Appunti di Teoria dei Gruppi

Versione del 8 Gennaio 2007

Appunti per alcune parti dei corsi di *Teoria dei Gruppi* e *Algebra B* tenuti da Roberto Catenacci al Corso di Laurea in Matematica e Applicazioni dell'Università del Piemonte Orientale; tratti, con alcune modifiche e molti tagli dalle *Note per il corso di Algebra* (a.a. 2001/2002) dei prof. R. Schoof (Università di Roma 'Tor Vergata') e L. van Geemen (Università di Milano).

Testi di riferimento consigliati:

I.N. Herstein, *Algebra*, Editori Riuniti, 3a edizione, Roma 1994
M. Artin, *Algebra*, Bollati Boringhieri, Torino 1997

Indice

1 Numeri interi **2**

2 Gruppi **10**

3 Sottogruppi, omomorfismi, prodotti **20**

4 Generatori, ordine e indice **29**

5 Sottogruppi normali e gruppi quoziente **38**

6 Teoremi di isomorfismo **44**

1 Numeri interi

1.1 L'insieme dei numeri interi è

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

Si sa bene come addizionare, sottrarre e moltiplicare i numeri interi. In questo paragrafo discuteremo le proprietà della divisione fra interi. Introdurremo i numeri *primi* e dimostreremo il Teorema Fondamentale dell' Aritmetica (1.14): ogni intero positivo può essere scritto in modo unico come prodotto di numeri primi.

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

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

Dimostrazione. Sia

$$A = \{a - xb : x \in \mathbb{Z}\}.$$

Prendendo, per esempio, $x = 0$ se $a \geq 0$ e $x = a$ se a è negativo, si vede che A contiene elementi non-negativi. Allora l'insieme

$$A \cap \{0, 1, 2, \ldots\}$$

non è vuoto. Secondo il principio del minimo intero contiene dunque un elemento minimo $r = a - xb$ per un certo $x \in \mathbb{Z}$. Adesso poniamo $q = x$ e troviamo che

$$a = qb + r$$

con $r \geq 0$. Se r soddisfacesse $r \geq b$, allora $r - b \in A \cap \{0, 1, 2, \ldots\}$ perché $r - b \geq 0$ e $r - b = a - (q+1)b$. Siccome $r - b < r$, questo contraddirebbe la minimalità di r. Concludiamo che $0 \leq r < b$.

Adesso abbiamo trovato q ed r con le proprietà volute. Dobbiamo ancora dimostrare l'unicità di questi numeri. Se ci fossero un altro quoziente q' e resto r' con le proprietà desiderate, allora

$$a = qb + r \qquad \text{e} \quad a = q'b + r', \qquad \text{con} \quad 0 \leq r, r' < b.$$

Supponiamo che $q \neq q'$. Scambiando q' e q, se necessario, possiamo supporre che $q > q'$. Adesso sottraiamo membro a membro le due uguaglianze e, siccome $q - q' \geq 1$, troviamo

$$b \leq (q - q')b = r' - r \leq r' < b.$$

Questa contraddizione implica che $q = q'$ e dunque $r = r'$ e la dimostrazione è completa. □

1.3 Definizione. Siano $a, b \in \mathbb{Z}$. Si dice che a *divide* b se esiste un intero $c \in \mathbb{Z}$ tale che

$$b = ac.$$

1.4 Per esempio, 3 divide 15, perche $15 = 3 \cdot 5$. Ogni intero divide 0. Se a divide b, si dice anche che a è un *divisore* di b oppure che b è *divisibile* per a. In tal caso si scrive $a|b$. Si controlla che 1 è un divisore di ogni numero. Si verifica facilmente che b divide $a \pm a'$ quando b divide sia a che a'. Se $a \neq 0$ e b divide a, allora $|b| \leq |a|$. Per quest'ultima proprietà la seguente definizione ha senso.

1.5 Definizione. Se a e b sono interi non entrambi nulli, il *massimo comun divisore* $\mathrm{mcd}(a, b)$ di a e b è il più grande intero che divide a e b. Definiamo $\mathrm{mcd}(0, 0) = 0$.

1.6 Proposizione. Siano $a, b \in \mathbb{Z}$.

(*i*) $\mathrm{mcd}(b, a) = \mathrm{mcd}(a, b)$,

(*ii*) $\mathrm{mcd}(-a, b) = \mathrm{mcd}(a, b)$,

(*iii*) Per ogni $q \in \mathbb{Z}$ si ha che $\mathrm{mcd}(a, b + qa) = \mathrm{mcd}(a, b)$.

Dimostrazione. Dimostriamo soltanto la parte *(iii)* perché le dimostrazioni delle altre parti sono simili e più facili. Sia $q \in \mathbb{Z}$. Se d divide a e b, allora d divide $b + qa$. Viceversa, se d divide a e $b + qa$ allora d 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 $b + qa$. Questo dimostra 1.6(*iii*). □

1.7 Teorema. Siano $a, b \in \mathbb{Z}$, non entrambi nulli. Allora il massimo comun divisore di a e b è uguale al più piccolo elemento *positivo* nell'insieme

$$A = \{ax + by : x, y \in \mathbb{Z}\}.$$

Dimostrazione. Prendendo $x = 0$, $y = \pm 1$ e $x = \pm 1$, $y = 0$, si vede che i numeri $a, -a, b, -b$ sono tutti in A. Dunque A contiene qualche elemento positivo. Sia $d = ax + by$ il più piccolo elemento positivo in A. Tutti gli elementi in A sono somme di un multiplo di a e uno di b. Allora tutti, ed in particolare d, sono divisibili per $\mathrm{mcd}(a, b)$. Questo implica che

$$\mathrm{mcd}(a, b) \leq d.$$

D'altra parte, se $c = ax' + by' \in A$, utilizzando il Teorema 1.2, possiamo dividere l'intero c per d con quoziente q e resto r:

$$c = qd + r \qquad \text{con } 0 \leq r < d.$$

Sostituendo $c = ax' + by'$ e $d = ax + by$, si vede che $r = a(x' - qx) + b(y' - qy) \in A$. Siccome $r < d$ e d era minimale, dobbiamo avere che $r = 0$. Dunque $c = qd$ e d divide c. Siccome c era un qualsiasi elemento di A, concludiamo che d divide *ogni* $c \in A$. In particolare d divide $a, b \in A$. Risulta che

$$d \leq \mathrm{mcd}(a, b)$$

e la dimostrazione è completa. □

1.8 Corollario. Siano $a, b \in \mathbb{Z}$. Allora esistono $x, y \in \mathbb{Z}$ tali che

$$ax + by = \mathrm{mcd}(a, b).$$

Dimostrazione. L'affermazione è banale quando $a = b = 0$ e nell' altro caso segue dal Teorema 1.7. □

1.9 Corollario. Siano $a, b \in \mathbb{Z}$. Se l'intero d divide a e b, allora d divide $\mathrm{mcd}(a, b)$.

Dimostrazione. L'affermazione è banale quando $a = b = 0$ e nell'altro caso segue dal Corollario 1.8. □

1.10 Corollario. Siano $a, b, c \in \mathbb{Z}$. Se $\mathrm{mcd}(a, b) = 1$ e $a|bc$ allora $a|c$.

Dimostrazione. Per il Corollario 1.8 esistono x, $y \in \mathbb{Z}$ tale che $ax + by = 1$. Moltiplicando per c otteniamo:

$$cax + bcy = c.$$

Siccome a divide bc, esiste $m \in \mathbb{Z}$ tale che $am = bc$. Troviamo $c = cax + amy = a(cx + my)$ e vediamo che a divide c. □

1.11 Definizione. Un intero p si dice un *numero primo*, se è positivo e se i soli divisori positivi di p sono 1 e p.

1.12 Esempi. Esempi di numeri primi sono:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots,\ 94291,\ 94307,\ 94309, \ldots.$$

I numeri primi sono infiniti (si veda l'Eserc. (1.K))

1.13 Proposizione. Siano $b, c \in \mathbb{Z}$ e sia p un numero primo. Se $p|bc$ allora $p|b$ oppure $p|c$.

Dimostrazione. Ovviamente, il massimo comun divisore di b e p divide p. Quindi $\mathrm{mcd}(b, p) = 1$ oppure p. Se p non divide b allora $\mathrm{mcd}(b, p) = 1$ e per il Cor. 1.10 abbiamo che p divide c. □

1.14 Teorema. (Teorema Fondamentale dell'Aritmetica.) Per ogni intero $n > 1$ esistono numeri primi $p_1, p_2, \ldots, p_t$ tali che

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_t.$$

I primi $p_1, \ldots, p_t$ sono unici a meno dell'ordine.

Dimostrazione. Prima dimostriamo l'esistenza di una tale decomposizione. Se questa decomposizione, in generale, non esistesse, ci sarebbe un minimo intero $n > 1$ "senza decomposizione. Questo intero n non può essere primo, perché p stesso è la decomposizione banale di p. Allora si può scrivere $n = ab$ dove a, b sono interi che soddisfano $a, b > 1$ e dunque $a, b < n$.

Siccome n era minimale, gli interi a e b ammettono una decomposizione

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_t, \qquad b = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

dove $p_1, p_2, \ldots, p_t$ e $q_1, q_2, \ldots, q_s$ sono numeri primi. Questa implica che

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_t \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

contraddicendo la definizione di n. Allora un intero n senza decomposizione in primi non esiste.

Per dimostrare l'unicità, prendiamo un intero $n > 1$ con due decomposizioni diverse e minimo rispetto a questa proprietà:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_t = q_1 \cdot q_2 \cdot \ldots \cdot q_s.$$

Allora, il primo p_1 divide il prodotto $q_1 \cdot q_2 \cdot \ldots \cdot q_s$ e dunque, applicando iterativamente il Cor. 1.13, p_1 divide q_i per un certo indice i, $0 \leq i \leq s$. Siccome p_1 e q_i sono tutti e due primi, vale $p_1 = q_i$. Adesso dividiamo n per $p_1 = q_i$ e troviamo

$$n/p_1 = p_2 \cdot \ldots \cdot p_t = q_1 \cdot q_2 \cdot \ldots \cdot q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_s.$$

Il numero n/p_1, essendo più piccolo di n ha una decomposizione unica, a meno dell'ordine dei fattori. Concludiamo che le decomposizioni $n = p_1 \cdot p_2 \cdot \ldots \cdot p_t$ e $n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ erano uguali. Questa contraddizione conclude la dimostrazione. □

1.15 Osservazione. Il teorema vale anche per $n = 1$ ponendo il prodotto vuoto uguale a 1. Se n è *negativo*, si applica il teorema precedente a $-n$ e si trova che esistono numeri primi $p_1, p_2, \ldots, p_t$, unici a meno dell'ordine, tali che

$$n = -p_1 \cdot p_2 \cdot \ldots \cdot p_t.$$

1.16 Definizione. Sia a un intero positivo e sia p un primo. Allora $\mathrm{ord}_p(a)$ indica il numero dei fattori p che occorrono nella decomposizione di a. Se a è negativo definiamo $\mathrm{ord}_p(a) = \mathrm{ord}_p(-a)$. Il valore di $\mathrm{ord}_p(0)$ non è definito.

Se a è un intero, $\mathrm{ord}_p(a)$ e un numero non-negativo. Per i primi p che non dividono a, il valore di $\mathrm{ord}_p(a)$ è zero. Per ogni intero $a > 0$ si ha

$$a = \prod_p p^{\mathrm{ord}_p(a)}.$$

Tutti i numeri primi p occorrono nel prodotto, ma soltanto per un numero finito di essi, l'esponente $\mathrm{ord}_p(a)$ è positivo. Similmente, per un numero negativo a si ha $a = -\prod_p p^{\mathrm{ord}_p(a)}$.

1.17 Proposizione. Siano a, b due interi diversi da 0. Allora

(*i*) per ogni primo p si ha $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$,

(*ii*) un intero $c \neq 0$ divide a se e soltanto se $\mathrm{ord}_p(c) \leq \mathrm{ord}_p(a)$ per ogni primo p,

(*iii*) $\mathrm{mcd}(a,b) = \prod_p p^{\min(\mathrm{ord}_p(a),\mathrm{ord}_p(b))}$.

Dimostrazione. *(i)* Possiamo assumere che $a, b > 0$. Si ha $a = \prod_p p^{\mathrm{ord}_p(a)}$ e $b = \prod_p p^{\mathrm{ord}_p(b)}$. Per il prodotto ab si ha la stessa formula $ab = \prod_p p^{\mathrm{ord}_p(ab)}$. Dunque

$$ab = \prod_p p^{\mathrm{ord}_p(a)+\mathrm{ord}_p(b)} = \prod_p p^{\mathrm{ord}_p(ab)}.$$

Siccome, per il Teorema 1.14, la decomposizione in fattori primi di ab è unica, troviamo che gli esponenti sono uguali: $\mathrm{ord}_p(a) + \mathrm{ord}_p(b) = \mathrm{ord}_p(ab)$.

(ii) Se $c = \prod_p p^{\mathrm{ord}_p(c)}$ divide $a = \prod_p p^{\mathrm{ord}_p(a)}$, allora, per la parte *(i)*,

$$\mathrm{ord}_p(a) = \mathrm{ord}_p(c) + \mathrm{ord}_p(a/c)$$

per ogni p e, $\mathrm{ord}_p(a/c)$ essendo non negativo, $\mathrm{ord}_p(c) \leq \mathrm{ord}_p(a)$. Viceversa, se per ogni primo p si ha $\mathrm{ord}_p(c) \leq \mathrm{ord}_p(a)$, allora c divide a con quoziente $\prod_p p^{\mathrm{ord}_p(a)-\mathrm{ord}_p(c)}$.

(iii) Se c divide a e anche b, si ha per la parte *(ii)* che $\mathrm{ord}_p(c) \leq \mathrm{ord}_p(a)$ e $\mathrm{ord}_p(c) \leq \mathrm{ord}_p(b)$. In altre parole $\mathrm{ord}_p(c) \leq \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$ e dunque c divide il numero $d = \prod_p p^{\min(\mathrm{ord}_p(a),\mathrm{ord}_p(b))}$.

Questo vale, in particolare, per $c = \mathrm{mcd}(a,b)$. Dunque il massimo comun divisore $\mathrm{mcd}(a,b)$ divide d. Per la parte *(ii)*, d è un divisore di a e b. Siccome $\mathrm{mcd}(a,b)$ è il massimo divisore di a e b, concludiamo che $\mathrm{mcd}(a,b) = d$ come richiesto. □

1.18 Algoritmo di Euclide. Infine diamo un *algoritmo* per calcolare il mcd di due interi. Questo metodo si chiama *algoritmo di Euclide*: siano $a, b \in \mathbb{Z}$ e supponiamo che $a, b > 0$. Per la Proposizione 1.6(*i*) non è una restrizione seria. Definiamo i numeri interi r_k per $k = 0, 1, 2, 3, \ldots$ come segue. Poniamo $r_0 = a$ e $r_1 = b$. Poi, utilizzando il Teorema 1.2, dividiamo r_0 per r_1 con quoziente q_1 e resto r_2 dove $0 \leq r_2 < r_1$. Se r_2 non è zero, dividiamo r_1 per r_2 con quoziente q_2 e resto r_3 soddisfacendo $0 \leq r_3 < r_2 \ldots$ eccetera. In generale, se r_k non è zero, dividiamo r_{k-1} per r_k con quoziente q_k e resto r_{k+1}:

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

Si vede che $r_1 > r_2 > r_3 > \ldots$. Ad un certo punto il resto r_k diventa zero e si smette. Il resto precedente r_{k-1} è uguale a $\mathrm{mcd}(a,b)$, come vedremo nella prossima proposizione.

