$a_1 x_1 + a_2 x_2 + \cdots + a_k x_k$$

al variare di k nei naturali, a_1, a_2, \dots, a_k in A e x_1, x_2, \dots, x_k in X . Se l'insieme X è finito, diciamo $X = \{x_1, x_2, \dots, x_r\}$, scriviamo (x_1, x_2, \dots, x_r) per (X) . In particolare, se $X = \{x\}$ e A è commutativo, allora l'ideale (x) generato da x è il sottoinsieme $A \cdot x$ di A di tutti i multipli ax con $a \in A$.

1.5.3 Anelli di polinomi

Vediamo ora la definizione di polinomio a coefficienti in un anello commutativo A . Per non appesantire la trattazione, introducendo ad esempio il linguaggio delle

successioni definitivamente nulle, scegliamo di non essere completamente formali; ci accontentiamo di un minore livello di rigore confidando che il lettore abbia già un'idea intuitiva di cosa siano i polinomi.

Sia x un simbolo, che chiamiamo *indeterminata*; consideriamo inoltre i simboli $1 = x^0, x = x^1, x^2, x^3, \dots$ che chiamiamo *potenze* dell'indeterminata. Se n è un naturale e $a_0, a_1, a_2, \dots, a_n$ sono elementi dell'anello A , la somma formale

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

è detta *polinomio* nell'indeterminata x con *coefficienti* a_0, a_1, \dots, a_n nell'anello A . Per comodità di linguaggio, pensiamo che $f(x)$ abbia i coefficienti a_{n+1}, a_{n+2}, \dots tutti nulli. Il coefficiente a_0 è detto il *termine noto* del polinomio. Il polinomio *nullo*, indicato con 0 si ottiene scegliendo $n = 0$ e $a_0 = 0$; esso ha quindi tutti i coefficienti nulli. Due polinomi $a_0 + a_1x + \dots + a_nx^n$ sono *uguali* se hanno i coefficienti corrispondentemente uguali, cioè se $a_0 = b_0, a_1 = b_1$ e così via.

Dato un polinomio $f(x) = a_0 + a_1x + \dots + a_nx^n$ non nullo, chiamiamo *grado* di $f(x)$, indicato con $\deg(f)$, il più piccolo intero r per cui i coefficienti a_{r+1}, a_{r+2}, \dots sono tutti nulli. Sottolineiamo che non assegniamo alcun grado al polinomio nullo. Per un polinomio di grado r , il coefficiente a_r si chiama *coefficiente direttore* di $f(x)$. Se A è unitario, un polinomio *monico* è un polinomio con coefficiente direttore 1 . Un polinomio *costante* è un polinomio nullo o di grado 1 , quindi $f(x)$ è costante se e solo se $f(x) = a_0$, con $a_0 \in A$.

L'insieme dei polinomi a coefficienti in A e nell'indeterminata x è indicato con $A[x]$. Vediamo ora come usare le operazioni dell'anello A per definire un'addizione e una moltiplicazione che rendano $A[x]$ un anello. Se $f(x) = a_0 + a_1x + a_2x^2 + \dots$ e $g(x) = b_0 + b_1x + b_2x^2 + \dots$ sono polinomi allora definiamo l'addizione di $f(x)$ e $g(x)$ come

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$$

È facile verificare che con questa operazione $A[x]$ è un gruppo abeliano, l'elemento neutro è il polinomio nullo e l'opposto di $a_0 + a_1x + a_2x^2 + \dots$ è il polinomio $-a_0 - a_1x - a_2x^2 - \dots$.

Per la moltiplicazione cominciamo definendo il prodotto tra potenze della indeterminata: $x^n \cdot x^m = x^{n+m}$ per ogni n e m naturali. Estendiamo poi questa operazione ai polinomi *per bilinearità*: se $f(x)$ e $g(x)$ sono i polinomi introdotti sopra poniamo

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1x + a_2x^2 + \dots) \cdot (b_0 + b_1x + b_2x^2 + \dots) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots \\ &= \sum_k \left(\sum_{h=0}^k a_h b_{k-h} \right) x^k. \end{aligned}$$

È molto facile provare che l'operazione così definita è commutativa e associativa e, se A è unitario, allora il polinomio 1 è l'elemento neutro per il prodotto. Inoltre,

come è chiaro dalla stessa definizione di prodotto, la moltiplicazione è distributiva rispetto alla somma. Abbiamo quindi

Proposizione 5.6 *Dato un anello commutativo A , l'insieme $A[x]$ dei polinomi a coefficienti in A è un anello commutativo. Se inoltre A è unitario allora anche $A[x]$ lo è.*

Il grado dei polinomi ha due importanti proprietà rispetto all'addizione e alla moltiplicazione

Osservazione 5.7 *Siano $f(x)$ e $g(x)$ due polinomi non nulli in $A[x]$, valgono*

(i) *se $f(x) + g(x)$ non è il polinomio nullo allora*

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\},$$

(ii) *se A è un dominio di integrità allora $\deg(f \cdot g) = \deg(f) + \deg(g)$; in particolare $A[x]$ è un dominio di integrità.*

Possiamo subito ricavare da ciò gli elementi invertibili

Corollario 5.8 *Se A è un dominio di integrità allora $A[x]^* = A^*$.*

Nel seguito useremo spesso la valutazione di un polinomio in un elemento, precisiamo ora cosa intendiamo con questo. Sia a un fissato elemento di A . Esiste allora un unico omomorfismo di anelli

$$A[x] \ni f(x) \xrightarrow{v_a} f(a) \in A$$

detto, *valutazione* in a , ottenuto sostituendo ogni occorrenza di x in $f(x)$ con a . Una *radice* di $f(x)$ è un elemento a di A per cui $f(a) = 0$. È chiaro che se A è un sottoanello di B allora $A[x]$ è un sottoanello di $B[x]$, possiamo quindi valutare i polinomi di $A[x]$ anche negli elementi di B . In particolare possiamo cercare le radici di un polinomio in un anello più grande dell'anello dei coefficienti. È inoltre chiaro che l'immagine di $A[x]$ in B attraverso la mappa di valutazione in a è il sottoanello $A[a]$ di B generato da a su A .

Se abbiamo un omomorfismo tra anelli $A \xrightarrow{f} B$ possiamo indurre una mappa tra i rispettivi anelli di polinomi ponendo

$$A[x] \ni a_0 + a_1x + \cdots + a_nx^n \longmapsto f(a_0) + f(a_1)x + \cdots + f(a_n)x^n \in B[x].$$

Segue subito dalla definizione delle operazioni sui polinomi che questa mappa è un omomorfismo di anelli. Osserviamo che questo omomorfismo non aumenta il grado dei polinomi e, in particolare, se il coefficiente direttore a_n di $f(x)$ non è nel nucleo di f , allora l'omomorfismo mantiene il grado di $f(x)$.

Esercizi scelti di Algebra

Volume 1

Chirivì, R.; Del Corso, I.; Dvornicich, R.
2017, XII, 230 pagg. 1 figg., Softcover
ISBN: 978-88-470-3960-5