Indice

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 $0 \leq r_3 < r_2$ ... 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 $b = 1991$:

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

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 $0 \le a_i < b$ per ogni $i \ge 0$. 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) Sia n un intero positivo e sia p un primo. Determinare $\mathrm{ord}_p(n!)$. Con quanti zeri finisce 1000! ?

(1.N) Sia n un intero positivo e sia $\binom{2n}{n}$ il coefficiente binomiale. Dimostrare che $\mathrm{ord}_p(\binom{2n}{n}) = 1$ per ogni primo p per il quale $n < p < 2n$.

(1.O) Siano $a, b \in \mathbb{Z}$.

(i) Siano $r, s \in \mathbb{Z}$ con $\mathrm{mcd}(r,s) = 1$. Provare: se $x = r/s$ è una soluzione razionale dell'equazione $aX^2 + bX + c = 0$ allora r divide c e s divide a.

(ii) Dimostrare: se l'equazione $X^2 + bX + c = 0$ ha una soluzione $x \in \mathbb{Q}$, allora $x \in \mathbb{Z}$.

(1.P) 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.Q) 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.R) Un intero postivo a si chiama *perfetto* se la somma dei divisori positivi di a tranne a stesso è uguale ad a. Per esempio $6 = 1 + 2 + 3$ e $28 = 1 + 2 + 4 + 7 + 14$ sono numeri perfetti. Dimostrare che $2^{n-1}(2^n - 1)$ è perfetto quando $2^n - 1$ è un primo. Trovare altri numeri perfetti.

(1.S) 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*.

(1.T) Sia p un primo e sia p' il più piccolo primo $> p$. Dimostrare che $p + p'$ non è un prodotto di due primi.

(1.U) Sia p un primo tale che $p^2 - 1$ è il prodotto di 5 numeri primi. Far vedere che $p = 7$, 11 oppure 13.

(1.V) Sia p un primo tale che $p^2 + 8$ è primo; dimostrare che $p^3 + 4$ è primo.

(1.W) * Sia n un intero positivo. Provare che $n^4 + 4^n$ è primo se e soltanto se $n = 1$. (Sugg.: per n dispari addizionare e sottrarre il *quadrato* $n^2 2^{n+1}$.)

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

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

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

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

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.H). 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.L)). 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*, vedi 9.22. 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 $S(X)$. Si veda il paragrafo 4 per i gruppi S_n.

2.17 Esempio. *Il gruppo ortogonale $O_2(\mathbb{R})$.*
Una *isometria* A del piano $\mathbb{R}^2$ è una mappa $A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ che rispetta l'usuale distanza $d(P, Q)$ fra punti $P, Q \in \mathbb{R}^2$, cioè $d(A(P), A(Q)) = d(P, Q)$ per ogni $P, Q \in \mathbb{R}^2$. Definiamo

$$O_2(\mathbb{R}) = \{A : \ A \text{ è una isometria che fissa l'origine } \mathbf{0}\}.$$

L'applicazione identica I è in $O_2(\mathbb{R})$. La composizione di due elementi di $O_2(\mathbb{R})$ è in $O_2(\mathbb{R})$. Esempi di elementi di $O_2(\mathbb{R})$ sono *rotazioni* R_α con centro $\mathbf{0}$ e angolo α. Altri esempi sono le *riflessioni* S_ℓ lungo una retta ℓ passante per $\mathbf{0}$. Si può mostrare che $O_2(\mathbb{R})$ è un gruppo.

2.18 Esempio. *Il gruppo diedrale D_n.*

Sia n un intero positivo. Sia Δ_n l'n-gono regolare in $\mathbb{R}^2$ con centro $\mathbf{0} = (0,0)$ e un vertice P_0 in $\mathbf{e}_1 = (1,0)$. Gli altri vertici di Δ_n sono $P_1, \ldots, P_{n-1}$ dove P_i è sulla circonferenza di raggio 1 e l'angolo formato da $\overline{\mathbf{0}P_0}$ e $\overline{\mathbf{0}P_i}$ è $2\pi i/n$.

Definiamo il gruppo *diedrale*

$$D_n = \{A \in O_2(\mathbb{R}) : \ A \text{ trasforma l'}n\text{-gono } \Delta_n \text{ in se stesso}\}.$$

La verifica che D_n è un gruppo rispetto alla composizione è facile ed è lasciata al lettore. Si vede che D_n contiene le rotazioni $I = R^0$ (l'identità), R, $R^2 = R \circ R$, ..., R^{n-1} con angolo $\alpha = 0$, $2\pi/n$, $4\pi/n, \ldots$, $2(n-1)\pi/n$ e centro $\mathbf{0}$. Inoltre, D_n contiene certe riflessioni rispetto a rette passanti per $\mathbf{0}$. Ci sono le riflessioni rispetto alle rette passanti per $\mathbf{0}$ e per un vertice: ce ne sono n diverse quando n è dispari e $n/2$ quando n è pari. Inoltre, per n pari, ci sono anche le $n/2$ riflessioni rispetto alle rette passanti per $\mathbf{0}$ e per il punto medio di un lato. In questo modo si ottengono $2n$ elementi in D_n.

2.19 Lemma. Sia R la rotazione di centro $\mathbf{0}$ e angolo $\alpha = 2\pi/n$ e sia S la riflessione rispetto alla retta $y = 0$. Allora

(*i*) Il gruppo D_n ha $2n$ elementi.