1.19 Esempio. $a = 7007$ e $b = 1991$:

$$\begin{array}{lcrl}
 & & r_0 & = 7007 \\
 & & r_1 & = 1991 \\
q_1 = 3 & \text{ed} & r_2 = r_0 - 3 \cdot r_1 & = 1034 \\
q_2 = 1 & \text{ed} & r_3 = r_1 - 1 \cdot r_2 & = 957 \\
q_3 = 1 & \text{ed} & r_4 = r_2 - 1 \cdot r_3 & = 77 \\
q_4 = 12 & \text{ed} & r_5 = r_3 - 12 \cdot r_4 & = 33 \\
q_5 = 2 & \text{ed} & r_6 = r_4 - 2 \cdot r_5 & = 11 \\
q_6 = 3 & \text{ed} & r_7 = r_5 - 3 \cdot r_6 & = 0.
\end{array}$$

Allora, si trova che $\mathrm{mcd}(7007, 1991) = 11$.

1.20 Proposizione. L'algoritmo di Euclide è un algoritmo corretto: termina e dà come risposta il massimo comun divisore.

Dimostrazione. L'algoritmo termina perché i resti r_k sono non-negativi, ma diventano sempre più piccoli. Ad un certo punto il resto diventa zero e l'algoritmo termina.

Siccome $r_{k-1} = q_k \cdot r_k + r_{k+1}$ si ha per la Proposizione 1.6(*iii*)

$$\mathrm{mcd}(r_{k-1}, r_k) = \mathrm{mcd}(r_k, r_{k+1}).$$

Si trova

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(r_0, r_1) = \mathrm{mcd}(r_1, r_2) = \ldots = \mathrm{mcd}(r_{k-1}, r_k) = \ldots$$

Alle fine, quando r_k diventa 0, abbiamo $\mathrm{mcd}(r_{k-1}, r_k) = \mathrm{mcd}(r_{k-1}, 0) = r_{k-1}$. Concludiamo che $\mathrm{mcd}(a, b) = \ldots = \mathrm{mcd}(r_{k-1}, 0) = r_{k-1}$ come richiesto. □

Ecco una versione estesa dell'algoritmo di Euclide, che calcola anche i due interi $x, y \in \mathbb{Z}$ del Cor.1.8 tali che

$$ax + by = \mathrm{mcd}(a, b).$$

1.21 Algoritmo. Scriviamo

$$1 \cdot a + 0 \cdot b = a = r_0 \qquad 0 \cdot a + 1 \cdot b = b = r_1,$$

adesso facciamo i calcoli dell'algoritmo di Euclide, non solo con i resti r_1, r_2, r_3, ... ecc., ma ogni volta con l'intera equazione. Come spiegazione prendiamo l'esempio sopra con $a = 7007$ e $b = 1991$. Sottraiamo la seconda uguaglianza $q_1 = 3$ volte dalla prima, la terza $q_2 = 1$ volta dalla seconda e così via.

$$\begin{array}{rrrrll}
1\cdot & 7007 & +0\cdot & 1991 & = 7007 & \\
0\cdot & 7007 & +1\cdot & 1991 & = 1991 & (\text{sottrarre } q_1 = 3 \text{ volte}) \\
1\cdot & 7007 & -3\cdot & 1991 & = 1034 & (\text{sottrarre } q_2 = 1 \text{ volta}) \\
-1\cdot & 7007 & +4\cdot & 1991 & = 957 & (\text{sottrarre } q_3 = 1 \text{ volta}) \\
2\cdot & 7007 & -7\cdot & 1991 & = 77 & (\text{sottrarre } q_4 = 12 \text{ volte}) \\
-25\cdot & 7007 & +88\cdot & 1991 & = 33 & (\text{sottrarre } q_5 = 2 \text{ volte}) \\
52\cdot & 7007 & -183\cdot & 1991 & = 11 & (\text{sottrarre } q_6 = 3 \text{ volte}) \\
-181\cdot & 7007 & +637\cdot & 1991 & = 0. &
\end{array}$$

Si trova che $52 \cdot 7007 - 183 \cdot 1991 = 11$.

Esercizi.

(1.A) Sia b un intero positivo (per esempio $b = 10$). Dimostrare che per ogni intero positivo a esistono unici degli interi $a_0, a_1, a_2, \ldots, a_i, \ldots$, tale che $a = a_0 + a_1 b + a_2 b^2 + \ldots + a_i b^i + \ldots$ e $0 \leq a_i < b$ per ogni $i \geq 0$. I numeri b_i sono le cifre di a in base b.

(1.B) Calcolare $d = \mathrm{mcd}(10001, 6497)$. Trovare $x, y \in \mathbb{Z}$ tali che $10001x + 6497y = d$.

(1.C) Calcolare $\mathrm{mcd}(10000000000, 2^5 \cdot 91)$. (Utilizzare la Prop.1.17(*iii*).)

(1.D) Siano $a, b \in \mathbb{Z}$. Dimostrare che:

(i) $\mathrm{mcd}(|a|, |b|) = \mathrm{mcd}(-a, -b) = \mathrm{mcd}(a, b)$.

(ii) Sia $d = \mathrm{mcd}(a, b)$. Allora $\mathrm{mcd}(a/d, b/d) = 1$.

(iii) Sia c un intero positivo. Allora $\mathrm{mcd}(ac, bc) = c \cdot \mathrm{mcd}(a, b)$.

(1.E) (Il mcd di più numeri.)

(i) Siano $a, b, c \in \mathbb{Z}$. Provare che $\mathrm{mcd}(a, \mathrm{mcd}(b, c))$=$\mathrm{mcd}(\mathrm{mcd}(a, b), c)$.

(ii) Per $a_1, a_2, \ldots, a_m \in \mathbb{Z}$ definiamo induttivamente:
$\mathrm{mcd}(a_1, a_2, \ldots, a_m) = \mathrm{mcd}(a_1, \mathrm{mcd}(a_2, \ldots, a_m))$.
Dimostrare che esistono $x_1, x_2 \ldots, x_m \in \mathbb{Z}$ tali che $x_1a_1 + x_2a_2 + \ldots + x_ma_m = \mathrm{mcd}(a_1, a_2, \ldots, a_m)$.

(1.F) Sia $x \in \mathbb{Q}$. Provare che esistono unici $a, b \in \mathbb{Z}$ con $b > 0$ e $\mathrm{mcd}(a, b) = 1$ tali che $x = a/b$.

(1.G) Siano $a, b \in \mathbb{Z}$. Il *minimo comune multiplo* $\mathrm{mcm}(a, b)$ di a e b è il più piccolo intero positivo d tale che sia a che b dividono d.

(i) Dimostrare che $\mathrm{mcm}(a, b) = \prod_p p^{\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b))}$.

(ii) Dimostrare che $\mathrm{mcm}(a, b) \cdot \mathrm{mcd}(a, b) = |ab|$.

(1.H) Siano $a, b \in \mathbb{Z}$. Dimostrare che $\mathrm{mcd}(a, b) = 1$ se e soltanto se esistono $x, y \in \mathbb{Z}$ tali che $ax + by = 1$.

(1.I) Siano $a, b, c \in \mathbb{Z}$. Se $\mathrm{mcd}(a, b) = 1$ e $\mathrm{mcd}(a, c) = 1$ allora $\mathrm{mcd}(a, bc) = 1$.

(1.J) Dimostrare: p è un primo se e soltanto se $p > 1$ e p non ha divisori d con $1 < d \leq \sqrt{p}$. È primo 249? È primo 289?

(1.K) Dimostrare che esiste una infinità di numeri primi. (Suggerimento: se $p_1, \ldots, p_n$ fossero tutti i numeri primi, allora $p_1 \cdot \ldots \cdot p_n + 1$ sarebbe un numero privo di divisori primi.)

(1.L) Provare che per ogni primo $p > 3$ il numero $p^2 - 1$ è divisibile per 24.

(1.M) Siano a e b interi positivi con $\mathrm{mcd}(a, b) = 1$ e tali che $a^2 - b^2$ sia un quadrato. Dimostrare che o $a + b$ e $a - b$ sono dei quadrati, oppure $a + b$ e $a - b$ sono due volte un quadrato.

(1.N) Siano $a, b \in \mathbb{Z}$ e sia n un intero non-negativo.

(i) Dimostrare che $a - b$ divide $a^n - b^n$.

(ii) Dimostrare che $a^n - 1$ è primo implica che $a = 2$ ed n è un primo. Dimostrare che il viceversa è falso. I numeri $2^n - 1$ con n primo si chiamano *numeri di Mersenne*.

(1.O) Siano $a, b \in \mathbb{Z}$ e sia n un intero positivo.

(i) Dimostrare che $a + b$ divide $a^n + b^n$ quando n è dispari.

(ii) Dimostrare che $2^n + 1$ è primo implica che n è una potenza di 2. Dimostrare che il viceversa è falso. I numeri $2^{2^m} + 1$ si chiamano *numeri di Fermat*.

2 Gruppi

2.1 In questo paragrafo introduciamo i gruppi. Diamo diversi esempi importanti di gruppi ai quali faremo continuamente riferimento in seguito.

2.2 Definizione. Un gruppo G è un insieme fornito di una *composizione* $\circ : G \times G \longrightarrow G$ e di un *elemento neutro* $e \in G$ per cui i seguenti assiomi valgono:

(G_1) (*Associatività*) Per ogni $x, y, z \in G$

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

(G_2) (*Elemento neutro*) Per ogni $x \in G$

$$x \circ e = e \circ x = x.$$

(G_3) (*Inverso*) Per ogni $x \in G$ esiste $x^* \in G$ tale che

$$x \circ x^* = x^* \circ x = e.$$

Questi sono gli assiomi di un gruppo G. In generale, non vale l'assioma di commutatività:

(G_4) (*Commutatività*) Per ogni $x, y \in G$

$$x \circ y = y \circ x.$$

Se (G_4) vale, il gruppo G si dice *commutativo* oppure *abeliano*.

2.3 Chiusura. Talvolta si trova in letteratura un ulteriore assioma:

(G_0) (*Chiusura*)

$$x \circ y \in G \qquad \text{per ogni } x, y \in G.$$

Nella nostra presentazione, la chiusura è una consequenza automatica dal fatto che l'immagine della composizione $\circ : G \times G \longrightarrow G$ è in G. Si dice che G è *chiuso* rispetto alla composizione $\circ$.

2.4 Associatività. Per l'associatività (G_1), le due espressioni $x \circ (y \circ z)$ ed $(x \circ y) \circ z$ sono uguali per ogni $x, y, z \in G$. Ecco perché possiamo omettere le parentesi e scrivere $x \circ y \circ z$. Così faremo sempre, anche per più di tre elementi. Per esempio, $x \circ y \circ z \circ t = x \circ (y \circ (z \circ t)) = (x \circ (y \circ z) \circ t)$ etc, ci sono 5 modi di calcolare $x \circ y \circ z \circ t$:

$$x \circ (y \circ (z \circ t)) = x \circ ((y \circ z) \circ t)) = (x \circ (y \circ z)) \circ t = ((x \circ y) \circ z) \circ t = (x \circ y) \circ (z \circ t).$$

2.5 Inverso. L'elemento inverso x^* associato a $x \in G$ nell'assioma G_2) è unico: se x^* e x^{**} soddisfano $x \circ x^* = x^* \circ x = e$ ed anche $x \circ x^{**} = x^{**} \circ x = e$ allora

$$x^* \overset{(G_2)}{=} e \circ x^* = (x^{**} \circ x) \circ x^* \overset{(G_1)}{=} x^{**} \circ (x \circ x^*) \overset{(G_3)}{=} x^{**} \circ e \overset{(G_2)}{=} x^{**},$$

cioè, $x^* = x^{**}$. Dunque ha senso chiamare x^* *l'*elemento inverso di x.

2.6 Un gruppo è una tripla $(G, \circ, e)$. Spesso, quando è chiaro quale composizione e quale elemento neutro sono intesi, si dice semplicemente "G è un gruppo. Di solito si chiama la composizione "moltiplicazione; si scrive $\cdot$ (o niente) per la composizione $\circ$ e 1 per l'elemento neutro e. Per gruppi *commutativi* la composizione è detta anche "addizione e si indica con $+$. In questo caso l'elemento neutro si scrive 0.

Ecco un piccolo dizionario:

	molt.	add.
$a \circ b$	ab	$a + b$
e	1	0
a^*	a^{-1}	$-a$
$\underbrace{a \circ \ldots \circ a}_{n}$	a^n	na

2.7 Esempio. *I gruppi additivi* $\mathbb{Z}$, $\mathbb{Q}$ *ed* $\mathbb{R}$.
I numeri naturali $0, 1, 2, \ldots$ non formano un gruppo per l'addizione perché G_3 non vale: nell'insieme degli interi positivi non c'è inverso. L'insieme $\mathbb{Z}$ degli numeri interi invece è un gruppo rispetto all'addizione. L'elemento neutro è 0. È ben noto che valgono gli assiomi G_1, G_2 e G_3. Anche G_4 vale: $\mathbb{Z}$ è un gruppo commutativo. Si verifica in modo simile che anche i numeri razionali $\mathbb{Q}$ e i numeri reali $\mathbb{R}$ formano un gruppo per l'addizione. In questi tre esempi l'elemento neutro è 0. I gruppi $\mathbb{Q}$ ed $\mathbb{R}$ sono commutativi.

2.8 Esempio. *I gruppi moltiplicativi* $\mathbb{Q}^*$ *e* $\mathbb{R}^*$.
Due numeri interi si possono moltiplicare tra di loro. L'elemento neutro è 1. Ma $\mathbb{Z}$ non è un gruppo per la moltiplicazione perché mancano gli inversi moltiplicativi. Per esempio, se $x \in \mathbb{Z}$ fosse l'inverso di 2, allora sarebbe $2x = 1$ e questa equazione non ha soluzioni in $\mathbb{Z}$. In $\mathbb{Q}$ e $\mathbb{R}$ invece, ogni elemento $a \neq 0$ ha un inverso. Definiamo

$$\mathbb{Q}^* = \mathbb{Q} - \{0\}, \qquad \mathbb{R}^* = \mathbb{R} - \{0\}.$$

Siccome il prodotto ab di due numeri a, b non nulli è diverso da zero, l'assioma G_0 vale per $\mathbb{Q}^*$ e $\mathbb{R}^*$; vale a dire la composizione $\mathbb{Q}^* \times \mathbb{Q}^* \longrightarrow \mathbb{Q}^*$ data da $(a, b) \mapsto ab$ è ben definita e similmente per $\mathbb{R}^*$. Si verifica che valgono gli assiomi G_1, G_2, G_3 e G_4 e si conclude che $\mathbb{Q}^*$ e $\mathbb{R}^*$ sono gruppi commutativi rispetto alla moltiplicazione.

2.9 Esempio. *I numeri complessi* $\mathbb{C}$.
L'insieme dei numeri complessi $\mathbb{C}$ è definito come

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

dove "i è un simbolo. Due numeri complessi $a + bi$ ed $a' + b'i$ sono uguali se e soltanto se $a = a'$ e $b = b'$. Se $b = 0$ si scrive spesso a per $a + bi = a + 0i$.

Addizioniamo due numeri complessi $a + bi$ ed $a' + b'i$ secondo la regola

$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i.$$

Si verifica che in questo modo $\mathbb{C}$ diventa un gruppo per l'addizione. L'elemento neutro è $0 = 0 + 0i$. L'insieme $\mathbb{C}$ è detto il gruppo *additivo* dei numeri complessi.

