APPUNTI DI ALGEBRA PER IL CORSO DI ALGEBRA E GEOMETRIA

LUCIA ALESSANDRINI

1. Numeri

1.1 I numeri naturali. Indichiamo con $\mathbb{N}$ l'insieme dei numeri naturali:

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

Questi numeri, le operazioni di somma e di prodotto e la relazione $>$ "maggiore di"sono ben conosciuti fin dalla scuola primaria. Tuttavia se si cerca di darne una definizione matematicamente corretta, si scopre che ciò non è semplice, anche perché i numeri naturali possono essere considerati sotto vari punti di vista, principalmente come numeri cardinali (che rispondono alla domanda: quanti sono?) e come numeri ordinali (primo, secondo, ...), e non da ultimo come etichette (potrebbero essere rimpiazzati da altri simboli, e non si considerano le operazioni: per esempio, i numeri di telefono).

La piú importante proprietà di $\mathbb{N}$ è la seguente:

1.2 Assioma del buon ordinamento. Ogni sottoinsieme non vuoto di $\mathbb{N}$ ha un elemento minimo. Ovvero,

sia $S \subseteq \mathbb{N}, S \neq \emptyset$: allora esiste $m \in S$ tale che $\forall s \in S,\ m \leq s$.

Da questo assioma deriva il

1.3 Principio di induzione. Consideriamo, per ogni numero naturale n, un'asserzione $A(n)$ ad esso associata. Se valgono queste due ipotesi:

a) $A(0)$ è vera;

b) $\forall n \in \mathbb{N}$, supposta vera $A(n)$, ne segue che è vera $A(n+1)$;

allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.

La necessità di avere l'opposto di ogni numero, ovvero di poter "fare la sottrazione", rende opportuno ampliare l'insieme dei numeri da $\mathbb{N}$ a $\mathbb{Z}$.

1.4 I numeri interi. Indichiamo con $\mathbb{Z}$ l'insieme dei numeri interi:

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

Dunque $\mathbb{N} \subset \mathbb{Z}$. Dalla scuola secondaria, si sa come addizionare, sottrarre e moltiplicare numeri interi (invece, per quanto riguarda la divisione, se $a, b \in \mathbb{Z}$, diversi da zero, non è detto che a diviso b stia in $\mathbb{Z}$: c'è bisogno

quindi di un nuovo ampliamento dell'insieme dei numeri, con le frazioni). Qui studieremo invece la cosiddetta "divisione con resto".

1.5 Teorema (Divisione con resto). Siano $a, b \in \mathbb{Z}$ con $b > 0$. Allora esistono e sono unici due interi, il quoziente q e il resto r, tali che

$$a = qb + r, \quad 0 \leq r < b.$$

Scriveremo $a : b = q$ con resto r.

Dimostrazione (dell'esistenza). Consideriamo l'insieme $A = \{a - xb / \ x \in \mathbb{Z}\}$. Prendendo, per esempio, $x = 0$ se $a \geq 0$ e $x = a$ se a è negativo, si vede che A contiene elementi non negativi: questo significa che l'insieme $A \cap \mathbb{N}$ non è vuoto.

Per l'assioma del buon ordinamento, esso contiene un elemento minimo r con $0 \leq r = a - xb$ per un certo $x \in \mathbb{Z}$. Ponendo $q = x$, abbiamo trovato $a = qb + r, \ 0 \leq r$. Vale anche $r < b$, perché se per assurdo fosse $r \geq b$, il numero $r - b \in A \cap \mathbb{N}$, mentre sappiamo che il minimo è r.

Esercizio. Trovare quoziente e resto delle divisioni $1000 : 38$, $38 : 1000$ e $-1000 : 38$.

1.6 Definizione. Siano $d, b \in \mathbb{Z}$. Diremo che d divide b, o che d è un divisore di b, o che b è un multiplo di d, o che b è divisibile per d, e scriveremo $d|b$, se esiste $c \in \mathbb{Z}$ tale che $b = dc$.

Esempi. 3 divide 15, ma anche $(-3)|15, (-3)|(-15)$. Ogni intero d divide 0, ma 0 non divide alcun numero, eccetto se stesso. 1 è un divisore di ogni numero.

1.7 Osservazioni.

(1) Ogni numero intero $n \neq 0$ ha almeno quattro divisori: $\pm 1, \pm n$.
(2) Se d divide sia a che b, allora divide $a \pm b$.
(3) Se d divide $a \neq 0$, allora $|d| \leq |a|$.

Grazie all'ultima delle precedenti osservazioni, possiamo porre la seguente definizione:

1.8 Definizione. Siano $a, b \in \mathbb{Z}$, non entrambi nulli. Il loro massimo comun divisore $MCD(a, b)$ è il più grande intero che divide sia a che b. Definiamo inoltre $MCD(0, 0) = 0$.

1.9 Osservazioni.

(1) Se $(a, b) \neq (0, 0)$, $MCD(a, b) > 0$.
(2) $MCD(a, 0) = |a|$, il più grande intero che divide a, e $MCD(a, a) = |a|$.
(3) $MCD(a, b) = MCD(b, a), \ MCD(-a, b) = MCD(a, b)$.

1.10 Proposizione. Siano $a, b \in \mathbb{Z}$: per ogni $q \in \mathbb{Z}$, $MCD(a, b + qa) = MCD(a, b)$.

Dimostrazione. Sia $q \in \mathbb{Z}$. Se d divide sia a che b, allora divide $b + qa$. Viceversa, se d divide sia a che $b+qa$, allora divide $b = (b+qa)-qa$. Dunque l'insieme dei divisori comuni di a e b è uguale all'insieme dei divisori comuni di a e $b + qa$. Perciò anche il massimo è lo stesso.