Moltiplichiamo due numeri complessi $a + bi$ e $a' + b'i$ secondo la regola

$$(a + bi) \cdot (a' + b'i) = (aa' - bb') + (ab' + a'b)i.$$

Con $a, a' = 0$ e $b, b' = 1$ si trova che $i^2 = -1$. Basta ricordare questa identità e si vede che la regola per la moltiplicazione si ottienne sviluppando il prodotto $(a + bi) \cdot (a' + b'i)$. Si vede facilmente che $1 \in \mathbb{C}$ ha la proprietà $1 \cdot (a + bi) = (a + bi) \cdot 1 = a + bi$. Siccome 0 soddisfa $0 \cdot (a + bi) = 0$ per ogni $a + bi \in \mathbb{C}$, non può avere un inverso moltiplicativo. Per questa ragione poniamo

$$\mathbb{C}^* = \mathbb{C} - \{0\}.$$

Segue dalla definizione che la moltiplicazione in $\mathbb{C}^*$ è commutativa. Dimostriamo adesso che $\mathbb{C}^*$ è un gruppo commutativo rispetto alla moltiplicazione con elemento neutro 1: Verifichiamo prima l'associatività G_1: siano $a, b, c, d, e, f \in \mathbb{R}$ e $a + bi$, $c + di$ e $e + fi$ in $\mathbb{C}$, allora

$$\begin{aligned}
((a + bi)(c + di))\,(e + fi) &= ((ac - bd) + (ad + bc)i)\,(e + fi) \\
&= ((ac - bd)e - (ad + bc)f) + ((ac - bd)f + (ad + bc)e)i \\
&= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i
\end{aligned}$$

$$\begin{aligned}
(a + bi)\,((c + di)(e + fi)) &= (a + bi)\,((ce - df) + (cf + de)i) \\
&= ((a(ce - df) - b(cf + de)) + (a(cf + de) + b(ce - fd))i \\
&= (ace - adf - bcf - bde) + (acf + ade + bce - bfd)i
\end{aligned}$$

e vediamo che vale l'associatività della moltiplicazione in $\mathbb{C}^*$. Osserviamo adesso che per $a+bi \in \mathbb{C}$ si ha

$$(a + bi)(a - bi) = (a^2 + b^2) + (-ab + ba)i = a^2 + b^2.$$

Siccome $a + bi = 0$ se e soltanto se $a^2 + b^2 = 0$, si conclude che per $a + bi \neq 0$

$$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \right) = 1.$$

Questo implica l'assioma G_3: ogni $a + bi \in \mathbb{C}^*$ ha un inverso moltiplicativo.

Similmente si verifica che $\mathbb{C}^*$ è chiuso rispetto alla moltiplicazione: siano $a + bi, c + di \in \mathbb{C}^*$. Se $(a + bi)(c + di)$ fosse 0, allora

$$0 = (a - bi)(a + bi)(c + di)(c - di) = (a^2 + b^2)(c^2 + d^2)$$

e dunque $a^2 + b^2 = 0$ oppure $c^2 + d^2 = 0$. Questa è una contraddizione perché $a + bi$ e $c + di$ sono diversi da 0.

2.10 Esempio. *I Quaternioni $\mathbb{H}$ di Hamilton.*
L'insieme $\mathbb{H}$ dei quaternioni di Hamilton è definito come

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

dove i, j e k sono simboli per i quali valgono le regole

$$\begin{array}{ccc} & i^2 = j^2 = k^2 = -1 & \\ ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array} \qquad \begin{array}{ccc} & i & \\ \nearrow & & \searrow \\ k & \leftarrow & j \end{array}$$

che si possono memorizzare con il disegno, moltiplicando due elementi in senso orario si ottiene il terzo con il segno "+ e moltiplicando in senso antiorario con il segno "-.

Esplicitamente, per $a, b, c, d, a', b', c', d' \in \mathbb{R}$, si definisce la somma

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

ed il prodotto

$$\begin{aligned} (a + bi + cj + dk)(a' + b'i + c'j + d'k) = \ & (aa' - bb' - cc' - dd') \\ & +(ab' + ba' + cd' - dc')i \\ & +(ac' - bd' + ca' + db')j \\ & +(ad' + bc' - cb' + da')k. \end{aligned}$$

I quaternioni $\mathbb{H}$ formano un gruppo additivo. Lasciamo la verifica al lettore. L'insieme $\mathbb{H}^* = \mathbb{H} - \{0\}$ dei quaternioni non zero è un gruppo per la moltiplicazione. Siccome $ij \neq ji$, il gruppo $\mathbb{H}^*$ non è commutativo. Si può verificare l'associatività in modo diretto. Per un metodo più efficiente veda l'Eserc.(2.F). Gli altri assiomi si verificano come nel caso di $\mathbb{C}^*$, utilizzando la formula

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

I quaternioni sono importanti non solo in algebra ma anche in geometria differenziale.

2.11 Esempio. *Il gruppo Q dei quaternioni.*
Il gruppo Q è un sottoinsieme di 8 elementi di $\mathbb{H}^*$:

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}.$$

La composizione è la moltiplicazione di $\mathbb{H}^*$. L'associatività segue da quella di $\mathbb{H}^*$. Lasciamo la verifica degli altri assiomi al lettore.

2.12 Esempio. *Il "Vierergruppe V_4 di Klein.*
Il gruppo di Klein V_4 contiene 4 elementi: $V_4 = \{e, a, b, c\}$.
La moltiplicazione è data dalla seguente tavola:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

L'elemento neutro è e. Si vede che $a^2 = b^2 = c^2 = e$. In altre parole ogni elemento è l'inverso di se stesso. Per verificare l'associatività basta, utilizzando la simmetria del diagramma, distinguere qualche caso. Si lascia la verifica al lettore.

2.13 Esempio. *Il gruppo $\mathbb{Z}/n\mathbb{Z}$ delle classi resto modulo n.*
Sia $n \in \mathbb{Z}$ un intero positivo. Per $k \in \mathbb{Z}$, con $0 \leq k < n$, definiamo per $0 \leq k < n$

$$\begin{aligned} R_k &= \{a \in \mathbb{Z} : \ k \text{ è il resto della divisione di } a \text{ per } n\} \\ &= \{\ldots, k-2n, k-n, k, k+n, k+2n, \ldots\}. \end{aligned}$$

Per il Teorema 1.2 si ha $\mathbb{Z} = R_0 \cup R_1 \cup \ldots R_{n-1}$ e $R_i \cap R_j = \emptyset$ se $i \neq j$. Se $a \in R_k$, si dice che R_k *è la classe di congruenza modulo n di a,* oppure, brevemente, che R_k è la classe di a. Scriviamo anche $\overline{a}$ per la classe di a. Si dice che a è un rappresentante della classe $\overline{a}$.

Per $a, b \in \mathbb{Z}$ si ha che $\overline{a} = \overline{b}$ se e soltanto se a e b hanno lo stesso resto della divisione per n e questo è equivalente a dire che n divide $a - b$ (vedi l'Eserc. (2.I)). In tal caso si dice che a *è congruente a b modulo n,* oppure che a è *uguale* a b modulo n e si scrive $a \equiv b \bmod n$.

Definiamo

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} : a \in \mathbb{Z}\}$$

o, equivalentemente,

$$\mathbb{Z}/n\mathbb{Z} = \{R_0, R_1, \ldots, R_{n-1}\}.$$

Dunque, gli elementi di $\mathbb{Z}/n\mathbb{Z}$ sono *sottoinsiemi di* $\mathbb{Z}$. Mettiamo una struttura di gruppo additivo su $\mathbb{Z}/n\mathbb{Z}$. Definiamo

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Questa definizione *non* dipende della scelta di a e b, ma soltanto delle *classi* $\overline{a}$ e $\overline{b}$: se prendiamo a' e b' tali che $\overline{a'} = \overline{a}$ e $\overline{b'} = \overline{b}$, allora $a' - a$ e $b' - b$ sono divisibili per n e dunque $(a' + b') - (a + b)$ è divisibile per n, da cui $\overline{a' + b'} = \overline{a + b}$. Si vede dunque che il risultato $\overline{a + b}$ non dipende dalla scelta dei rappresentanti delle classi $\overline{a}$ e $\overline{b}$.

La composizione è associativa perché l'addizione in $\mathbb{Z}$ è associativa:

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}).$$

L'elemento neutro è la classe $\overline{0}$ perché per ogni $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$:

$$\overline{0} + \overline{a} = \overline{0+a} = \overline{a}, \qquad \overline{a} + \overline{0} = \overline{a+0} = \overline{a}.$$

L'inverso della classe $\overline{a}$ è la classe $\overline{-a}$:

$$\overline{-a} + \overline{a} = \overline{(-a)+a} = \overline{0}, \qquad \overline{a} + \overline{-a} = \overline{a+(-a)} = \overline{0}.$$

Concludiamo che $\mathbb{Z}/n\mathbb{Z}$ è un gruppo con l'addizione. Siccome per $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$

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

il gruppo delle classi resto modulo n è commutatitivo.

2.14 Esempio. *Il gruppo moltiplicativo* $(\mathbb{Z}/n\mathbb{Z})^*$ *delle classi resto modulo* n.
Sia n un intero positivo. Definiamo

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \mathrm{mcd}(a, n) = 1\}.$$

Se $\overline{a'} = \overline{a}$ si ha che n divide $a' - a$ esiste dunque $k \in \mathbb{Z}$ tale che $a' - a = kn$. Per la Prop.1.6(*iii*) si ha $\mathrm{mcd}(a', n) = \mathrm{mcd}(a + kn, n) = \mathrm{mcd}(a, n)$. Questo dimostra che l'insieme $(\mathbb{Z}/n\mathbb{Z})^*$ è ben definito, cioè il valore di $\mathrm{mcd}(a, n)$ nella definizione non dipende della scelta di a ma soltanto della classe $\overline{a}$.

Mettiamo una struttura di gruppo *moltiplicativo* su $(\mathbb{Z}/n\mathbb{Z})^*$. Definiamo

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Anche questa definizione dipende, a priori, dalle scelte dei rappresentanti a e b. Vediamo, invece, che la moltiplicazione è ben definita: prendiamo a' e b' tali che $\overline{a'} = \overline{a}$ e $\overline{b'} = \overline{b}$, allora $a' - a$ e $b' - b$ sono divisibili per n. Scriviamo $a' = a + kn$ e $b' = b + ln$, per certi $k, l \in \mathbb{Z}$. Quindi

$$a' \cdot b' = (a + kn) \cdot (b + ln) = ab + aln + kbn + kln^2 = ab + (al + kb + kln) \cdot n.$$

Siccome la differenza di $a'b'$ e ab è divisibile per n, le classi $\overline{ab}$ e $\overline{a'b'}$ sono uguali. Concludiamo che la moltiplicazione è ben definita.

L'associatività segue, come nel caso del gruppo additivo $\mathbb{Z}/n\mathbb{Z}$, dall'associatività in $\mathbb{Z}$. Si verifica che l'elemento neutro è la classe $\overline{1}$. Dimostriamo che ogni classe $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ ha un inverso: siccome $\mathrm{mcd}(a, n) = 1$, esistono, per il Cor.1.8, interi x, y tali che

$$ax + ny = 1.$$

Questo implica che la differenza di ax e 1 è divisibile per n. In altre parole, le classi $\overline{ax} = \overline{a} \cdot \overline{x}$ e $\overline{1}$ sono uguali e si vede che $\overline{x}$ è l'inverso di $\overline{a}$.

Concludiamo che $(\mathbb{Z}/n\mathbb{Z})^*$ è un gruppo moltiplicativo. Definiamo

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*.$$

La funzione φ si dice la *funzione di Eulero*. Si vede che

$$\varphi(n) = \#\{a \in \{1, 2, \ldots, n\} : \mathrm{mcd}(a, n) = 1\}.$$

Per $n = 12$ si trova la seguente tavola:

	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Si vede che è la "stessa tavola del gruppo di Klein 2.12. Siccome la moltiplicazione di $(\mathbb{Z}/12\mathbb{Z})^*$ è associativa, abbiamo gratis una dimostrazione dal fatto che la composizione del gruppo V_4 di Klein è associativa.

2.15 Esempio. *Vettori.*
Sia n un intero positivo. L'addizione di vettori $\mathbf{v} = (v_1, \ldots, v_n)$ e $\mathbf{w} = (w_1, \ldots, w_n)$ nello spazio vettoriale $\mathbb{R}^n$ è data da

$$\mathbf{v} + \mathbf{w} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix}.$$

Con questa addizione lo spazio vettoriale $\mathbb{R}^n$ diventa un gruppo commutativo. L'elemento neutro è il vettore $\mathbf{0} = (0, \ldots, 0)$. L'inverso del vettore $\mathbf{v} = (v_1, \ldots, v_n)$ è $-\mathbf{v} = (-v_1, \ldots, -v_n)$.

Similmente, si può definire una struttura di gruppo additivo sullo spazio vettoriale complesso $\mathbb{C}^n$. Per $\mathbf{v} = (v_1, \ldots, v_n)$ e $\mathbf{w} = (w_1, \ldots, w_n)$ in $\mathbb{C}^n$ si definisce la somma come nel caso di $\mathbb{R}$. Per la teoria degli spazi vettoriali su $\mathbb{R}$ e $\mathbb{C}$ si veda il corso di geometria I.

2.16 Esempio. *Gruppi di mappe.*
Sia X un insieme. Sia $S(X)$ l'insieme delle *biiezioni* da X a X. Si definisce la composizione $f \circ g$ di $f, g \in S(X)$ per

$$(f \circ g)(x) = f(g(x)) \qquad \text{per ogni } x \in X.$$

Attenzione! $f \circ g$ significa "prima g e poi f:

$$(f \circ g): \quad X \xrightarrow{g} X \xrightarrow{f} X.$$

La composizione è associativa e l'elemento neutro è l'identità id_X, cioè l'applicazione $x \mapsto x$ per ogni $x \in X$. Siccome ogni biiezione ammette una mappa inversa, l'insieme $S(X)$ è un gruppo con questa composizione. Se X è l'insieme $\{1, 2, \ldots, n\}$ si scrive S_n per $S(X)$. Per una descrizione più approfondita dei gruppi S_n si veda il paragrafo $4, 4$ dei **Complementi agli appunti di teoria dei gruppi**.

Esercizi.

(2.A) Per i seguenti insiemi G e "composizioni $\circ$, vedere quali delle condizioni (G_0), (G_1), (G_2), (G_3) e (G_4) sono soddisfatte:

(i) $G = \{1, 2, 3, 4 \ldots\}$, $a \circ b = a^b$.

(ii) $G = \mathbb{R}$, $a \circ b = a + b + 3$,

(iii) $G = \mathbb{R}_{>1}$, $a \circ b = a^{\log(b)}$.

(iv) $G = \{-1, 0, 1\}$, $a \circ b = a + b$.

(v) $G = \{1, 2, 3, 4, \ldots\}$, $a \circ b = \max(a, b)$.

(vi) $G = \mathbb{R}^2$, $\binom{a}{b} \circ \binom{c}{d} = \binom{c+ad}{bd}$.

(vii) $G = \{0, 1, 2, 3, 4, 5\}$ e la composizione $a \circ b$ è data dalla seguenta tavola. La composizione $a \circ b$ è data dall'elemento che si trova sulla riga a e sulla colonna b:

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2
2	2	3	0	5	1	4
3	3	4	5	0	2	1
4	4	5	1	2	0	3
5	5	2	4	1	3	0

(2.B) Sia G un gruppo con elemento neutro e. Dimostrare: se un elemento $e' \in G$ soddisfa

$$ae' = e'a = a \qquad \text{per ogni } a \in G$$

allora $e' = e$.

(2.C) (i) Mostrare che l'equazione

$$ax = b$$

ha una unica soluzione $x \in G$. Questa soluzione è $x = a^{-1}b$. Similmente, Mostrare che esiste una unica soluzione $x \in G$ di $xa = b$, vale a dire $x = ba^{-1}$.

(ii) Provare che, nella tabella di composizione di un gruppo finito, ogni elemento compare esattamente una volta in ogni riga ed ogni colonna.

(2.D) Il *coniugato* $\overline{x}$ di un numero complesso $x = a + bi$, con $a, b \in \mathbb{R}$, è definito da $\overline{x} = a - bi$.

(i) Mostrare che

$$\overline{x + y} = \overline{x} + \overline{y}, \qquad \overline{xy} = \overline{x}\,\overline{y}.$$

per ogni $x, y \in \mathbb{C}$.

(ii) Definiamo $\mathrm{N}(x) = x\overline{x}$. Dimostrare che $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ per ogni $x, y \in \mathbb{C}$.

(2.E) (i) Dimostrare che l'insieme $\{+1, -1\} \subset \mathbb{R}^*$ è un gruppo moltiplicativo.

(ii) Dimostrare che l'insieme $\{+1, -1, +i, -i\} \subset \mathbb{C}^*$ è un gruppo moltiplicativo. Confrontare con il gruppo V_4 di Klein.

(iii) Mostrare che $\zeta = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$ soddisfa $\zeta^8 = 1$. Dimostrare che le potenze di ζ formano un gruppo moltiplicativo. Quanti elementi ha questo gruppo?

(2.F) Il *coniugato* $\overline{x}$ di un quaternione $x = a + bi + cj + dk \in \mathbb{H}$ con $a, b, c, d \in \mathbb{R}$ è definito da $\overline{x} = a - bi - cj - dk$.

(i) Far vedere che

$$\overline{x + y} = \overline{x} + \overline{y}, \qquad \overline{xy} = \overline{y} \cdot \overline{x}.$$

per ogni $x, y \in \mathbb{H}$.

(ii) Definiamo $\mathrm{N}(x) = x\overline{x}$. Dimostrare che $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ per ogni $x, y \in \mathbb{H}$.

(2.G) (*Associatività dei quaternioni.*) Siano $a, b, c, d \in \mathbb{R}$ e sia $x = a + bi + cj + dk \in \mathbb{H}$. Si ha

$$x = \alpha + \beta j$$

dove $\alpha = a + bi$ e $\beta = c + di$ sono in $\mathbb{C} \subset \mathbb{H}$. In questo esercizio scriviamo i quaternioni in questo modo.

(i) Sia $\alpha \in \mathbb{C}$ e sia $\overline{\alpha}$ il coniugato di α. (Veda Eserc.(2.D)). Mostrare

$$j\alpha = \overline{\alpha} j$$

(ii) Siano $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$. Dimostrare

$$(\alpha + \beta j)(\alpha' + \beta' j) = (\alpha\alpha' - \beta\overline{\beta'}) + (\alpha\beta' + \beta\overline{\alpha'})j.$$

(iii) Dimostrare l'associatività della moltiplicazione dei quaternioni. (Sugg. Utilizzare l'uguaglianza in (ii).)

(2.H) Sia x un elemento del gruppo Q dei quaternioni di ordine 8. Provare: se $x \neq \pm 1$, allora $x^2 = -1$.

(2.I) Sia n un intero positivo e siano $a, b \in \mathbb{Z}$. Mostrare che le seguenti affermazioni sono equivalenti:

(i) $\overline{a} = \overline{b}$,

(ii) n divide $a - b$,

(iii) a e b hanno lo stesso resto della divisione per n,

(iv) $a \in \overline{b}$,

(v) $b \in \overline{a}$,

(vi) $a \equiv b \bmod n$.

(2.J) Sia G un gruppo. Provare: se $x^2 = 1$ per ogni $x \in G$, allora G è abeliano.

(2.K) Sia G un gruppo.

(i) Provare: Se $a^{-1}b^{-1} = (ab)^{-1}$ per ogni $a, b \in G$, allora G è abeliano.

(ii) Provare: Se $a^2b^2 = (ab)^2$ per ogni $a, b \in G$, allora G è abeliano.

(iii) Sia $n \in \mathbb{Z}$. Mostrare che $a^n b^n = (ab)^n$ per ogni $a, b \in G$ se e soltanto se $a^{1-n}b^{1-n} = (ab)^{1-n}$ per ogni $a, b \in G$.

(iv) * Trovare un gruppo *non* abeliano G tale che $a^{-2}b^{-2} = (ab)^{-2}$.

(2.L) Sia G un gruppo e siano $a, b \in G$ con le proprietà:

$$aba^{-1} = b^2, \qquad bab^{-1} = a^2.$$

Dimostrare che $a = b = e$.

(2.M) Sia G un gruppo e sia X un insieme. Sia G^X l'insieme delle mappe $X \longrightarrow G$. Siano $f, g \in G^X$. Definiamo $f \circ g$ nel modo seguente:

$$(f \circ g)(x) = f(x)g(x) \qquad \text{per } x \in X.$$

(i) Dimostrare che G^X è un gruppo rispetto alla composizione $\circ$.

(ii) Dimostrare che G^X è commutativo se e soltanto se G è commutativo.

3 Sottogruppi, omomorfismi, prodotti

In questo paragrafo discuteremo vari metodi per costruire gruppi nuovi partendo da gruppi dati. Introduciamo gli omomorfismi fra gruppi.

3.1 Definizione. (*Sottogruppo*) Sia G un gruppo. Un sottoinsieme H di G si dice un *sottogruppo* di G se H è, con la stessa composizione e lo stesso elemento neutro di G, un gruppo.

3.2 Esempi. Per esempio, $\mathbb{Z}$ è un sottogruppo del gruppo additivo $\mathbb{R}$. Ogni gruppo G possiede i sottogruppi G e $\{e\}$: sono i sottogruppi *banali* di G. Prima da dare altri esempi, dimostriamo un criterio efficiente per decidere se un sottoinsieme H di G è un sottogruppo o meno.

3.3 Teorema. Sia G un gruppo e sia H un sottoinsieme di G. Allora le seguenti affermazioni sono equivalenti:

(*i*) H è un sottogruppo di G.

(*ii*) $H \neq \emptyset$ e

- per ogni $a, b \in H$ si ha $ab \in H$,
- per ogni $a \in H$ si ha $a^{-1} \in H$.

(*iii*) $H \neq \emptyset$ e per ogni $a, b \in H$ si ha $ab^{-1} \in H$.

Dimostrazione. Le implicazioni *(i)* $\Longrightarrow$ *(ii)* $\Longrightarrow$ *(iii)* sono banali.

Supponiamo *(iii)*. Siccome $H \neq \emptyset$, possiamo prendere $x \in H$. Ponendo $a = x$ e $b = x$ troviamo che $e = xx^{-1} \in H$. Dunque, l'elemento neutro è in H. Per $a = e$ e $b = x \in H$ un elemento qualsiasi, troviamo $x^{-1} = ex^{-1} \in H$. Dunque, per ogni $x \in H$ anche l'inverso x^{-1} è in H. Finalmente, siano $x, y \in H$ due elementi qualsiasi. Sappiamo già che y^{-1} è in H. Prendendo $a = x$ e $b = y^{-1}$ troviamo che $xy = x(y^{-1})^{-1} \in H$. Questo dimostra che *(iii)* implica *(ii)*.

Supponiamo *(ii)*. Siccome $ab \in H$ per ogni $a, b \in H$, l'insieme H è chiuso per la composizione di G. Inoltre, la restrizione della composizione di G è una composizione associativa di H. Come abbiamo gia visto l'elemento neutro è in H. Siccome per ogni $a \in H$ anche l'elemento inverso a^{-1} è in H concludiamo che H è un sottogruppo di G. Questo dimostra il teorema. □

3.4 Esempi.

(*i*) Sia $H \subset \mathbb{Z}$ l'insieme dei numeri pari. Ovviamente $H \neq \emptyset$ e $a - b \in H$ per ogni $a, b \in H$. Per il Teorema 3.3(*iii*), l'insieme H è un sottogruppo di $\mathbb{Z}$. L'insieme dei numeri dispari, invece, non è un sottogruppo di $\mathbb{Z}$, perché non contiene lo zero.

(*ii*) Se x, y sono numeri reali positivi, il quoziente x/y è positivo. Dunque, per il Teorema 3.3(*iii*), l'insieme $\mathbb{R}_{>0}$ dei numeri reali positivi è un sottogruppo di $\mathbb{R}^*$.

(*iii*) L'insieme $\{\pm 1, \pm i\}$ è un sottogruppo del gruppo Q dei quaternioni.

(*iv*) Sia n un intero positivo. Sia $k \in \{1, 2, \ldots, n\}$ e sia H il sottoinsieme di S_n (vedi l'Esempio 2.16) dato da

$$H = \{\sigma \in S_n : \sigma(k) = k\}.$$

Lasciamo al lettore la verifica che H è un sottogruppo di S_n.

3.5 Esempio. Un esempio di sottogruppo importante è il *centro* di un gruppo: Sia G un gruppo. Il *centro* (in tedesco: *Zentrum*) $Z(G)$ di G è il sottogruppo

$$Z(G) = \{g \in G : gh = hg \quad \text{per ogni } h \in G\}.$$

Lasciamo al lettore la verifica che $Z(G)$ è un sottogruppo di G.

3.6 Teorema.

(*i*) I sottogruppi di $\mathbb{Z}$ sono $\{0\}$ e gli insiemi

$$d\mathbb{Z} = \{\ldots, -2d, -d, 0, d, 2d, 3d, \ldots\}$$

per d un intero positivo. I sottogruppi $d\mathbb{Z}$ sono diversi fra loro.

(*ii*) Sia n un intero positivo. I sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono

$$H_d = \{\overline{d}, \overline{2d}, \ldots, \overline{n-d}, \overline{0}\}$$

dove d è un divisore positivo di n. I sottogruppi H_d sono diversi fra loro.

Dimostrazione. *(i)* Sia H un sottogruppo di $\mathbb{Z}$. Allora $0 \in H$. Se H non contiene altri elementi, abbiamo $H = \{0\}$. Supponiamo che $a \neq 0$ sia in H. Siccome anche $-a \in H$, vediamo che H contiene elementi positivi. Sia d il più piccolo elemento positivo di H. Siccome H è un gruppo, ogni multiplo di d è in H; cioè $d\mathbb{Z} \subset H$.

Affermiamo che è anche $H \subset d\mathbb{Z}$, vale a dire che ogni elemento $a \in H$ è divisibile per d. Infatti, sia $a \in H$ e dividiamo a per d con resto r, sfruttando il Teorema 1.2:

$$a = qd + r \qquad \text{con } q, r \in \mathbb{Z} \quad \text{e} \quad 0 \leq r < d.$$

Poiché H è un gruppo, $r = a - qd$ è in H. Siccome $0 \leq r < d$ per la minimalità di d concludiamo che $r = 0$ e che d divide a come richiesto.

I sottogruppi $d\mathbb{Z}$ sono diversi fra loro perché sono caratterizzati da d: l'intero d è l'elemento positivo minimo in $d\mathbb{Z}$.

(ii) Sia H un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$. Definiamo

$$H' = \{a \in \mathbb{Z} : \overline{a} \in H\}.$$

Siccome H è un sottogruppo, contiene l'elemento neutro $\overline{0}$. Questo implica che $0 \in H'$. Siano $a, b \in H'$, allora $\overline{a}, \overline{b} \in H$. Siccome H è un sottogruppo, $\overline{a-b} \in H$ e dunque $a - b \in H'$. Questo dimostra che H' è un sottogruppo di $\mathbb{Z}$. Siccome $\overline{0} = \overline{n} \in H$ abbiamo $n \in H'$. Dunque $H' \neq \{0\}$ e per la prima parte abbiamo che $H' = d\mathbb{Z}$ per un intero positivo d. Siccome $n \in H'$, abbiamo che d divide n.

Lasciamo la facile verifica che i gruppi H_d sono tutti distinti al lettore. Questo finisce la dimostrazione di *(ii)*. □

3.7 Definizione. (*Omomorfismo*) Siano G e G' due gruppi. Una applicazione $f : G \longrightarrow G'$ si dice un *omomorfismo* se

$$f(ab) = f(a)f(b) \qquad \text{per ogni } a, b \in G.$$

Si noti che il prodotto ab è in G, ma il prodotto $f(a)f(b)$ è in G'. Un omomorfismo $f : G \longrightarrow G'$ che è una biiezione si dice un *isomorfismo.* In tal caso si dice che i gruppi G e G' *sono isomorfi.* Un omomorfismo $f : G \longrightarrow G$ si dice un *endomorfismo* di G. Un endomorfismo biiettivo di G si dice un *automorfismo* di G.

3.8 Esempi.

(*i*) Sia $G = G' = \mathbb{R}^*$ e sia $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ la funzione data da $f(x) = x^2$. Quest'omomorfismo è un endomorfismo. Non è un automorfismo perché non è suriettivo.

(*ii*) Sia $f : \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ data da $f(x) = \log(x)$. Siccome

$$\log(xy) = \log(x) + \log(y)$$

la funzione f è un omomorfismo. L'applicazione inversa è data da $y \mapsto e^y$. Dunque f è un isomorfismo: i gruppi $\mathbb{R}_{>0}$, con la moltiplicazione, e $\mathbb{R}$, con l'addizione, sono gruppi isomorfi.

(*iii*) Sia H un sottogruppo di G. L'applicazione $f : H \longrightarrow G$ data da $f(x) = x$ è un omomorfismo.

(*iv*) Sia n un intero positivo. L'applicazione $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ data da $a \mapsto \overline{a}$ è un omomorfismo.

(*v*) Sia V_4 il gruppo di Klein. L'applicazione $f : (\mathbb{Z}/12\mathbb{Z})^* \longrightarrow V_4$ data da

$$\overline{1} \mapsto e \qquad \overline{5} \mapsto a \qquad \overline{7} \mapsto b \qquad \overline{11} \mapsto c$$

è un isomorfismo (si vedano gli Esempi 2.12 e 2.14).

(*vi*) Sia G un gruppo e sia $g \in G$. L'applicazione

$$f : \mathbb{Z} \longrightarrow G$$

definita da $n \mapsto g^n$ è un omomorfismo.

3.9 Teorema. Sia G un gruppo con elemento neutro e e sia G' un gruppo con elemento neutro e'. Sia $f : G \longrightarrow G'$ un omomorfismo. Allora

(*i*) $f(e) = e'$.

(*ii*) $f(a^{-1}) = f(a)^{-1}$.

Dimostrazione. Abbiamo $f(e) = f(e \cdot e) = f(e)f(e)$. Dunque

$$e' = f(e)^{-1}f(e) = f(e)^{-1}\left(f(e)f(e)\right) = \left(f(e)^{-1}f(e)\right)f(e) = e'f(e) = f(e)$$

come richiesto.
(ii) Come conseguenza della parte *(i)* abbiamo

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'.$$

Siccome l'elemento inverso di $f(a)$ è unico, concludiamo che $f(a^{-1}) = f(a)^{-1}$. □

3.10 Definizione. Siano G e G' due gruppi con elementi neutri rispettivamente e ed e'. Sia $f : G \longrightarrow G'$ un omomorfismo. Il *nucleo* (in inglese: *kernel*) $\ker(f)$ di f è il sottoinsieme di G definito da

$$\ker(f) = \{a \in G : f(a) = e'\}.$$

L'*immagine* $f(G)$, denotata anche con il simbolo $\mathrm{im}(f)$, è il sottoinsieme di G' definito da

$$f(G) = \{f(a) : a \in G\}.$$

3.11 Teorema. Siano G e G' gruppi con elementi neutri rispettivamente e ed e'. Se $f : G \longrightarrow G'$ un omomorfismo, allora

(*i*) Il nucleo $\ker(f)$ è un sottogruppo di G.

(*ii*) L'immagine $f(G)$ è un sottogruppo di G'.

(*iii*) f è iniettiva se e soltanto se $\ker(f) = \{e\}$.

Dimostrazione. *(i)* Per il Teorema 3.9, l'elemento neutro e è in $\ker(f)$. Dunque $\ker(f) \neq \emptyset$. Se $x, y \in \ker(f)$, allora $f(xy^{-1}) = f(x)f(y)^{-1} = e'e'^{-1} = e'$, cioè $xy^{-1} \in \ker(f)$. Il punto *(i)* segue ora dal Teorema 3.3(*iii*).
(ii) Per il Teorema 3.9, l'elemento e' è in $f(G)$. Dunque $f(G)$ non è vuoto. Se $x, y \in f(G)$, esistono $a, b \in G$ tali che $f(a) = x$ e $f(b) = y$. Dunque $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(G)$ e *(ii)* segue dal Teorema 3.3(*iii*).
(iii) Supponiamo che f sia iniettiva. Per il Teorema 3.9 abbiamo sempre $\{e\} \subset \ker(f)$. Per dimostrare l'inclusione opposta, prendiamo $x \in \ker(f)$. Allora $f(x) = e'$. Ma vale anche $f(e) = e'$ e per l'iniettività segue $x = e$, come richiesto.