1.11 Teorema. Siano $a, b \in \mathbb{Z}$, non entrambi nulli. Allora il massimo comun divisore di a e b è il piú piccolo elemento positivo dell'insieme $A = \{ax + by/\ x, y \in \mathbb{Z}\}$.

1.12 Corollari. Siano $a, b \in \mathbb{Z}$.

(1) Esistono $x, y \in \mathbb{Z}$ tali che $MCD(a, b) = ax + by$.
(2) Se d divide sia a che b, allora $d|MCD(a, b)$.
(3) Se $MCD(a, b) = 1$ (in questo caso a e b si dicono *primi tra loro*) e $a|bc$, allora $a|c$.

Dimostrazione di (3). Per (1), esistono $x, y \in \mathbb{Z}$ tali che $1 = ax + by$, dunque $c = cax + bcy$. Ma per ipotesi esiste m tale che $am = bc$, perciò $c = cax + amy = a(cx + my)$.

1.13 Definizione. Un intero positivo p si dice *numero primo* se ha esattamente due divisori positivi, 1 e p.

Esempi. 1 non è primo; 2, 3, 5, 7, 11, 13, 17 sono numeri primi.

1.14 Proposizione. Siano $a, b \in \mathbb{Z}$, e p un numero primo. Se $p|ab$, allora $p|a$ oppure $p|b$.

Dimostrazione. Facciamo vedere che, se p non divide a, allora $p|b$. Ovviamente $MCD(a, p)$ divide sia a che p; essendo p primo, $MCD(a, p)$ è 1 oppure p. Non può essere p, poiché p non divide a, perciò è $MCD(a, p) = 1$ e si conclude dal Corollario 1.12 (3).

1.15 Teorema (Teorema fondamentale dell'aritmetica). Per ogni intero $n > 1$ esistono k numeri primi $p_1, \ldots, p_k$ tali che

$$n = p_1 \cdot \cdots \cdot p_k.$$

I numeri primi $p_1, \ldots, p_k$ sono unici a meno dell'ordine; chiamiamo la formula precedente la *decomposizione di n in fattori primi.*

Dimostrazione (dell'esistenza). Se per assurdo non esistesse questa decomposizione per ogni numero naturale maggiore di 1, ci sarebbe un minimo naturale $n > 1$ senza decomposizione. n non può essere primo, perché la decomposizione per i numeri primi è $p = p$. Allora n ha divisori positivi e si può scrivere $n = ab$ con a, b numeri maggiori di 1 e minori di n.

Ma per la minimalità di n, a e b devono ammettere la decomposizione in fattori primi, e allora la ammette anche $n = ab$.

Per poter considerare questa decomposizione in fattori primi per ogni $n \in \mathbb{Z},\ n \neq 0$, poniamo per convenzione che la decomposizione di 1 è 1=1. Per i numeri negativi, si applica la decomposizione precedente a $-n$.

1.16 Corollario. I numeri primi sono infiniti.

Dimostrazione. Se fossero in numero finito k, ovvero se $p_1, \ldots, p_k$ fossero tutti i numeri primi, denotiamo con a il loro prodotto, e sia $b = a+1$. Allora $MCD(a, b) = 1$, poiché $1 = b-a = 1b+(-1)a$ e si può usare il Teorema 1.11. Dunque b non potrebbe avere la decomposizione in fattori primi, altrimenti avrebbe almeno un fattore primo in comune con a, e perciò $MCD(a, b) > 1$: ma questo è assurdo.

1.17 Definizione. Sia a un intero positivo, e p un primo; allora $ord_p(a)$ indica il numero dei fattori p che compaiono nella decomposizione di a. Se a è un intero negativo, definiamo $ord_p(a) = ord_p(-a)$, mentre $ord_p(0)$ non è definito.

Ne segue che per ogni $a \neq 0$, $ord_p(a)$ è un numero non negativo; se p non divide a, allora $ord_p(a) = 0$. Inoltre, per ogni $a > 0$, vale

$$a = \prod_p p^{ord_p(a)}.$$

Tutti i numeri primi sono presenti nel prodotto, ma soltanto per un numero finito di essi (quelli che effettivamente sono presenti nella decomposizione di a) l'esponente è positivo. Analogamente, per ogni $a < 0$, vale $a = -\prod_p p^{ord_p(a)}$.

1.18 Osservazioni. Siano a e b due interi non nulli. Allora:

(1) Per ogni primo p si ha $ord_p(ab) = ord_p(a) + ord_p(b)$.
(2) Un intero $d \neq 0$ divide a se e solo se $ord_p(d) \leq ord_p(a)$ per ogni primo p.
(3) $MCD(a, b) = \prod_p p^{min(ord_p(a), ord_p(b))}$.

1.19 Definizione. Siano a e b due interi non nulli. Allora il minimo comune multiplo di a e b, $mcm(a, b)$, è il piú piccolo intero positivo m tale che $a|m,\ b|m$.

1.20 Osservazioni. Siano a e b due interi non nulli. Allora:

(1) $mcm(a, b) = \prod_p p^{max(ord_p(a), ord_p(b))}$.
(2) $mcm(a, b) \cdot MCD(a, b) = |ab|$.