Supponiamo adesso $\ker(f) = \{e\}$ e assumiamo $f(x) = f(y)$ per certi $x, y \in G$. Allora $f(xy^{-1}) = f(x)f(y)^{-1} = e'$ e quindi $xy^{-1} \in \ker(f)$. Perciò $xy^{-1} = e$ e dunque $x = y$. Questo finisce la dimostrazione del Teorema 3.11. □

Nel prossimo teorema stabiliamo qualche proprietà importante degli *isomorfismi*.

3.12 Teorema.

(*i*) Siano G, G', G'' tre gruppi. Se $f : G \longrightarrow G'$ e $g : G' \longrightarrow G''$ sono isomorfismi, allora l'applicazione $(g \circ f) : G \longrightarrow G''$ è un isomorfismo.

(*ii*) Siano G, G' gruppi. Se $f : G \longrightarrow G'$ è un ismorfismo, allora la mappa inversa $f^{-1} : G' \longrightarrow G$ è un isomorfismo.

Dimostrazione. *(i)* È ovvio che la composizione di due omomorfismi è un omomorfismo ed è noto che la composizione di due biiezioni è una biiezione. Questo dimostra *(i)*.
(ii) Siccome f è una biiezione, l'applicazione inversa f^{-1} esiste. Abbiamo

$$f(f^{-1}(ab)) = ab = f(f^{-1}(a))f(f^{-1}(b)) = f(f^{-1}(a)f^{-1}(b))$$

e dunque, per l'iniettività di f,

$$f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$$

come richiesto. □

3.13 Definizione. (*Prodotto di gruppi*) Siano G_1 e G_2 due gruppi. Sul prodotto Cartesiano $G_1 \times G_2$ definiamo la composizione

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

dove $g_1, g_1' \in G_1$ e $g_2, g_2' \in G_2$. È immediato verificare che l'insieme $G_1 \times G_2$ con tale composizione è un gruppo, detto *il prodotto di* G_1 *e* G_2.

3.14 Esempi.

(*i*) Prendiamo $G = G' = \mathbb{R}$. Allora $G \times G' = \mathbb{R} \times \mathbb{R}$ è isomorfo allo spazio vettoriale $\mathbb{R}^2$ dell'Esempio 2.15.

(*ii*) Prendiamo $G = G' = \mathbb{Z}/2\mathbb{Z}$. La tavola di composizione del gruppo prodotto $G \times G'$, cioè di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ è data da:

	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{0})$	$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{0})$
$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$
$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{0})$

Si vede che questo gruppo è isomorfo al gruppo V_4 di Klein (Esempio 2.12). Più precisamente l'applicazione data da

$$e \mapsto (\overline{0}, \overline{0}) \qquad a \mapsto (\overline{0}, \overline{1}) \qquad c \mapsto (\overline{1}, \overline{0}) \qquad d \mapsto (\overline{1}, \overline{1})$$

è un isomorfismo da V_4 a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Non è l'unico isomorfismo.

3.15 Prima di formulare il prossimo teorema studiamo, per $n, d \in \mathbb{Z}_{>0}$, e d un divisore di n, l'applicazione *canonica*

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$$

data da

$$a \bmod n \mapsto a \bmod d.$$

Utilizziamo la notazione $a \bmod n$ piuttosto di $\overline{a}$ per indicare la dipendenza da n. La definizione dell'applicazione canonica dipende, a priori, dalla scelta del rappresentante a della classe $a \bmod n$. In realtà, essa è ben definita perché d divide n. Infatti, se le classi di a e a' in $\mathbb{Z}/n\mathbb{Z}$ sono uguali, la differenza di a e a' è divisibile per n (Eserc. (2.I)) e quindi anche divisibile per d. Questo implica che le classi di a e a' modulo d sono uguali, perciò l'applicazione è ben definita. È banale verificare che si tratta di un omomorfismo.

Si noti però che la 'regola' $a \bmod 3 \longmapsto a \bmod 2$ non è ben definita, infatti si ha $0 \bmod 3 = 3 \bmod 3$ però $0 \bmod 2$ *non* è uguale a $3 \bmod 2$. La condizione che d divide n è essenziale.

3.16 Teorema. (*Teorema cinese del resto*) Siano n, m due interi maggiori di 1 con $\mathrm{mcd}(n, m) = 1$. Allora l'applicazione

$$f : \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

data da

$$f(a \bmod nm) = (a \bmod n, a \bmod m)$$

è un'isomorfismo.

Dimostrazione. Come abbiamo osservato sopra: siccome n e m dividono nm, l'applicazione f è ben definita ed è un omomorfismo. Sia $a \bmod nm \in \ker(f)$. Abbiamo $a \equiv 0 \bmod n$ e $a \equiv 0 \bmod m$, cioè n ed m dividono a. Esistono quindi $u, v \in \mathbb{Z}$ tali che $a = un$ e $a = vm$.

Siccome $\mathrm{mcd}(n, m) = 1$, esistono per il Cor.1.8 due interi $x, y \in \mathbb{Z}$ tali che $nx + my = 1$. Moltiplicando per a otteniamo

$$a = anx + amy = (vm)nx + (un)my = (vx + uy)nm.$$

Quindi nm divide a. In altre parole è $a \equiv 0 \bmod nm$. Per il Teorema 3.11, l'omomorfismo f è iniettivo. Siccome le cardinalità di $\mathbb{Z}/nm\mathbb{Z}$ e di $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sono entrambe uguali a nm, si conclude che f è una biiezione come richiesto. $\square$

3.17 Corollario. (*Teorema cinese del resto*) Siano n, m due interi positivi con $\mathrm{mcd}(n, m) = 1$ e siano $\alpha, \beta \in \mathbb{Z}$. Allora esiste $z \in \mathbb{Z}$ tale che

$$z \equiv \alpha \bmod n, \qquad \text{e} \quad z \equiv \beta \bmod m.$$

L'intero z è unico modulo nm.

Dimostrazione. La prima affermazione è equivalente alla suriettività della mappa f del Teorema 3.16 e la seconda alla iniettività. □

Esercizi.

(3.A) Sia G un gruppo *finito* e sia $H \subset G$. Provare: se $H \neq \emptyset$ e se $ab \in H$ per ogni $a, b \in H$, allora H è un sottogruppo di G.

(3.B) Determinare quali sottoinsiemi sono sottogruppi:

(i) $\mathbb{Q}_{>0} \subset \mathbb{Q}^*$,

(ii) $\{1, i, j, k\} \subset Q$,

(iii) $\{\pm 1, \pm i\} \subset \mathbb{C}^*$

(iv) $\{z \in \mathbb{C} : z\overline{z} = 1\} \subset \mathbb{C}^*$,

(3.C) Dimostrare che un sottogruppo di un gruppo abeliano è abeliano. Dare un esempio di un gruppo non abeliano con sottogruppo abeliano non banale.

(3.D) (i) Sia G un gruppo e sia $\{H_\alpha : \alpha \in A\}$ una famiglia di sottogruppi di G. Dimostrare che $\cap_\alpha H_\alpha = \{h : h \in H_\alpha \quad \text{per ogni } \alpha \in A\}$ è un sottogruppo di G.

(ii) Sia G un gruppo e siano $H \subset G$ e $H' \subset G$ due sottogruppi. Dimostrare: se $G = H \cup H'$ allora $G = H$ oppure $G = H'$.

(iii) Dimostrare che il gruppo V_4 di Klein ha 3 sottogruppi H_1, H_2 e H_3 diversi da V_4 tali che $G = H_1 \cup H_2 \cup H_3$.

(3.E) Siano G, G' gruppi e sia $f : G \longrightarrow G'$ un omomorfismo. Dimostrare

(i) Se H è un sottogruppo di G allora $f(H) = \{f(h) : h \in H\}$ è un sottogruppo di G'.

(ii) Se H è un sottogruppo di G' allora $f^{-1}(H) = \{h \in G : f(h) \in H\}$ è un sottogruppo di G.

(3.F) Sia G un gruppo e sia $g \in G$.

(i) Dimostrare che l'applicazione data da $x \mapsto gxg^{-1}$ è un endomorfsimo di G.

(ii) Sia $H \subset G$ un sottogruppo. Dimostrare che $gHg^{-1} = \{gxg^{-1} : x \in H\}$ è un sottogruppo di G.

(3.G) (*Il Centro*)

(i) Dimostrare: se G è abeliano allora $Z(G) = G$.

(ii) Dimostrare che il centro di Q è $\{1, -1\}$.

(iii) Calcolare il centro di D_n.

(3.H) Dimostrare che le seguenti applicazioni sono omomorfismi:

(i) $\mathbb{C} \longrightarrow \mathbb{C}$, $a + bi \mapsto a - bi$,

(ii) $\mathbb{C}^* \longrightarrow \mathbb{C}^*$, $a + bi \mapsto a - bi$,

(iii) $\mathbb{C}^* \longrightarrow \mathbb{R}^*$, $a + bi \mapsto a^2 + b^2$,

(iv) $\mathbb{R}^* \longrightarrow \mathbb{R}^*$, $x \mapsto |x|$,

(v) $\mathbb{Z}/10\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$, $x \bmod 10 \mapsto x \bmod 5$,

(vi) $(\mathbb{Z}/10\mathbb{Z})^* \longrightarrow (\mathbb{Z}/5\mathbb{Z})^*$, $x \bmod 10 \mapsto x \bmod 5$,

(vii) $\mathbb{R} \longrightarrow \mathbb{C}^*$, $x \mapsto \cos(x) + \operatorname{sen}(x)i$,

(viii) $\mathbb{Z}/4\mathbb{Z} \longrightarrow (\mathbb{Z}/5\mathbb{Z})^*$, $x \mapsto 2^x$.

Quali sono iniettive e quali suriettive?

(3.I) Sia G un gruppo. Dimostrare che l'applicazione $F : G \longrightarrow G$ data da $F(x) = x^2$ è un omomorfismo se e soltanto se G è abeliano. Dimostrare che l'applicazione $x \mapsto x^{-1}$ è un'omomorfismo se e soltanto se G è abeliano.

(3.J) Determinare i nuclei e le immagini degli omomorfismi nell'Eserc. (3.H).

(3.K) (i) Siano G_1 e G_2 due gruppi con un solo elemento. Dimostrare che G_1 e G_2 sono isomorfi.

(ii) Come (i), ma G_1 e G_2 hanno due elementi.

(iii) È anche vero quando G_1 e G_2 hanno 3 elementi? 4 elementi?

(3.L) Dimostrare che $\mathbb{R} \times \mathbb{R} \cong \mathbb{C}$. Dimostrare che $\mathbb{H} \cong \mathbb{R}^4$.

(3.M) Sia G un gruppo e siano H e H' due sottogruppi con le seguenti proprietà:

(i) $hh' = h'h$ per ogni $h \in H$, $h' \in H'$,

(ii) $H \cap H' = \{e\}$,

(iii) Per ogni $g \in G$ ci sono $h \in H$ e $h' \in H'$ tali che $g = hh'$.

Dimostrare che l'applicazione

$$f : H \times H' \longrightarrow G$$

data da $f(h, h') = hh'$ è un isomorfismo.

(3.N) (i) Trovare $n \in \mathbb{Z}$ con $0 \leq n \leq 1000$ tale che

$$n \equiv 3 \bmod 7, \quad n \equiv 4 \bmod 11, \quad n \equiv 8 \bmod 13.$$

Dimostrare che l'intero n è unico.

(ii) Trovare $n \in \mathbb{Z}$ tale che

$$n \equiv 12 \bmod 13,\ n \equiv 16 \bmod 17,\ n \equiv 18 \bmod 19,\ n \equiv 22 \bmod 23,\ n \equiv 28 \bmod 29.$$

4 Generatori, ordine e indice

4.1 In questo paragrafo parleremo di generatori di gruppi e gruppi ciclici. Poi introdurremo l'ordine di un gruppo e di un elemento di un gruppo. Concluderemo con le classi laterali e l'indice di un sottogruppo di un gruppo.

4.2 Definizione. Sia G un gruppo e sia X un sottoinsieme di G. L'insieme che consiste di tutti i prodotti $x_1 \cdot x_2 \cdot \ldots \cdot x_m$ dove $x_i \in X$ oppure $x_i^{-1} \in X$ è un sottogruppo di X. Esso si denota con $< X >$ e si dice il sottogruppo *generato da* X.

È facile vedere che $< X > \subset G$ è un sottogruppo. Se $X = \emptyset$ poniamo $< X >= \{e\}$. Se X contiene un solo elemento, si scrive $< x >$ per $< \{x\} >$. Se il sottogruppo generato da X è uguale a G, si dice che G è generato da X.

4.3 Definizione. Un gruppo G si dice *ciclico* se è generato da un solo elemento. Cioè G è ciclico se esiste $x \in G$ tale che $G =< x >$. In questo caso x si dice un *generatore* di G.

4.4 Esempi. Il gruppo $\mathbb{Z}$ è un gruppo ciclico. È generato da 1, ma anche da -1. I gruppi $\mathbb{Z}/m\mathbb{Z}$ sono ciclici. Sono tutti generati da $\overline{1}$. In generale, il gruppo $\mathbb{Z}/m\mathbb{Z}$ ha diversi generatori. Si veda l'Eserc.(4.E) per maggiori dettagli. Altri esempi sono il gruppo $\{\pm 1, \pm i\} \subset \mathbb{C}^*$ con generatore i e $(\mathbb{Z}/7\mathbb{Z})^*$ con generatore $\overline{3}$. Invece, il gruppo V_4 di Klein non è ciclico. Neppure $\mathbb{R}$ nè S_3 sono ciclici.

4.5 Definizione. (*Ordine*)

(*i*) Sia G un gruppo. *L'ordine* $\#G$ di G è la cardinalità dell'insieme G.

(*ii*) Sia G un gruppo e sia $x \in G$. *L'ordine* $\mathrm{ord}(x)$ di x è il più piccolo intero positivo m tale che

$$x^m = e.$$

Se per $x \in G$ non esiste un intero $m > 0$ tale che $x^m = e$, si dice che l'ordine di x è infinito.

Ogni gruppo contiene esattamente un elemento di ordine 1: l'elemento neutro.

4.6 Proposizione. Sia G un gruppo e sia $x \in G$ di ordine finito m. Sia $n \in \mathbb{Z}$. Allora

$$x^n = e$$

se e soltanto se m divide n.

Dimostrazione. Se m divide n allora

$$x^n = (x^m)^{n/m} = e^{n/m} = e.$$

Per dimostrare il viceversa, dividiamo n per l'ordine m con quoziente q e resto r:

$$n = qm + r \qquad \text{con } 0 \leq r < m.$$

Ora abbiamo

$$x^r = x^{n-qm} = x^n \cdot (x^m)^{-q} = e \cdot e^{-q} = e.$$

Siccome m è il minimo intero positivo tale che $x^m = e$, concludiamo che $r = 0$ e che m divide n come richiesto. □

Ora proviamo che ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/m\mathbb{Z}$ per un intero positivo m.

4.7 Teorema. Sia G un gruppo e sia $x \in G$.

(*i*) $< x > \cong \mathbb{Z}$ se l'ordine di x è infinito.

(*ii*) $< x > \cong \mathbb{Z}/m\mathbb{Z}$ se l'ordine di x è m.

(*iii*) Se G è ciclico allora $G \cong \mathbb{Z}$ oppure $G \cong \mathbb{Z}/m\mathbb{Z}$.

Dimostrazione. *(i)* Consideriamo l'omomorfismo

$$f : \mathbb{Z} \longrightarrow G$$

dato da $f(n) = x^n$. (si veda l'Esempio 3.8(*vi*).) Per definizione, l'immagine di f è uguale a $< x >$. Il nucleo di f consiste degli interi m tali che $x^m = 1$. Dunque, se l'ordine di x è infinito, il nucleo è uguale a $\{0\}$ e la mappa f è un omomorfismo iniettivo. Segue che la mappa $f : \mathbb{Z} \longrightarrow < x >$ è un isomorfismo. *(ii)* Definiamo un'applicazione

$$f : \mathbb{Z}/m\mathbb{Z} \longrightarrow < x >$$

con

$$f(\overline{a}) = x^a.$$

Verifichiamo che f è ben definita, cioè che non dipende della scelta del rappresentante a: se $\overline{a} = \overline{b}$ allora m divide $a - b$ e quindi $b = a + km$, per un certo $k \in \mathbb{Z}$. Adesso abbiamo

$$x^b = x^{a+km} = x^a \cdot x^{km} = x^a \cdot (x^m)^k = x^a \cdot e^k = x^a.$$

L'applicazione f è ovviamente un omomorfismo suriettivo. Affermiamo che è anche iniettiva: sia $\overline{n}$ in $\ker(f)$. Allora $x^n = e$. Per la Prop.4.6, l'ordine m divide n, cioè $\overline{n} = \overline{0}$. Concludiamo che f è iniettiva.
(iii) è una consequenza immediata di *(i)* e *(ii)*. Questo completa la dimostrazione del Teorema 4.7. □

4.8 Corollario. Sia G un gruppo e sia $x \in G$. Allora

$$\text{ord}(x) = \# < x >$$

cioè, l'ordine dell'elemento x è uguale all'ordine del gruppo generato da x.

Dimostrazione. Si tratta di una conseguenza immediata del teorema precedente. □

4.9 Definizione. Sia H un sottogruppo di un gruppo G e sia $g \in G$. L'insieme

$$gH = \{gh : h \in H\}$$

si dice una *classe laterale sinistra* (in inglese: *left coset*) di H e

$$Hg = \{hg : h \in H\}$$

si dice una *classe laterale destra* (in inglese: *right coset*) di H. Si indica con G/H l'insieme delle classi laterali sinistre e con H/G l'insieme delle classi laterali destre. Se G è commutativo si ha $gH = Hg$ e si parla semplicemente di *classe laterale* di H. Se G non è commutativo l'uguaglianza $gH = Hg$ non è garantita; la questione dipende da H.

4.10 Esempi.

(*i*) Prendiamo $G = \mathbb{R}^*$ e H il sottogruppo $\mathbb{R}^*_{>0}$. Se $x \in \mathbb{R}^*$ è positivo, allora la classe laterale $x\mathbb{R}^*$ è uguale a $\mathbb{R}^*_{>0}$. Se invece $x < 0$, la classe $x\mathbb{R}^*$ è uguale a $\mathbb{R}^*_{<0}$. Ci sono dunque soltanto due classi laterali diverse: l'insieme dei numeri positivi e quello dei numeri negativi. Sono classi sia sinistre che destre perché il gruppo $\mathbb{R}^*$ è commutativo.

(*ii*) Prendiamo $G = \mathbb{Z}$ e $H = d\mathbb{Z}$ per un intero positivo d (si veda il Teorema 3.6). Il gruppo $\mathbb{Z}$ è un gruppo *additivo.* Abbiamo dunque per $a \in \mathbb{Z}$ la classe laterale

$$a + d\mathbb{Z} = \{a + dk : k \in \mathbb{Z}\}.$$

Siccome $\mathbb{Z}$ è un gruppo *commutativo,* la classe $a + d\mathbb{Z}$ è sia sinistra che destra. Le classi laterali $a + d\mathbb{Z}$ e $a' + d\mathbb{Z}$ sono uguali se e soltanto se $a' \equiv a \bmod d$. Quindi per $0 \leq a < d$ le classi laterali $a + d\mathbb{Z} = \{a + dk : k \in \mathbb{Z}\}$ sono distinte. La loro lista esaurisce tutte le classi laterali di H.

(*iii*) Sia $G = \mathbb{R}^2$ e sia $\mathbf{v} \neq \mathbf{0}$ un vettore in G. Consideriamo il sottoinsieme di G definito da

$$H = \{\lambda\mathbf{v} : \lambda \in \mathbb{R}\}.$$

L'insieme H è una retta per $\mathbf{0}$ in $\mathbb{R}^2$. Lasciamo al lettore la verifica che H è un sottogruppo di G. Sia $\mathbf{w}$ un vettore in G. La classe laterale di H e data da

$$\mathbf{w} + H = \{\mathbf{w} + \lambda\mathbf{v} : \lambda \in \mathbb{R}\}$$

è una retta parallela a H. Dunque le classi laterali di H sono esattamente le rette in $\mathbb{R}^2$ parallele a H.

(*iv*) Nei primi tre esempi il gruppo G è sempre commutativo, così le classi laterali sinistre e destre sono uguali. Adesso studiamo un esempio non commutativo: Prendiamo $G = S_3$ e sia $H = \{(1), (2\,3)\}$ il sottogruppo delle permutazioni che fissano 1. Per $a = (1\,2\,3)$ troviamo

$$\begin{aligned} aH &= \{(1\,2\,3), (1\,2)\} \\ Ha &= \{(1\,2\,3), (1\,3)\} \end{aligned}.$$

Si vede che la classe laterale sinistra aH non è uguale alla classe laterale destra Ha.

4.11 Teorema. Sia H un sottogruppo di un gruppo G.

(*i*) Siano $a, b \in G$. Allora $aH = bH$ se e soltanto se $a^{-1}b \in H$.

(*ii*) Siano $a, b \in G$. Allora $aH = bH$ oppure $aH \cap bH = \emptyset$.

(*iii*) Ogni $x \in G$ è contenuto in una classe laterale sinistra aH di G.

Le classi laterali sinistre ripartiscono G in sottoinsiemi disgiunti.

Dimostrazione. *(i)* Se $aH = bH$, allora $ah = be$ per un certo $h \in H$ e dunque $a^{-1}b = h \in H$. Viceversa: siccome $a^{-1}b = h \in H$, abbiamo $b = ah$ e anche $a = bh^{-1}$. Se $x \in aH$, allora $x = ah_1$ per un $h_1 \in H$ e dunque $x = ah_1 = bh^{-1}h_1 \in bH$. Similmente, se $x \in bH$, allora $x = bh_2$ per un $h_2 \in H$ e dunque $x = bh_2 = ahh_2 \in aH$. Questo dimostra *(i)*.
(ii) Supponiamo che $aH \cap bH \neq \emptyset$. Sia $z \in aH \cap bH$, allora $z = ah = bh_1$ per certe h, $h_1 \in H$. Da $ah = bh_1$ segue $a^{-1}b = hh_1^{-1}$. Dato che H è un sottogruppo di G si ha $a^{-1}b = hh_1^{-1} \in H$, quindi $aH = bH$ per *(i)*.
(iii) Sia $x \in G$. Allora $x = xe \in xH$, quindi x è contenuto nella classe laterale xH.

Da *(ii)* e *(iii)* segue che ogni $x \in G$ appartiene ad un unico classe laterale sinistra, quindi otteniamo una decomposizione di G come unione di classi laterali disgiunte. Questo conclude la dimostrazione del Teorema 4.11. □

4.12 Si potrebbe dire che il Teorema 4.11 segue dal fatto che la relazione $\sim$ su G data da

$$a \sim b \quad \Longleftrightarrow \quad a^{-1}b \in H,$$

è una *relazione di equivalenza*. Le classi di equivalenza sono le classi laterali sinistre. La decomposizione di G, come unione di classi laterali disgiunte, è l'usuale partizione in classi di equivalenza.

4.13 Vale un analogo del Teorema 4.11 per le classi laterali destre prendendo la relazione $a \sim b$ se $ab^{-1} \in H$. La prima parte del teorema diventa in tal caso: $Ha = Hb$ se e soltanto se $ab^{-1} \in H$.

4.14 Teorema. Sia H un sottogruppo di un gruppo G. Sia $a \in G$. L'applicazione

$$f : H \longrightarrow aH$$

data da $f(h) = ah$ è una biiezione.

Dimostrazione. La mappa f è suriettiva per definizione della classe laterale $aH = \{ah : h \in H\}$. Supponiamo che $f(h) = f(h')$ per $h, h' \in H$. Allora $ah = ah'$ e dunque $h = h'$. Quindi f è una iniezione e concludiamo che è una biiezione. Si noti che se $a \notin H$, l'applicazione f non è un omomorfismo. L'insieme aH non è neanche un gruppo! □

4.15 Definizione. Sia H un sottogruppo di G. Allora *l'indice* $[G : H]$ è il numero delle classi laterali sinistre di H. Un *sistema di rappresentanti per le classi laterali sinistre di H* è un sottoinsieme S di G che contiene esattamente un elemento in ogni classe laterale sinistra. Per un tale S si ha

$$G = \bigcup_{s \in S} sH$$

e

$$[G : H] = \#S.$$

Un sistema di rappresentanti non è unico. Ce ne sono, in generale, tanti.

4.16 Utilizzeremo l'indice quasi esclusivamente nel caso in cui esso è finito, cioè, quando ci sono soltanto un numero *finito* di classi laterali. Però, tutti i teoremi seguenti valgono in generale, vale a dire per cardinalità anche infinite. Si veda l'Eserc.(4.K) per il fatto che $[G : H]$ è anche uguale al numero delle classei laterali destre di H.

4.17 Esempio.

(*i*) Nell'esempio 4.10(*i*) abbiamo considerato il sottogruppo $H = \mathbb{R}^*_{>0}$ di $G = \mathbb{R}^*$. In questo caso l'indice $[G : H]$ è uguale a 2. Un sistema di rappresentanti delle classi laterali di H è $\{x, y\}$ dove $x, y \in \mathbb{R}^*$ con $x > 0$ e $y < 0$.

(*ii*) Consideriamo, come nell'esempio 4.10(*ii*), il sottogruppo $H = d\mathbb{Z}$ in $G = \mathbb{Z}$. Allora l'indice $[G : H]$ è d. Un sistema S di rappresentanti è dato da $S = \{1, 2, \ldots, d-1\}$.

(*iii*) Sia ora $G = S_3$ e $H = \{(1), (1\,2)\}$. Le classi laterali sinistre di H sono

$$\begin{aligned} H &= \{(1), (1\,2)\}, \\ aH &= \{(1\,2\,3), (1\,3)\}, \\ a^2H &= \{(1\,3\,2), (2\,3)\} \end{aligned}$$

dove $a = (1\,2\,3)$. Dunque, in questo caso $[G : H] = 3$.

4.18 Teorema. (J. Lagrange) Sia G un gruppo e sia H un sottogruppo di G. Allora

$$\#G = \#H \cdot [G : H].$$

Dimostrazione. Sia S un sistema di rappresentanti per le classi laterali sinistre di H. Per il Teorema 4.11 le classi laterali sinistre sH con rappresentanti in S sono disgiunte ed il gruppo

G è l'unione delle classi laterali sinistre sH, $s \in S$. Allora

$$\#G = \sum_{s \in S} \#(sH).$$

Per il Teorema 4.14 ogni classe laterale ha la stessa cardinalità di H. Concludiamo che

$$\#G = \#S \cdot \#H = \#H \cdot [G : H],$$

come richiesto. □

4.19 Corollario. Sia G un gruppo *finito*.

(*i*) Se H è un sottogruppo di G, allora $\#H$ divide $\#G$.

(*ii*) Se $x \in G$ allora l'ordine $\mathrm{ord}(x)$ di x divide $\#G$.

(*iii*) Sia G' un gruppo e sia $f : G \longrightarrow G'$ un'omomorfismo. Allora $\#\ker(f)$ divide $\#G$. Se il gruppo G' è finito, allora $\#f(G)$ divide $\#G'$.

Dimostrazione. Le affermazioni seguono direttamente dal teorema precedente. Per la parte *(iii)* osservare che il Teorema 3.11 implica che $\ker(f)$ è sottogruppo di G e che $f(G)$ è sottogruppo di G'. □

4.20 Corollario.

(*i*) (P. de Fermat) Sia p un numero primo e sia $x \in \mathbb{Z}$ tale che p non divide x. Allora

$$x^{p-1} \equiv 1 \bmod p.$$

(*ii*) (L. Eulero) Sia n un intero positivo e si $x \in \mathbb{Z}$ con $\mathrm{mcd}(x, n) = 1$ e sia φ la funzione di Eulero (Esempio 2.14). Allora

$$x^{\varphi(n)} \equiv 1 \bmod n.$$

Dimostrazione. *(i)* Sia G il gruppo moltiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$. Siccome p non divide x, la classe $\overline{x}$ è in $(\mathbb{Z}/p\mathbb{Z})^*$. Per il Corollario 4.19(*ii*) l'ordine di $\overline{x}$ divide la cardinalità di $(\mathbb{Z}/p\mathbb{Z})^*$ cioè $\mathrm{ord}(x)$ divide $p - 1$. Segue dalla Proposizione 4.6 che

$$\overline{x}^{p-1} = \overline{1}$$

come richiesto.
(ii) La cardinalità di $G = (\mathbb{Z}/n\mathbb{Z})^*$ è data da $\varphi(n)$. Dunque la dimostrazione è simile a quella della prima parte. □

4.21 Corollario. Sia p un primo e sia G un gruppo di ordine p. Allora

$$G \cong \mathbb{Z}/p\mathbb{Z}.$$

Dimostrazione. Sia $x \in G$ un elemento diverso dall'elemento neutro. L'ordine di x è dunque diverso da 1. Siccome $\mathrm{ord}(x)$ divide la cardinalità p di G, vediamo che l'ordine di x è p. Per il Teorema 4.7(*ii*), il gruppo $H \subset G$ generato da x è isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Concludiamo che $\mathbb{Z}/p\mathbb{Z} \cong H = G$ come richiesto. □

4.22 Il teorema di Lagrange e i suoi corollari impongono forti restrizioni sulla struttura di un gruppo. Come sua applicazione "classifichiamo i gruppi di ordine ≤ 5:

4.23 Teorema. Sia G un gruppo di ordine ≤ 5. Allora

$$G \cong \mathbb{Z}/n\mathbb{Z} \qquad \text{con } n \leq 5, \text{ oppure} \qquad G \cong V_4.$$

Dimostrazione. Se $n = 1$ il gruppo G è $\{e\}$. Per $n = 2, 3, 5$ il Cor.4.20 implica che G è ciclico e dunque isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Se $n = 4$ gli ordini possibili per un elemento $g \in G$ sono 1,2 oppure 4. Adesso ci sono due possibilità: si esiste $g \in G$ di ordine 4, allora $G =< g >\cong \mathbb{Z}/4\mathbb{Z}$. Se non esiste un tale elemento, allora $g^2 = e$ per ogni $g \in G$. Indicando gli elementi non banali di G con a, b, c possiamo scrivere parte della tavola di moltiplicazione di G:

	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	e	?
c	c	?	?	e

Siccome ogni riga ed ogni colonna della tavola contiene ogni elemento di G esattamente una volta (si veda l'Eserc.(2.C)), gli elementi nelle posizione con "? sono determinati e ritroviamo la tavola del gruppo V_4 di Klein. □

4.24 Lista. Diamo ora una tabella con il numero dei gruppi non isomorfi di ordine al più 32. Per questa tabella e per una panoramica generale dell'algebra e delle sue applicazioni si veda l'articolo divulgativo di I.R. Safarevich: Basic Notions of Algebra, in *Encyclopaedia of Mathematical Sciences* **11**, Algebra I, Springer-Verlag, Berlin 1990.