1.21 Algoritmo di Euclide. Diamo un algoritmo per calcolare il massimo comun divisore di due interi. Siano $a, b \in \mathbb{Z}$, dalle osservazioni 1.9 possiamo limitarci a studiare il caso $a > b > 0$. Definiamo i resti $r_0, r_1, r_2, \ldots$ (ci fermiamo appena otteniamo zero) come i seguenti numeri naturali:

$r_0 = a, r_1 = b, \ldots, r_{k+1} =$ il resto della divisione dei due precedenti (utilizziamo il Teorema 1.5). In questo modo si ha, per ogni $k > 0$,

$$r_{k-1} = q_k r_k + r_{k+1}, \quad 0 \leq r_{k+1} < r_k.$$

Ne risulta che $r_0 > r_1 > r_2 > \ldots$ dunque ad un certo punto si deve arrivare a $r_s = 0$. Allora $MCD(a, b) = r_{s-1}$.

Infatti dalla scrittura precedente, utilizzando la Proposizione 1.10, risulta $MCD(r_k, r_{k-1}) = MCD(r_k, r_{k+1})$. Dunque

$$MCD(a, b) = MCD(r_0, r_1) = MCD(r_1, r_2) = \ldots$$
$$= MCD(r_{s-1}, r_s) = MCD(r_{s-1}, 0) = r_{s-1}.$$

1.22 Esercizi.

a) Verificare con l'algoritmo di Euclide che $MCD(7007, 1991) = 11$ (la successione dei resti r_k è: $7007 > 1991 > 1034 > 957 > 77 > 33 > 11 > 0$.)

b) Calcolare $MCD(10001, 6497)$.

c) Calcolare MCD e mcm dei numeri $a =$ dieci miliardi, $b = 2^5 \cdot 91$.

d) Sia $n \in \mathbb{N}^*$, e siano $a, b \in \mathbb{Z}$ due interi non nulli. Mostrare che $MCD(an, bn) = nMCD(a, b)$.

e) Siano $a, b \in \mathbb{Z}$, non entrambi nulli. Mostrare che $MCD(a, b) = 1$ se e solo se esistono $x, y \in \mathbb{Z}$ tali che $ax + by = 1$.

f) Siano $a, b, c \in \mathbb{Z}$ interi non nulli. Mostrare che se $MCD(a, b) = 1$, $MCD(a, c) = 1$, allora $MCD(a, bc) = 1$.

1.23 Frazioni e numeri razionali. Consideriamo $\mathbb{Z} \times \mathbb{Z}^*$, l'insieme delle coppie di numeri interi, con il secondo elemento non nullo. Diremo che due coppie (a, b) e (c, d) sono *equivalenti* se vale $ad = bc$.

Prescindendo dai dettagli matematici che sarebbero necessari, definiremo numero razionale (il loro insieme si denota con $\mathbb{Q}$) una classe di equivalenza di coppie di $\mathbb{Z} \times \mathbb{Z}^*$, ovvero l'insieme di tutte le coppie equivalenti a una coppia fissata, per esempio la classe che contiene $(2, 3), (4, 6), (6, 9) \ldots$: questo numero razionale lo denotiamo con $\frac{2}{3}$ (o con $\frac{4}{6}$ ... nel senso che $\frac{2}{3} = \frac{4}{6}$).

Identifichiamo il numero razionale $\frac{a}{1}$ con il numero intero a. Quindi possiamo dire che $\mathbb{Z} \subset \mathbb{Q}$. E' molto semplice dunque estendere le operazioni già conosciute ai numeri razionali:

1.24 Definizioni. Siano $\frac{a}{b}$ e $\frac{c}{d}$ due numeri razionali. Allora:

(1) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad}{bd} \pm \frac{cb}{db} = \frac{ad \pm bc}{bd}$.
(2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

(3) Se anche $a \neq 0$, $(\frac{a}{b})^{-1} = \frac{b}{a}$, perció $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$.
(4) $\frac{a}{b} > 0 \iff ab > 0$.

L' insieme $\mathbb{Q}$ è denso: ciò significa che per ogni $x, y \in \mathbb{Q}$ con $x > y$, esiste $t \in \mathbb{Q}$ con $x > t > y$ (basta prendere, per esempio, $t = \frac{x+y}{2}$).

1.25 Esercizi.

a) Siano $a, b \in \mathbb{Z}^*$, e sia $d = MCD(a, b)$. Provare che $MCD(\frac{a}{d}, \frac{b}{d})$ è definito e vale 1.

b) Sia $x \in \mathbb{Q}$. Provare che esistono unici $a, b \in \mathbb{Z}, b > 0$ e $MCD(a, b) = 1$ tali che $x = \frac{a}{b}$.

c) Dimostrare che $\frac{a}{b} - \frac{c}{d} > 0$ (ovvero $\frac{a}{b} > \frac{c}{d}$) $\iff ad > bc$.
d) Provare che $\forall x, y \in \mathbb{Q}$, con $x \neq 0$, esiste un unico $t \in \mathbb{Q}$ per cui $tx = y$.

1.26 Numeri complessi. In $\mathbb{R}^2$ definiamo le operazioni di addizione e moltiplicazione nel modo seguente: $\forall z = (x, y),\ z' = (x', y')$,

$$z + z' := (x + x', y + y'), \quad z \cdot z' := (xx' - yy', xy' + x'y).$$

Chiamiamo $z = (x, y)$ numero complesso, e denotiamo con $\mathbb{C}$ l'insieme dei numeri complessi (ovvero, $\mathbb{C}$ è $\mathbb{R}^2$ dotato delle due operazioni appena descritte). Consideriamo poi $\mathbb{R}$ come sottoinsieme di $\mathbb{C}$ identificando $x \in \mathbb{R}$ con $(x, 0) \in \mathbb{C}$.

Il numero complesso $(0, 1)$ si denota con il simbolo i; per esso vale

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

Ne segue che ogni numero complesso si può scrivere come

$$z = (x, y) = (x, 0) + (0, y) = (x, 0) + y(0, 1) = x + iy;$$

$x = Rez$ è la parte reale, $y = Imz$ è la parte immaginaria. Useremo sempre la scrittura $x + iy$ con le regole del calcolo letterale.