$\#G$	num	$\#G$	num	$\#G$	num	$\#G$	num
1	1	9	2	17	1	25	2
2	1	10	2	18	5	26	2
3	1	11	1	19	1	27	5
4	2	12	5	20	5	28	4
5	1	13	1	21	2	29	1
6	2	14	2	22	2	30	4
7	1	15	1	23	1	31	1
8	5	16	14	24	15	32	51

Esercizi.

(4.A) Dimostrare

(i) $Q =< i, j >$,

(ii) $(\mathbb{Z}/23\mathbb{Z})^* =< \overline{5} >$,

(4.B) Sia G un gruppo e sia S un suo sottoinsieme. Dimostrare che $< S >$ è uguale all'intersezione dei sottogruppi H di G che contengono S.

(4.C) Calcolare gli ordini degli elementi dei gruppi Q, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $\mathbb{Z}/8\mathbb{Z}$.

(4.D) Sia G un gruppo e siano $a, b \in G$. Far vedere:

(i) $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$.

(ii) $\mathrm{ord}(a) = \mathrm{ord}(bab^{-1})$.

(iii) $\mathrm{ord}(ab) = \mathrm{ord}(ba)$.

(4.E) (*la formula di Gauss*) Per la definizione della funzione ϕ si veda l'Esempio 2.14. Sia n un intero positivo.

(i) Dimostrare: $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ha ordine d se e soltanto se $\mathrm{mcd}(a, n) = n/d$.

(ii) Quanti sono i generatori di $\mathbb{Z}/n\mathbb{Z}$?

(iii) Mostrare che il numero delle classi $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ con $\mathrm{mcd}(a, n) = n/d$ è uguale a $\varphi(d)$ (Sugg. scrivere $a = b \cdot n/d$ dove $\mathrm{mcd}(b, d) = 1$ e definire una biiezione da $\{a \in \mathbb{Z}/n\mathbb{Z} : \mathrm{mcd}(a, n) = n/d\}$ a $(\mathbb{Z}/d\mathbb{Z})^*$.

(iv) Concludere che

$$\sum_{\substack{d|n \\ d>0}} \varphi(d) = n.$$

(4.F) Sia G un gruppo abeliano e siano $\alpha, \beta \in G$ di ordine finito a e b, rispettivamente. Mostrare che

(i) L'ordine di $\alpha\beta$ divide $\mathrm{mcm}(a, b)$.

(ii) Se $\mathrm{mcd}(a, b) = 1$ allora $\mathrm{ord}(\alpha\beta) = ab$.

(4.G) Sia G un gruppo *abeliano*. Dimostrare che

$$\{g \in G : \mathrm{ord}(g) \text{ è finito}\}$$

è un sottogruppo di G detto il *sottogruppo di torsione di* G.

(4.H) Siano G e G' due gruppi e siano $\alpha \in G$ e $\beta \in G'$ elementi di ordine finito a e b rispettivamente. Allora l'ordine di $(\alpha, \beta) \in G \times G'$ è uguale a $\mathrm{mcm}(a, b)$.

(4.I) Siano G e G' due gruppi e sia $f : G \longrightarrow G'$ un omomorfismo. Mostrare che

(i) Se $g \in G$ ha ordine finito, allora $\mathrm{ord}(f(g))$ divide $\mathrm{ord}(g)$.

(ii) Se f è un'isomorfismo allora $\mathrm{ord}(f(g)) = \mathrm{ord}(g)$ per ogni $g \in G$.

(4.J) (i) Sia p un primo e sia $a \in \mathbb{Z}$. Mostrare che

$$a^{k(p-1)+1} \equiv a \bmod p$$

per ogni intero $k \geq 0$.

(ii) Provare che $a^{13} - a$ è divisibile per 2730 per ogni $a \in \mathbb{Z}$.

(4.K) Sia H un sottogruppo di G e sia S un sistema di rappresentanti per le classi laterali sinistre. Dimostrare che $\{s^{-1} : s \in S\}$ è un sistema di rappresentanti per le classi laterali destre.

(4.L) Sia $B = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Definiamo una moltiplicazione su B:

$$(a, b) \cdot (a', b') = (a + (-1)^b a', b + b') \quad \text{per } (a, b), (a', b') \in B.$$

Dimostrare che B è un gruppo non abeliano con questa moltiplicazione.

(4.M) Sia G un gruppo e siano $a, b \in G$ di ordine 2.

(i) Provare: *abababa* ha ordine 2.

(ii) * Dimostrare che $[< a, b >:< ab >] = 2$.

5 Sottogruppi normali e gruppi quoziente

5.1 In questo paragrafo introduciamo il concetto di *sottogruppo normale N di un gruppo G*. Poi definiamo una struttura naturale di gruppo sull'insieme delle classe laterali G/N di N e otteniamo il *gruppo quoziente* G/N. La costruzione è una generalizzazione del gruppo $\mathbb{Z}/n\mathbb{Z}$ delle classi resto modulo n: se si prende $G = \mathbb{Z}$ e $N = n\mathbb{Z}$ si ritrova il gruppo $G/N = \mathbb{Z}/n\mathbb{Z}$ dell'Esempio 2.13.

5.2 Definizione. Sia G un gruppo. Un sottogruppo H di G si dice *normale in G* se

$$ghg^{-1} \in H \qquad \text{per ogni } h \in H \text{ e per ogni } g \in G.$$

5.3 Esempi.

(*i*) Ogni gruppo G possiede i sottogruppi normali *banali* $\{e\}$ e G.

(*ii*) Per un gruppo commutativo G *ogni* sottogruppo è automaticamente normale.

(*iii*) Il centro $Z(G)$ (si veda Esempio 3.5) è un sottogruppo normale: sia $h \in Z(G)$ e sia $g \in G$. Allora $ghg^{-1} = hgg^{-1} = h$ e quindi $ghg^{-1} \in Z(G)$.

5.4 Teorema. Sia G un gruppo e sia H un sottogruppo di G. Le seguenti affermazioni sono equivalenti:

(*i*) H è un sottogruppo normale di G.

(*ii*) $gH = Hg$ per ogni $g \in G$.

(*iii*) $gHg^{-1} = H$ per ogni $g \in G$.

Dimostrazione. *(i)* $\Rightarrow$ *(ii)* Sia $g \in G$ e sia $x \in gH$. Dunque $x = gh$ per un $h \in H$. Siccome H è un sottogruppo normale abbiamo $x = gh = (ghg^{-1})g \in Hg$. Dunque $gH \subset Hg$ e similmente $Hg \subset Hg$.
(ii) $\Leftrightarrow$ *(iii)* Sia $g \in G$. Dato che $gH = Hg$, cioè

$$\{gh : h \in H\} = \{hg : h \in H\}$$

è immediato che

$$\{ghg^{-1} : h \in H\} = \{h : h \in H\}$$

cioè $gHg^{-1} = H$: basta moltiplicare a sinistra con g^{-1}. Anche il viceversa è immediato.
(ii) $\Rightarrow$ *(i)* Sia $h \in H$ e $g \in G$. Abbiamo $gh \in gH = Hg$. Esiste dunque $h' \in H$ tale che $gh = h'g$ e vediamo che $ghg^{-1} = h' \in H$ come richiesto. $\square$

5.5 Esempio. Nell'Esempio 4.10(*iv*) abbiamo visto che il sottogruppo $H = \{(1), (2\,3)\}$ di S_3 ha la proprietà che le sue classi laterali sinistre sono diverse da quelle destre. Per il Teorema 5.4 concludiamo che H non è un sottogruppo normale di S_3.

5.6 Teorema. Sia G un gruppo e sia H un sottogruppo di G con indice $[G : H]$ uguale a 2. Allora H è un sottogruppo normale di G.

Dimostrazione. Il sottogruppo H ha soltanto due classi laterali sinistre. Una di queste è il gruppo H stesso. Siccome le classi laterali sono disgiunte e la riunione di tutte le classi sinistre è G, l'unica altra classe deve essere il complemento $G - H$ di H in G. Questo vale anche per le classi destre di H. Dunque:

$$\begin{array}{lll} gH = Hg = & H & \text{se } g \in H, \\ gH = Hg = & G - H & \text{se } g \notin H. \end{array}$$

Quindi la conclusione segue dal Teorema 5.4. □

5.7 Teorema. Siano G, G' gruppi e sia f un omomorfismo da G a G'. Allora $\ker(f)$ è un sottogruppo normale di G.

Dimostrazione. Per il Teorema 3.11, il nucleo $\ker(f)$ è un sottogruppo di G. Sia $h \in \ker(f)$ e sia $g \in G$. Scriviamo e' per l'elemento neutro di G'. Allora

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e'$$

e quindi $ghg^{-1} \in \ker(f)$. Questo implica che $\ker(f)$ è un sottogruppo normale come richiesto. □

5.8 Costruzione del gruppo quoziente. Sia G un gruppo e sia N un sottogruppo normale. Siccome N è normale, non c'è differenza fra le classi laterali sinistre e destre. Come nel paragrafo 4, indichiamo con $G/N = \{gN : g \in G\}$ l'insieme delle classi laterali di N. Scriviamo $\overline{g}$ per gN. Si ha $\overline{a} = \overline{b}$ se e soltanto se $a^{-1}b \in N$ (vedi 4.11).

Definiamo la composizione sull'insieme G/N in modo seguente:

$$\overline{a} \cdot \overline{b} = \overline{ab} \qquad \text{per } a, b \in G.$$

Questa definizione dipende, a priori, dalla scelta dei rappresentanti a e b delle classi $\overline{a}$ e $\overline{b}$. Verifichiamo che in realtà non c'è dipendenza da queste scelte: supponiamo che $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Per il Teorema 4.11 abbiamo $a' = an_1$ e $b' = bn_2$ per certi $n_1, n_2 \in N$. Troviamo

$$a'b' = an_1bn_2 = ab(b^{-1}n_1b)n_2.$$

Siccome n_2 e $b^{-1}n_1b$, e dunque il loro prodotto, sono in N concludiamo che

$$\overline{a'b'} = \overline{ab},$$

come richiesto.

È molto facile verificare che con questa moltiplicazione G/N diventa un gruppo:

l'associatività segue da quella di G:

$$(\overline{a} \cdot \overline{b})\overline{c} = \overline{ab}\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\overline{bc} = \overline{a}(\overline{b} \cdot \overline{c});$$

l'elemento neutro è $\overline{e} = N$. L'inverso di $\overline{a}$ è la classe $\overline{a^{-1}}$.

Il gruppo G/N si dice il gruppo G "modulo N. La cardinalità di G/N è il numero delle classi laterali sinistre, cioè l'indice $[G : N]$.

5.9 Teorema. L'applicazione

$$\pi : G \longrightarrow G/N, \qquad \pi(g) = \overline{g}$$

è un omomorfismo suriettivo con nucleo N ed è detta applicazione *canonica*.

Dimostrazione. Un elemento $x \in G/N$ è una classe laterale, cioè $x = gN$ per un certo $g \in G$. Allora $x = \pi(g)$ e perciò π è suriettiva. Abbiamo $g \in \ker(\pi)$ se e soltanto se $\overline{g} = N$, cioè $gN = N$ e questo vale se e soltanto se $g \in N$. □

5.10 Esempi.

(*i*) Sia $G = \mathbb{R}^*$ il gruppo moltiplicativo dei numeri reali non nulli. Si tratta di un gruppo commutativo e il sottogruppo $N = \mathbb{R}^*_{>0}$ dei numeri positivi è un sottogruppo normale di indice 2. Il gruppo quoziente ha due elementi: $\mathbb{R}^*_{>0}$ e $\mathbb{R}^*_{<0}$. Per calcolare i prodotti nel gruppo quoziente basta seguire la definizione: prendere rappresentanti, calcolare il prodotto in $G = \mathbb{R}^*$ e poi prendere la classe modulo N. Per esempio

$$(\mathbb{R}^*_{<0}) \cdot (\mathbb{R}^*_{<0}) = \mathbb{R}^*_{>0}$$

perché il prodotto di due numeri negativi è un numero positivo.

(*ii*) Sia $G = Q$ il gruppo dei quaternioni di ordine 8. Il centro di Q è $N = \{1, -1\}$ (Si veda l'Eserc. (3.G)). Il sottogruppo N è dunque un sottogruppo normale di Q. Le classi laterali di N sono

$$\{\pm 1\}, \quad \{\pm i\}, \quad \{\pm j\} \quad \text{e} \quad \{\pm k\}.$$

Come esempio moltiplichiamo $\{\pm i\}$ e $\{\pm j\}$: prendere rappresentanti, diciamo i e j; calcolare il prodotto nel gruppo dei quaternioni: $i \cdot j = k$; prendere la classe modulo N: la risposta è $\{\pm k\}$. Ecco la tavola di composizione di G/N:

	$\{\pm 1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
$\{\pm 1\}$	$\{\pm 1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
$\{\pm i\}$	$\{\pm i\}$	$\{\pm 1\}$	$\{\pm k\}$	$\{\pm j\}$
$\{\pm j\}$	$\{\pm j\}$	$\{\pm k\}$	$\{\pm 1\}$	$\{\pm i\}$
$\{\pm k\}$	$\{\pm k\}$	$\{\pm j\}$	$\{\pm i\}$	$\{\pm 1\}$

(*iii*) Adesso consideriamo un esempio *additivo*. Sia $G = \mathbb{Z}$, sia $n \in \mathbb{Z}$ e sia $N = n\mathbb{Z}$. Siccome $\mathbb{Z}$ è un gruppo commutativo, N è un sottogruppo normale. Le classi laterali di $N = n\mathbb{Z}$ sono

$$a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\}.$$

Si verifica che il gruppo quoziente $G/N = \mathbb{Z}/n\mathbb{Z}$ coincide con il gruppo delle classi resto modulo n dell'Esempio 2.13.

(*iv*) Sia $G = \mathbb{R}$ il gruppo additivo dei numeri reali e sia $N = \mathbb{Z}$. Siccome $\mathbb{R}$ è commutativo, N è un sottogruppo normale. Il gruppo quoziente $\mathbb{R}/\mathbb{Z}$ è il gruppo dei "numeri reali modulo 1. Vedremo nell'Esempio 6.5 che $\mathbb{R}/\mathbb{Z}$ è, in un certo senso, una circonferenza.

5.11 Definizione. Sia G un gruppo e sia $[G, G]$ il sottogruppo di G generato dai *commutatori* $[g, h] = ghg^{-1}h^{-1}$ dove $g, h \in G$.

Il sottogruppo $[G, G]$ è un sottogruppo normale: sia $h \in [G, G]$ e $g \in G$. Abbiamo

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in [G, G].$$

In generale, non è vero che ogni elemento di $[G, G]$ è un commutatore. Si veda l'Eserc.(5.M) per un esempio.

5.12 Teorema. Sia N un sottogruppo normale di un gruppo G. Allora G/N è commutativo se e soltanto se $[G, G] \subset N$.

Dimostrazione. Scriviamo $\overline{g}$ per la classe gN. Il gruppo quoziente G/N è commutativo se e soltanto se $\overline{g} \cdot \overline{h} = \overline{h} \cdot \overline{g}$ per ogni $g, h \in G$. Quindi, se e soltanto se $\overline{ghg^{-1}h^{-1}} = \overline{e}$. Dunque, G/N è commutativo se e soltanto se $ghg^{-1}h^{-1} \in N$ per ogni $g, h \in G$. Siccome i commutatori $ghg^{-1}h^{-1}$ generano $[G, G]$, questo è equivalente a $[G, G] \subset N$, come richiesto. □

Esercizi.

(5.A) Sia G un gruppo e sia $\{N_\alpha : \alpha \in A\}$ una famiglia di sottogruppi normali di G. Dimostrare che $\cap_{\alpha \in A} N_\alpha$ è un sottogruppo normale di G.

(5.B) Sia G un gruppo. Dimostrare che le seguenti affermazioni sono equivalenti:

(i) G è abeliano.,

(ii) $Z(G) = G$,

(iii) $[G, G] = \{e\}$.