Se $z = x + iy$, definiamo il coniugato di z come $\overline{z} := x - iy$; invece la norma di z è data da $|z|^2 := z\overline{z}$; si verifica facilmente che vale:
$z\overline{z} = (Rez)^2 + (Imz)^2, \quad z + \overline{z} = 2Rez, \quad z - \overline{z} = 2iImz,$
e quindi, se $z \neq 0$, $z^{-1} = \frac{\overline{z}}{|z|}$.

1.27 Forma trigonometrica dei numeri complessi. Nel piano cartesiano $\mathbb{R}^2$, consideriamo $z = (x, y) = P$; allora $r = |z|$ è la distanza di P dall'origine; se $P \neq O$, ovvero $|z| \neq 0$, chiamiamo α l'angolo fra il semiasse positivo delle x e il vettore OP; si ha $x = |z| \cos \alpha,\ y = |z| \sin \alpha$, per cui si puó scrivere il numero complesso z in forma trigonometrica come

$$z = x + iy = |z|(\cos \alpha + i \sin \alpha).$$

Questa forma è vantaggiosa per prodotto e potenze, infatti se $z = |z|(\cos\alpha + i\sin\alpha)$, $w = |w|(\cos\beta + i\sin\beta)$, vale

$$zw = |z||w|(\cos(\alpha+\beta) + i\sin(\alpha+\beta)), \quad z^n = |z|^n(\cos n\alpha + i\sin n\alpha).$$

1.28 Esercizi.

a) Calcolare coniugato, norma e inverso dei seguenti numeri complessi:
$3 - 2i,\ -5,\ \frac{3}{i}$.

b) Scrivere in forma trigonometrica i seguenti numeri complessi, e poi calcolare il loro prodotto:
$1 - i,\ -5i,\ 2 + \sqrt{3}$.

c) Per quali valori $x \in \mathbb{R}$ è reale il numero: $\frac{x-2+ix}{x-3-5i}$?

2. Gruppi

2.1 Sia S un insieme non vuoto. Una **operazione** (o **legge di composizione interna**) su S è una funzione $f : S \times S \to S$. Di solito, una operazione si denota con un simbolo, tipo $*, +, \circ \ldots$, e $f((a, b))$ si denota con $a * b,\ a + b,\ a \circ b, \ldots$.

L'operazione $*$ è detta **associativa** se, per ogni $a, b, c \in S$, vale $(a*b)*c = a*(b*c)$; in questo caso scriveremo semplicemente $a*b*c$.
E' detta **commutativa** se $\forall a, b \in S,\ a * b = b * a$.

Un elemento $s \in S$ è detto **elemento neutro** per l'operazione $*$ se vale

$$\forall a \in S,\ a * s = a, s * a = a.$$

Se in S esiste un elemento neutro per $*$, esso è unico e lo indicheremo con la lettera e, o con 0 (notazione additiva) o con 1 (notazione moltiplicativa).

Se $*$ è una operazione associativa sull'insieme S, con elemento neutro e (cosa che indicheremo con la terna $(S, *, e)$), useremo la notazione delle potenze, ovvero definiamo in modo ricorsivo, $\forall a \in S$, $a^0 := e, a^1 := a$, e per $n > 1$, $a^n := a * a^{n-1} = a * \cdots * a$, n volte.

Un elemento $a \in S$ è detto **invertibile** se c'è in S un elemento (che risulta essere unico quando $*$ è associativa), che denotiamo con a^{-1}, tale che $a^{-1} * a = e, a * a^{-1} = e$. L'elemento a^{-1} è detto **l'inverso di** a.

Esempi. La somma e il prodotto sono operazioni su $\mathbb{Z}$, associative e commutative. L'elemento neutro per la somma è il numero zero, infatti $\forall n \in \mathbb{Z},\ n + 0 = n$, e l'elemento neutro per il prodotto è il numero 1, infatti $\forall n \in \mathbb{Z},\ n \cdot 1 = n$.
Lo stesso si può dire di $\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
Ogni elemento di $\mathbb{Z}$ è invertibile rispetto alla somma, infatti dato il numero n, il suo inverso è $-n$, poiché $(-n) + n = 0$. Ciò non vale in $\mathbb{N}$.
Solo i numeri 1 e -1 di $\mathbb{Z}$ sono invertibili rispetto al prodotto, e il loro inverso coincide con il numero stesso. Infatti: $1 \cdot 1 = 1,\ (-1) \cdot (-1) = 1$, e se $n \neq \pm 1$, non c'è alcun numero $x \in \mathbb{Z}$ tale che $n \cdot x = 1$. Invece in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, se si esclude lo zero, ogni numero è invertibile rispetto al prodotto.

2.2 Definizione. Un **gruppo** è una terna $(G, *, e)$, dove G è un insieme, $*$ è una operazione associativa su G con elemento neutro e, tale che ogni elemento di G è invertibile, ovvero ha inverso in G.

La proprietà principale dei gruppi è **la legge di cancellazione**:
$\forall a, b, c \in G,\ a * b = a * c \Rightarrow b = c$ e $b * a = c * a \Rightarrow b = c$.

Dimostrazione. Siano $a, b, c \in G$; $a*b = a*c \Rightarrow a^{-1}*(a*b) = a^{-1}*(a*c) \Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \Rightarrow e * b = e * c \Rightarrow b = c$. Analogamente si procede per l'altra uguaglianza.

Un'altra proprietà importante dei gruppi è **la risolubilità delle equazioni**:
$\forall a, b \in G$, l'equazione $a * x = b$ ha un'unica soluzione in G
(e lo stesso vale per l'equazione $x * a = b$). Infatti basta notare che la soluzione cercata è $a^{-1} * b$: essa è unica dalla legge di cancellazione.

2.3 Definizione. Un **gruppo abeliano** è un gruppo in cui l'operazione è anche commutativa. In questo caso, si usa di solito la "notazione additiva"
$(G, +, 0)$, ovvero $a^{-1} := -a$, $a^n := na$, $a^{-n} := -na$.

2.4 Esempi di gruppi.
1. $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$ sono gruppi abeliani.

2. $(\mathbb{R}^*, \cdot, 1)$, $(\mathbb{C}^*, \cdot, 1)$, $(\mathbb{Q}^*, \cdot, 1)$ (dove $\mathbb{R}^* = \mathbb{R} - \{0\}$, e così gli altri) sono gruppi abeliani.

3. $(\mathbb{R}^n, +, O)$, $(\mathbb{C}^n, +, O)$, $(M(m \times n, \mathbb{R}), +, O)$, $(M(m \times n, \mathbb{C}), +, O)$ sono gruppi abeliani.

4. Se $GL(n, \mathbb{R}) := \{A \in M(n \times n, \mathbb{R}) \ / \ detA \neq 0\}$, $(GL(n, \mathbb{R}), \cdot, I_n)$, è il **gruppo generale lineare**. Esso non è abeliano.

5. $(Aut(S), \circ, id)$, dove S è un insieme non vuoto, e $Aut(S)$ è l'insieme delle applicazioni invertibili (cioè biettive) da S in S; $Aut(S)$ è un gruppo.

6. Il *gruppo simmetrico su n elementi,* S_n, è $Aut(T)$, dove T è un insieme con n elementi, che indichiamo con le cifre da 1 a n. Gli elementi di S_n sono detti anche le **permutazioni** su n oggetti, e il loro numero è $n!$. Per esempio, S_3 ha 6 elementi, ed è il più piccolo gruppo non commutativo.

I gruppi finiti, ovvero quelli che hanno un numero finito di elementi, si possono descrivere tramite la tavola di moltiplicazione: per esempio in S_2 ci sono esattamente 2 elementi, l'identità id e la permutazione che manda 1 in 2 e 2 in 1, che chiamiamo p e quindi per S_2 si ha:

	id	p
id	id	p
p	p	id

2.5 Definizione. Sia $(G, *, e)$ un gruppo. Un sottoinsieme H di G è detto un **sottogruppo** di G se $(H, *, e)$ è un gruppo, ovvero se:
$e \in H$,
$\forall a, b \in H$, anche $a * b \in H$,
$\forall a \in H$, anche $a^{-1} \in H$.

Queste tre condizioni si possono anche esprimere come
$\forall a, b \in H$, anche $a * b^{-1} \in H$

In questo caso si scrive $H < G$. I sottogruppi banali di G sono G stesso e $\{e\}$; tutti gli altri sono detti sottogruppi propri.

2.6 Esempi di sottogruppi.
1. L'insieme dei pari in $(\mathbb{Z}, +, 0)$. L'insieme dei multipli di un intero b in $(\mathbb{Z}, +, 0)$, che indichiamo con $b\mathbb{Z} = \{n \in \mathbb{Z} \ / \ n = kb\}$ (quindi l'insieme dei pari è $2\mathbb{Z}$).
2. $(\mathbb{Z}, +, 0) < (\mathbb{Q}, +, 0) < (\mathbb{R}, +, 0) < (\mathbb{C}, +, 0)$.
3. Le matrici diagonali non singolari in $(GL(n, \mathbb{R}), \cdot, I_n)$. Le matrici diagonali in $(M(n \times n, \mathbb{R}), +, O)$.

2.7 Teorema. Tutti i sottogruppi di $(\mathbb{Z}, +, 0)$ sono del tipo $b\mathbb{Z}$ per qualche $b \in \mathbb{Z}$.

Dimostrazione. Per i sottogruppi banali è vero: $\{0\}$ è l'insieme dei multipli di 0, cioè è $0\mathbb{Z}$, e $\mathbb{Z}$ è l'insieme dei multipli di 1, cioè è $1\mathbb{Z}$.

Sia H un sottogruppo non banale di $(\mathbb{Z}, +, 0)$: allora in H ci sono elementi non nulli, e dunque anche elementi positivi (se a è negativo, considero $-a$, che sta ancora in H). Sia dunque b il più piccolo intero positivo in H: dimostriamo che $H = b\mathbb{Z}$, controllando le due inclusioni.

Sia kb un qualsiasi elemento di $b\mathbb{Z}$: se k è positivo, $kb = b + \cdots + b$, che sta in H per la seconda condizione di sottogruppo; se $k < 0$, allora $-k > 0$ e quindi $(-k)b \in H$, e per la terza condizione anche $kb \in H$; se $k = 0$, $kb = 0 \in H$ dalla prima condizione. Abbiamo dunque provato che $b\mathbb{Z} \subset H$.

Per provare l'altra inclusione, dobbiamo dimostrare che ogni elemento $n \in H$ è multiplo di b. Usiamo la divisione con resto $(n : b)$ per scrivere $n = qb + r$ dove il quoziente q e il resto r sono interi, e $0 \leq r < b$: il nostro scopo è di dimostrare che $r = 0$. Da quanto visto prima, $qb \in H$ e dunque per le condizioni seconda e terza anche $r = n - qb \in H$: ma se r è un intero positivo, questo è assurdo, perché il più piccolo intero positivo in H è b. Dunque deve essere $r = 0$.