(5.C) Sia G un gruppo, $N \subset G$ un sottogruppo normale e $H \subset G$ un sottogruppo. Sia

$$NH = \{nh : n \in N,\ h \in H\}.$$

Dimostrare che NH è un sottogruppo di G. Dimostrare: se H è un sottogruppo normale di G anche NH lo è.

(5.D) Sia G un gruppo e siano N, M due sottogruppi normali di G che soddisfano $N \cap M = \{e\}$. Mostrare che:

(i) per ogni $n \in N$ ed ogni $m \in M$ abbiamo $nm = mn$.

(ii) se G è generato da $N \cup M$, allora

$$G \cong N \times M.$$

(5.E) Sia G un gruppo e sia $N \subset G$ un sottogruppo normale di ordine 2. Mostrare che $N \subset Z(G)$.

(5.F) Dimostrare che ogni sottogruppo del gruppo Q dei quaternioni è normale in Q.

(5.G) Sia G un gruppo e sia $H \subset G$ un sottogruppo. Dimostrare che

$$N = \cap_{g \in G} gHg^{-1}$$

è un sottogruppo normale di G, contenuto in H. Mostrare che N è "massimale, cioè, se $M \subset H$ è un sottogruppo normale di G, allora $M \subset N$.

(5.H) Sia G un gruppo. Provare che se $G/Z(G)$ è ciclico, allora G è abeliano.

(5.I) Sia G un gruppo *commutativo.* Sia

$$T(G) = \{g \in G : \text{ l'ordine di } g \text{ è finito}\}.$$

Dimostrare che $T(G)$ è un sottogruppo di G. (Detto il sottogruppo di *torsione.*) Dimostrare che l'unico elemento in $G/T(G)$ di ordine finito è l'elemento neutro.

(5.J) Sia G un gruppo e sia N il sottogruppo di G generato da $\{g^2 : g \in G\}$. Mostrare che N è un sottogruppo normale e che $[G, G] \subset N$.

(5.K) Sia $\mathrm{N} : \mathbb{H}^* \longrightarrow \mathbb{R}^*$ l'applicazione "norma dell'Eserc.(2.F). Dimostrare

(i) $[\mathbb{H}^*, \mathbb{H}^*] \subset \ker(N)$,

(ii) per ogni $x \in \mathbb{H}$ esiste $y \in \mathbb{H}^*$ tale che $yx = \overline{x}y$.

(iii) per $x \in \ker(N)$, $x \neq -1$ esiste $y \in \mathbb{H}^*$ tale che $x = [1 + \overline{x}, y]$,

(iv) $[\mathbb{H}^*, \mathbb{H}^*] = \ker(N) = \{x \in \mathbb{H}^* : x\overline{x} = 1\}$.

(5.L) Mostrare che i sottogruppi di G/N sono esattamente i gruppi H/N, cioè $\{hN : h \in H\}$, dove H è un sottogruppo di G tale che $N \subseteq H$.

(5.M) In questo esercizio costruiamo un gruppo G_1 tale che non ogni elemento in $[G_1, G_1]$ è un commutatore. Sia $N \subset \mathbb{H}$ il sottogruppo dei quaternioni immaginari puri:

$$N = \{bi + cj + dk : b, c, d \in \mathbb{R}\}$$

e sia $Q \subset \mathbb{H}^*$ il gruppo dei quaternioni di ordine 8. Sia $G = N \times Q$. Definiamo un prodotto $*$ su G in questo modo

$$(x, \alpha) * (y, \beta) = (x + \alpha y \alpha^{-1}, \alpha\beta) \qquad \text{per } (x, \alpha), (y, \beta) \in G.$$

Mostrare che:

(i) con la composizione $*$, l'insieme G è un gruppo,

(ii) $Z(G) = \{(0, 1), (0, -1)\}$,

(iii) $[G, G] = \{(x, \alpha) : x \in N, \alpha \in \{\pm 1\}\}$,

(iv) l'elemento $(i + j + k, 1) \in [G, G]$ non è un commutatore. (Sugg. Se $[(x, \alpha), (y, \beta)] = (z, 1)$, per certi α, β, allora l'uguaglianza vale anche con $\alpha = 1$ o con $\beta = 1$ o con $\alpha = \beta$.

(v) Costruire un gruppo G_1 di ordine 216 tale che

$$[G_1, G_1] \neq \{[g, h] : g, h \in G_1\}.$$

(Sugg. sostituire $\mathbb{R}$ con $\mathbb{Z}/3\mathbb{Z}$.)

(5.N) Esiste un sottogruppo H di $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ tale che

$$H \cong G/H \cong \mathbb{Z}/4\mathbb{Z}\,?$$

6 Teoremi di isomorfismo

In questo paragrafo dimostriamo i cosiddetti *teoremi di isomorfismo*. Questi teoremi sono utili per calcolare la struttura di gruppi quoziente.

6.1 Teorema. (Teorema di omomorfismo.) Sia f un omomorfismo del gruppo G nel gruppo G'. Sia N un sottogruppo normale di G con $N \subset \ker(f)$. Allora, esiste unico un omomorfismo $h : G/N \longrightarrow G'$ tale che $h(xN) = f(x)$. Si dice anche che il diagramma

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow \pi & \nearrow & h \\ G/N & & \end{array}$$

è commutativo. Con $\pi : G \longrightarrow G/N$ si indica l'applicazione canonica: $\pi(x) = xN$.

Dimostrazione. Scriviamo $\overline{x}$ per la classe laterale xN e e' per l'elemento neutro di G'. Definiamo

$$h : G/N \longrightarrow G'$$

ponendo $h(\overline{x}) = f(x)$.

Vediamo che h è ben definita: se $\overline{x} = \overline{y} \in G/N$, allora $x^{-1}y \in N$. Siccome $N \subset \ker(f)$, abbiamo $f(x^{-1}y) = e'$ e quindi $f(x)^{-1}f(y) = e'$. Perciò $h(\overline{x}) = f(x) = f(y) = h(\overline{y})$, come richiesto.

Siccome

$$h(\overline{xy}) = h(\overline{x}\overline{y}) = f(xy) = f(x)f(y) = h(\overline{x})h(\overline{y}),$$

l'applicazione h è un omomorfismo. Per definizione h soddisfa $h(\overline{x}) = f(x)$. Un omomorfismo $h' : G/N \longrightarrow G'$ con le stesse proprietà è evidentemente uguale ad h. □

6.2 Esempio. Siano n, $d \in \mathbb{Z}_{>0}$ tali che d divide n e sia $f : \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ la mappa canonica $f(a) = a \bmod d$. Dato che d divide n, si ha che $f(nk) = \overline{0}$ per ogni $k \in \mathbb{Z}$, cioè il sottogruppo $N = n\mathbb{Z}$ di $\mathbb{Z}$ è contenuto in $\ker(f)$. Dal Teorema 6.1 segue che esiste un omomorfismo

$$h : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}, \qquad h(a \bmod n) = a \bmod d$$

(vedi anche 3.15).

6.3 Teorema. (Primo teorema di isomorfismo).
Sia $f : G \longrightarrow G'$ un omomorfismo del gruppo G nel gruppo G'. Allora

$$G/\ker(f) \cong \mathrm{im}(f).$$

Dimostrazione. Applichiamo il Teorema 6.1 con $N = \ker(f)$. Otteniamo un omomorfismo

$$h : G/\ker(f) \longrightarrow G'$$

con $h(x\ker(f)) = f(x)$. Dunque, l'immagine di h è uguale all'immagine di f.

Sia $x\ker(f) \in \ker(h)$. Si ha dunque $h(x\ker(f)) = f(x) = e'$ e quindi $x \in \ker(f)$, cioè $x\ker(f)$ è uguale all'elemento neutro $\ker(f)$ del gruppo $G/\ker(f)$. Concludiamo che h è iniettiva.

Dunque, l'applicazione

$$h : G/\ker(f) \longrightarrow \mathrm{im}(f)$$

è una biiezione, come richiesto.

6.4 Corollario. Sia $f : G \longrightarrow G'$ un omorfismo suriettivo di gruppi. Allora

$$G/\ker(f) \cong G'.$$

Dimostrazione. Immediata dal Teorema 6.3. □

6.5 Esempio. Come esempio studiamo il sottogruppo $S = \{z \in \mathbb{C}^* : z\overline{z} = 1\}$ di $\mathbb{C}^*$ (Si veda l'Eserc.(2.D) per la defizione di $\overline{z}$). Scrivendo $z = a + bi$ con $a, b \in \mathbb{R}$, abbiamo che

$$S = \{a + bi : \quad a, b \in \mathbb{R} \text{ e } a^2 + b^2 = 1\};$$

gli elementi di S stanno sulla circonferenza unitaria in $\mathbb{C}$. L'applicazione $F : \mathbb{R} \longrightarrow S$ data da

$$F(\phi) = \cos(2\pi\phi) + i\mathrm{sen}(2\pi\phi)$$

è un omomorfismo (Si veda l'Eserc.(3.H).(vii)). È ben noto che per ogni $a, b \in \mathbb{R}$ con $a^2+b^2 = 1$ esiste $\phi \in \mathbb{R}$ tale che $a = \cos(2\pi\phi)$ e $b = \mathrm{sen}(2\pi\phi)$. L'applicazione F è dunque suriettiva. Il nucleo di F è dato da $\ker(F) = \{\phi \in \mathbb{R} : \cos(2\pi\phi) = 1 \text{ e } \mathrm{sen}(2\pi\phi) = 0\}$. Si vede dunque facilmente che $\ker(F) = \mathbb{Z}$. Adesso applichiamo il Corollario 6.4:

$$\mathbb{R}/\mathbb{Z} \cong S,$$

cioè, il gruppo quoziente $\mathbb{R}/\mathbb{Z}$ "è una circonferenza.

6.6 Sia $f : G \longrightarrow G'$ un omomorfismo dal gruppo G al gruppo G'. Per G' è abeliano si ha il seguente teorema, caso speciale del Teorema 6.1.

6.7 Teorema. . Sia $f : G \longrightarrow A$ un omomorfismo da un gruppo G a un gruppo commutativo A. Allora esiste un unico omomorfismo $h : G/[G, G] \longrightarrow A$ tale che $h(g[G, G]) = f(g)$. Cioè, il diagramma

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ \downarrow & \nearrow & h \\ G/[G,G] & & \end{array}$$

è commutativo.

Dimostrazione. Il nucleo $\ker(f)$ è un sottogruppo normale di G. Siccome $G/\ker(f) \cong f(G)$ è un sottogruppo di A, vediamo che $G/\ker(f)$ è un gruppo abeliano. Per il Teorema 5.12, abbiamo $[G, G] \subset \ker(f)$. Adesso il Teorema 6.1 con $N = [G, G]$ ha come consequenza il risultato. □

6.8 Teorema. (*Secondo teorema di isomorfismo.*)
Sia G un gruppo, sia $H \subset G$ un sottogruppo e sia $N \subset G$ un sottogruppo *normale* di G. Allora

(*i*) $H \cap N$ è un sottogruppo normale di H.

(*ii*) L'insieme $HN = \{hn : h \in H, n \in N\}$ è un sottogruppo di G. Il gruppo N è un sottogruppo normale di HN.

(*iii*) Abbiamo
$$H/(H \cap N) \cong HN/N.$$

Dimostrazione. *(i)* Sia $n \in H \cap N$ e sia $g \in H$. Ovviamente $gng^{-1} \in H$. Siccome N è un sottogruppo normale di G abbiamo anche $gng^{-1} \in N$. Quindi $gng^{-1} \in H \cap N$ e concludiamo che $H \cap N$ è un sottogruppo normale di H.
(ii) Siccome $e \in H, N$ abbiamo che $e = e \cdot e \in HN$ e dunque $HN \neq \emptyset$. Sia $a = h_1 n_1 \in HN$ e $b = h_2 n_2 \in HN$. Siccome N è un sottogruppo normale abbiamo
$$h_2(n_1 n_2^{-1})h_2^{-1} = n_3 \in N.$$
Dunque, $ab^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 h_2^{-1} n_3 \in HN$. Per il Teorema 3.3, l'insieme HN è un sottogruppo di G. Siccome N è un sottogruppo normale di G, esso è anche un sottogruppo normale del sottogruppo HN.
(iii) Sia
$$f : H \longrightarrow HN/N$$
l'applicazione data da $f(h) = hN$. È facile verificare che f è un omomorfismo suriettivo. Il nucleo di f è l'insieme $\{h \in H : hN = N\}$, cioè $\ker(f) = H \cap N$. Adesso la parte *(iii)* segue dal Corollario 6.4. □

6.9 Corollario.
Sia G un gruppo, sia $H \subset G$ un sottogruppo e sia $N \subset G$ un sottogruppo *normale* di G. Allora:
$$\#(HN) = \frac{\#H \times \#N}{\#(H \cap N)}$$

Dimostrazione. Immediata dal Teorema 6.8. □

Si osservi che la stessa formula vale anche nel caso in cui N non è normale (H e N sono semplicemente due *sottogruppi* di G); in questo caso HN non è necessariamente un sottogruppo di G ma solo un *sottoinsieme*.

Esercizi.

(6.A) Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi. Supponiamo che G sia finito. Dimostrare che $\#f(G)$ divide $\#G$.

(6.B) Sia G un gruppo e sia $g \in G$. Dimostrare che l'applicazione $F : \mathbb{Z} \longrightarrow G$ data da $n \mapsto g^n$ è un omomorfismo suriettivo da $\mathbb{Z}$ a $< g >$. Mostrare che F è iniettiva se e soltanto se g ha ordine infinito. Se F non è iniettiva, utilizzare il Teorema 6.3 per dimostrare che $\mathbb{Z}/n\mathbb{Z} \cong < g >$ dove n è l'ordine di g.

(6.C) Sia G un gruppo e siano N_1, N_2 due sottogruppi normali di G. Definiamo

$$F : G \longrightarrow (G/N_1) \times (G/N_2)$$

ponendo $F(g) = (gN_1, gN_2)$.

(i) Dimostrare che F è un omomorfismo con nucleo $N_1 \cap N_2$.

(ii) Dimostrare che $G/(N_1 \cap N_2)$ è isomorfo a un sottogruppo di $(G/N_1) \times (G/N_2)$.

(6.D) Dimostrare che l'insieme $H = \{\overline{1}, \overline{11}\}$ è un sottogruppo di $(\mathbb{Z}/15\mathbb{Z})^*$. Mostrare che $H = \ker(f)$ dove f è l'applicazione $(\mathbb{Z}/15\mathbb{Z})^* \longrightarrow (\mathbb{Z}/5\mathbb{Z})^*$ data da $(x \bmod 15) \mapsto (x \bmod 5)$. Dimostrare che $(\mathbb{Z}/15\mathbb{Z})^*/H$ è un gruppo ciclico di ordine 4.

(6.E) Sia G un gruppo e siano N_1, N_2 due sottogruppi normali di G con $N_1 \cap N_2 = \{e\}$ e $N_1N_2 = G$. Mostrare che

$$G \cong G/N_1 \times G/N_2.$$

(Sugg. considerare l'applicazione $G \longrightarrow G/N_1 \times G/N_2$ data da $g \mapsto (gN_1, gN_2)$).

(6.F) Dimostrare:

(i) $\mathbb{R}^* \cong \{\pm 1\} \times \mathbb{R}$,

(ii) $\mathbb{C}^* \cong \mathbb{R} \times S$.

(6.G) (i) Mostrare che esiste un omomorfismo suriettivo

$$h : (\mathbb{Z}/4\mathbb{Z})^2 \to (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), \qquad (a \bmod 4, b \bmod 4) \longmapsto (a + b \bmod 4, b \bmod 2).$$

(ii) Mostrare che $(\mathbb{Z}/4\mathbb{Z})^2/N \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ dove $N = \{(\overline{0}, \overline{0}),\ (\overline{2}, \overline{2})\}$.