2.8 Definizione. I gruppi $(G, *, e)$ e $(G', *', e')$ sono detti **isomorfi** se esiste una corrispondenza biunivoca (ovvero una applicazione biettiva) $\varphi : G \to G'$ che rispetta le operazioni, cioè

$$\forall a, b \in G, \ \varphi(a) *' \varphi(b) = \varphi(a * b).$$

φ si dice un **isomorfismo** fra G e G'.

Due gruppi isomorfi hanno la stessa "struttura"e le stesse proprietà. Un isomorfismo da un gruppo in se stesso è detto anche **automorfismo**; per esempio, l'identità è un automorfismo.

2.9 Esempi.

1. $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} / \, x \in \mathbb{R} \right\} < GL(2,\mathbb{R})$ è isomorfo a $(\mathbb{R}, +, 0)$ mediante l'isomorfismo $\varphi : \mathbb{R} \to H$ definito da $\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

2. $(\mathbb{Z}, +, 0)$ è isomorfo al suo sottogruppo $5\mathbb{Z}$. Dunque per ogni $h, k \in \mathbb{Z}$ non nulli, $k\mathbb{Z}$ è isomorfo a $h\mathbb{Z}$.

3. Sia P una matrice fissata in $GL(n,\mathbb{R})$: la applicazione φ definita da $\varphi(A) = P^{-1}AP$ è un automorfismo di $GL(n,\mathbb{R})$.

2.10 Definizione. Siano $(G, *, e)$ e $(G', *', e')$ gruppi: un **omomorfismo** da G a G' è una applicazione $\varphi : G \to G'$ che rispetta le operazioni, cioè

$$\forall a, b \in G, \;\; \varphi(a) *' \varphi(b) = \varphi(a * b).$$

Quindi, un isomorfismo è un omomorfismo invertibile. Osservazione: vale $\varphi(e) = e'$ e $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

2.11 Esempi di omomorfismi.

1. $\det : GL(n,\mathbb{R}) \to (\mathbb{R}^*, \cdot, 1)$

2. $exp : (\mathbb{Z}, +, 0) \to (\mathbb{R}^*, \cdot, 1)$, dove $exp(n) = e^n$.

2.12 Proposizione. Siano $(G, *, e)$ e $(G', *', e')$ gruppi e $\varphi : G \to G'$ un omomorfismo.

a) L'**immagine** di φ, denotata con $Im\varphi$, è un sottogruppo di G'.

b) La controimmagine di e', detta **nucleo** di φ e denotata con $Ker\varphi$, è un sottogruppo di G.

Dimostrazione. a) $e' \in Im\varphi$ poiché $e' = \varphi(e)$. Se $x, y \in Im\varphi$, allora esistono $a, b \in G$ tali che $x = \varphi(a)$, $y = \varphi(b)$, dunque $x *' y = \varphi(a) *' \varphi(b) = \varphi(a * b) \in Im\varphi$, e $x^{-1} = (\varphi(a))^{-1} = \varphi(a^{-1}) \in Im\varphi$.

b) Per definizione, $Ker\varphi := \{a \in G \, / \, \varphi(a) = e'\}$. Dunque $e \in Ker\varphi$ poiché $\varphi(e) = e'$. Se $a, b \in Ker\varphi$, allora $\varphi(a) = e'$, $\varphi(b) = e'$, dunque $\varphi(a * b) = \varphi(a) *' \varphi(b) = e' *' e' = e'$, e $\varphi(a^{-1}) = (\varphi(a))^{-1} = (e')^{-1} = e'$.

2.13 Esempi.

1. L'omomorfismo $\det : GL(n,\mathbb{R}) \to (\mathbb{R}^*, \cdot, 1)$ ha come nucleo $SL(n,\mathbb{R}) = \{A \in M(n \times n, \mathbb{R}) \, / \, detA = 1\}$ detto il **gruppo speciale lineare**, e come immagine tutto il gruppo $\mathbb{R}^*$.

2. Sia $O(n) := \{A \in M(n \times n, \mathbb{R}) \, / \, A^T \cdot A = I_n\}$ il **gruppo ortogonale** di ordine n, che è un sottogruppo di $GL(n,\mathbb{R})$.

Allora $\det : O(n) \to (\mathbb{R}^*, \cdot, 1)$ ha nucleo $SO(n,\mathbb{R}) = \{A \in O(n) \, / \, detA = 1\}$ detto il **gruppo speciale ortogonale**, e immagine $\{1, -1\} < \mathbb{R}^*$.

2.14 Definizione. La struttura algebrica $(F, +, \cdot, 0, 1)$ è un campo se:
(i) $(F, +, 0)$ è un gruppo abeliano
(ii) $\cdot$ è una operazione associativa e commutativa su F con elem. neutro 1
(iii) $(F^*, \cdot, 1)$ è un gruppo abeliano (dove $F^* = F - \{0\}$)
(iv) vale la proprietà distributiva: $\forall\ a, b, c \in F,\ (a + b) \cdot c = a \cdot c + b \cdot c$.

2.15 Esempi. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi. $GL(n, \mathbb{R})$ non è un campo, ma solo un "anello"(il prodotto di matrici ha meno proprietà). Una classe importante di esempi è quella dei campi finiti, che definiamo mediante le congruenze.

2.16 Congruenze. Sia $n \in \mathbb{N}, n \neq 0$ fissato, e siano $a, b \in \mathbb{Z}$. Diremo che a è **congruo** (o congruente) a b modulo n, e scriveremo

$$a \equiv b \ mod\ n$$

se $b - a$ è multiplo di n, cioè se $b = a + nk$ per qualche $k \in \mathbb{Z}$.

La classe di congruenza di $a \in \mathbb{Z}$, che denotiamo con $\overline{a}$, è l'insieme di tutti gli interi congruenti ad a:

$$\overline{a} = \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}.$$

Osserviamo che esistono esattamente n classi di congruenza modulo n: esse sono $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$. L'insieme formato da queste classi si denota con $\frac{\mathbb{Z}}{n\mathbb{Z}}$, ovvero $\mathbb{Z}_n$: dire che due elementi $\overline{a}$ e $\overline{b}$ sono uguali in $\mathbb{Z}_n$ significa dire che $a \equiv b\ mod\ n$.

Osservazione. In $\mathbb{Z}_n$ si possono introdurre le operazioni di somma e di prodotto in modo naturale come

$$\overline{a} + \overline{b} := \overline{a + b}\ ,\ \overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

infatti si può controllare facilmente che le due operazioni sono "ben definite", ovvero non dipendono dai rappresentanti scelti per le classi $\overline{a}$ e $\overline{b}$.

Rispetto alla somma, ogni elemento di $\mathbb{Z}_n$ ha inverso, come succede in $\mathbb{Z}$, mentre questo non accade rispetto al prodotto, esattamente come succede in $\mathbb{Z}$ (per esempio, si può controllare che in $\mathbb{Z}_6$ l'elemento $\overline{2}$ non ha inverso).

E' fondamentale (e di non immediata dimostrazione) il seguente risultato:

2.17 Teorema. Se p è un numero primo, allora ogni elemento non nullo (cioè diverso dalla classe $\overline{0}$) ha inverso in $\mathbb{Z}_p$, perciò $(\mathbb{Z}_p, +, \cdot, \overline{0}, \overline{1})$ è un campo, formato da p elementi.

2.18 Esercizi svolti.

(2.1) Dato $n \in \mathbb{N}, n \neq 0$, una radice n-esima dell'unità è un numero complesso z tale che $z^n = 1$. Dimostrare che le radici n-esime dell'unità formano un sottogruppo di $U := \{z \in \mathbb{C}^* / \ |z| = 1\}$ che è sottogruppo di $\mathbb{C}^*$. Quanti elementi hanno questi sottogruppi?

Dimostrazione. $U := \{z \in \mathbb{C}^* / \ |z| = 1\}$ è sottogruppo di $(\mathbb{C}^*, \cdot, 1)$ poiché:

(1) $|1| = 1$ dunque $1 \in U$;
(2) se z e $w \in U$, allora $|zw| = |z||w| = 1 \cdot 1 = 1$, dunque $zw \in U$;
(3) se $z \in U$, allora $|z^{-1}| = |z|^{-1} = 1$, dunque $z^{-1} \in U$.

Chiamiamo Rad_n l'insieme delle radici n-esime dell'unità: Rad_n è un sottogruppo di U (e quindi anche di $(\mathbb{C}^*, \cdot, 1)$) poiché:

(1) $1^n = 1$, dunque $1 \in Rad_n$;
(2) se z e $w \in Rad_n$, allora $(zw)^n = z^n w^n = 1 \cdot 1 = 1$, dunque $zw \in Rad_n$;
(3) se $z \in Rad_n$, allora $(z^{-1})^n = (z^n)^{-1} = 1$, dunque $z^{-1} \in Rad_n$.

U ha infiniti elementi, che formano il cerchio unitario nel piano complesso; invece, per il teorema fondamentale dell'algebra, Rad_n ha esattamente n elementi, i vertici del poligono regolare di n lati inscritto nel cerchio unitario con un vertice in $(1, 0)$.

(2.2) Dimostrare che il gruppo additivo dei reali è isomorfo al gruppo moltiplicativo dei reali positivi.

Dimostrazione. Un possibile isomorfismo è $exp : (\mathbb{R}, +, 0) \to (\mathbb{R}^+, \cdot, 1)$, $exp(x) = e^x$, che rispetta le operazioni e ha come inversa il logaritmo.

(2.3) Ci può essere un isomorfismo fra un gruppo abeliano e un gruppo non abeliano? E un omomorfismo? Giustificare le risposte.

Soluzione. Sia $(G, +, 0)$ un gruppo abeliano e $(H, \cdot, 1)$ un gruppo non abeliano: quindi esistono $h, k \in H$ tali che $h \cdot k \neq k \cdot h$. Se $\varphi : G \to H$ è un isomorfismo, a motivo della suriettività esistono $a, b \in G$ tali che $h = \varphi(a), k = \varphi(b)$, perciò

$$h \cdot k = \varphi(a) \cdot \varphi(b) = \varphi(a + b), \ k \cdot h = \varphi(b) \cdot \varphi(a) = \varphi(b + a) = \varphi(a + b),$$

e dunque φ non può esistere.

La funzione φ considerata nell'esempio 2.9(1) risponde affermativamente alla seconda domanda, prendendo come codominio $GL(2, \mathbb{R})$, che non è abeliano, cioè considerando $\varphi : \mathbb{R} \to GL(2, \mathbb{R})$.

(2.4) Descrivere le possibili relazioni di sottogruppo e di isomorfismo fra i seguenti sottogruppi di $\mathbb{Z}$: $\{0\}$, $2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, $5\mathbb{Z}$, $6\mathbb{Z}$.

Soluzione. Sono tutti isomorfi tra loro, escluso $\{0\}$. E' facile verificare che vale il seguente diagramma:

$$\{0\} < 4\mathbb{Z} < 2\mathbb{Z}, \quad \{0\} < 6\mathbb{Z} < 2\mathbb{Z}, \quad \{0\} < 6\mathbb{Z} < 3\mathbb{Z}, \quad \{0\} < 5\mathbb{Z}.$$

(2.5) Un sottogruppo N di un gruppo $(G, *, e)$ è detto *sottogruppo normale* se soddisfa questa proprietà: $\forall\ a \in N, \forall\ b \in G,\ b^{-1}ab \in N$.

Sia $\varphi : G \to H$ un omomorfismo tra gruppi: dimostrare che $Ker\varphi$ è un sottogruppo normale di G. Si può dire lo stesso per l'immagine? Giustificare la risposta.

Dimostrare che ogni sottogruppo di un gruppo abeliano è normale.

Il centro Z di un gruppo G è l'insieme degli elementi che commutano con ogni elemento del gruppo: $Z := \{x \in G / xg = gx\ \forall\ g \in G\}$. Dimostrare che il centro di un gruppo è sempre un sottogruppo normale.

Dimostrazione. Siano $b \in G$ e $a \in Ker\varphi$, per cui $\varphi(a) = e'$:

$$\varphi(b^{-1}ab) = \varphi(b^{-1})\varphi(a)\varphi(b) = \varphi(b)^{-1}e'\varphi(b) = \varphi(b^{-1}b) = e',$$

dunque $b^{-1}ab \in Ker\varphi$.

L'immagine invece non è sempre un sottogruppo normale di H: per esempio basta prendere l'omomorfismo φ da $\mathbb{R}$ in $GL(2,\mathbb{R})$ dato nell'esempio 2.9(1) (vedi anche esercizio (2.3)): $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in Im\varphi$, ma

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} \notin Im\varphi.$$

Se G è un gruppo abeliano, e N è un suo sottogruppo, $\forall\ a \in N, \forall\ b \in G$, vale $b^{-1}ab = b^{-1}ba = a \in N$, dunque ogni sottogruppo di un gruppo abeliano è normale.

Nello stesso modo si ragiona per il centro: $\forall\ a \in Z, \forall\ b \in G,\ b^{-1}ab = b^{-1}ba = a \in Z$.

(2.6) Sia $\varphi : G \to H$ un omomorfismo tra gruppi: dimostrare che $\varphi(x) = \varphi(y)$ se e solo se $xy^{-1} \in Ker\varphi$.

Dimostrazione. $\varphi(x) = \varphi(y) \iff \varphi(x)\varphi(y)^{-1} = e' \iff \varphi(xy^{-1}) = e' \iff xy^{-1} \in Ker\varphi$.

(2.7) Sia $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in GL(2,\mathbb{R})$: determinare tutti gli elementi del *gruppo ciclico* generato da A, ovvero formato da tutte le potenze di A.

Soluzione. $A^0 = I_2$, $A^1 = A$, $A^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$, perciò $A^4 = -A$, $A^5 = -A^2$, $A^6 = I_2$ (che ho già considerato). Anche tutte le potenze negative sono già considerate, dato che dall'ultima

uguaglianza si deduce che $A^{-1} = A^5 = -A^2$. Dunque questo gruppo ciclico ha 6 elementi.

(2.8) Dimostrare che l'applicazione $A \to (A^T)^{-1}$ è un automorfismo di $GL(n, \mathbb{R})$. Lo è anche per $SL(n, \mathbb{R})$? L'applicazione $A \to A^2$ è un automorfismo di $GL(n, \mathbb{R})$?

Dimostrazione. Sia $f(A) = (A^T)^{-1}$: questa funzione è invertibile, poiché la sua inversa è lei stessa (ovvero, $f \circ f = id$). Essa inoltre conserva il prodotto: $f(AB) = ((AB)^T)^{-1} = ((B^T)(A^T))^{-1} = (A^T)^{-1}(B^T)^{-1} = f(A)f(B)$. Tutto ciò vale anche su $SL(n, \mathbb{R})$.

Sia poi $g(A) = A^2$: questa funzione non è iniettiva, poiché per esempio $g(I) = I = g(M)$, dove $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. In realtà g non è un omomorfismo di $GL(2, \mathbb{R})$, dato che in generale $g(AB) \neq g(A)g(B)$.

(2.9) Calcolare l'inverso di $\overline{5}$ in $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_{11}$.

Soluzione. In $\mathbb{Z}_2$, $\overline{5} = \overline{1}$ il cui inverso è $\overline{1}$; in $\mathbb{Z}_3$, $\overline{5} = \overline{2}$ il cui inverso è $\overline{2}$ perché $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$. Per trovare l'inverso $\overline{x}$ di $\overline{5}$ in $\mathbb{Z}_{11}$, devo risolvere l'equazione $5x - 1 = 11k$, che dà $x = \frac{(11k+1)}{5}$: questo numero è intero per $k = -1$, dunque $x = -2$, e l'inverso di $\overline{5}$ è $\overline{x} = \overline{-2} = \overline{9}$ (verifica: $\overline{5} \cdot \overline{9} = \overline{45} = \overline{1}$ in $\mathbb{Z}_{11}$).

(2.10) Il gruppo di Klein V_4 è il sottogruppo di $GL(2, \mathbb{R})$ formato dalle quattro matrici $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. Controllare che si tratta di un sottogruppo e scrivere la sua tabella di moltiplicazione.

Soluzione. Se chiamo $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $V_4 = \{I_2, -I_2, A, -A\}$. La tabella di moltiplicazione mi dice che si tratta di un sottogruppo (abeliano).

	I_2	$-I_2$	A	$-A$
I_2	I_2	$-I_2$	A	$-A$
$-I_2$	$-I_2$	I_2	$-A$	A
A	A	$-A$	I_2	$-I_2$
$-A$	$-A$	A	$-I_2$	I_2