(*ii*) Sia $A \in D_n$. Allora $A = R^i$ oppure $A = R^i S$ per un unico $i \in \mathbb{Z}$ con $0 \leq i \leq n-1$.

(*iii*) Si ha $SR = R^{-1}S$ e quindi

$$(R^i S)R^j = R^{i-j}S, \qquad (R^i S)(R^j S) = R^{i-j}.$$

(*iv*) L'isometria $R^i S$ è la riflessione S_i rispetto alla retta l_i passante per $\mathbf{0}$ e con angolo $\pi i/n$ con l'asse x positivo.

Dimostrazione. *(i), (ii)* Sia $A \in D_n$, allora $A(P_0)$ è un vertice di Δ_n e quindi $A(P_0) = P_i$ per un certo i. Consideriamo $B = R^{-i}A$, allora $B \in D_n$ e $B(P_0) = P_0$. Ci sono allora solo due possibilità per $B(P_1)$: $B(P_1) = P_1$ oppure $B(P_1) = P_{n-1}$. Nel primo caso $B = I$ e nel secondo caso si ha $B = S$ e quindi $A = R^i$ oppure $A = R^i S$.
(iii) Sia $A = SR$, allora $A(P_0) = S(R(P_0)) = S(P_1) = P_{n-1}$. Definiamo come sopra $B = RA$. Allora $B(P_1) = R(S(R(P_1))) = RS(P_2) = R(P_{n-2}) = P_{n-1}$ quindi $B = S$ e $A = R^{-1}S$. Dato che $SR = R^{-1}S$ si ha $SR^2 = SRR = R^{-1}SR = R^{-1}R^{-1}S = R^{-2}S$ ecc.
(iv) Non è difficile verificare che $R^i S$ e S_i mandano entrambi P_0 in P_i e P_1 in P_{i-1}, quindi sono uguali. □

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) Far vedere che l'equazione

$$ax = b$$

ha una unica soluzione $x \in G$. Questa soluzione è $x = a^{-1}b$. Similmente, far vedere 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) (*Assiomi sinistri\destri.*) Sia G un insieme con una composizione associativa $\circ : G \times G \longrightarrow G$.

(i) Supponiamo che esista $e \in G$ tale che

(G_2') $$e \circ a = a \qquad \text{per ogni } a \in G$$

e tale che per ogni $a \in G$ esiste $a^* \in G$ con

(G_3') $$a^* \circ a = e.$$

Dimostrare che G è un gruppo con elemento neutro e.

(ii) Stessa richiesta del punto (i), ma adesso sapendo che

(G_2'') $$a \circ e = a \qquad \text{per ogni } a \in G$$

e per ogni $a \in G$ esiste a^* con

(G_3'') $$a \circ a^* = e.$$

(2.E) (*Assiomi "misti."*) Sia G un insieme con almeno due elementi. Definiamo una composizione $\circ$:

$$a \circ b = b.$$

Dimostrare che con questa composizione e con elemento neutro $e \in G$ un elemento qualsiasi, G soddisfa gli assiomi (G_0), (G_1), (G_2') e (G_3''). Provare che G non è un gruppo.

(2.F) 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) Far vedere 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.G) (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) Far vedere 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.H) 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.I) (*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.F)). Far vedere

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

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

(2.K) Sia X un insieme e sia $P(X)$ l'insieme dei sottoinsiemi di X. Definiamo *la differenza simmetrica* $A \triangle B$ di due sottoinsiemi A e B di X:

$$A \triangle B = (A \cup B) - (A \cap B).$$

Verificare che $A \triangle B = (A - B) \cup (B - A)$. Dimostrare che $P(X)$ con la composizione $\triangle$ è un gruppo abeliano. Scrivere la tabella di composizione per un insieme X di due elementi. Confrontare con il gruppo di Klein V_4.

(2.L) Sia n un intero positivo e siano $a, b \in \mathbb{Z}$. Far vedere 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.M) Sia G un gruppo. Provare: se $x^2 = 1$ per ogni $x \in G$, allora G è abeliano.

(2.N) * Sia G l'insieme $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Definiamo una moltiplicazione su G mettendo

$$(i, j, k) \cdot (l, m, n) = (i + l + km, j + m, k + n).$$

(i) Far vedere che l'elemento $e = (0, 0, 0) \in G$ soddisfa $e \cdot (i, j, k) = (i, j, k) \cdot e = (i, j, k)$ per ogni $(i, j, k) \in G$.

(ii) Dimostrare che con questa moltiplicazione G è un gruppo non abeliano.

(iii) Dimostrare che $x^3 = e$ per ogni $x \in G$.

(2.O) 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 $n \in \mathbb{Z}$. Far vedere 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.P) 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.Q) *Il gruppo* $O_2(\mathbb{R})$.

(i) Siano ℓ e ℓ' due rette passanti per $\mathbf{0}$. Sia S_ℓ la riflessione lungo la retta ℓ e $S_{\ell'}$ la riflessione lungo la retta ℓ'. Sia R_ε la rotazione con centro $\mathbf{0}$ di angolo ε. Dimostrare che

$$S_{\ell'} \cdot S_\ell = R_{2(\alpha-\beta)},$$

dove α è l'angolo tra ℓ ed il semiasse positivo delle x e β quello tra ℓ' ed il semiasse positivo delle x.

(ii) Sia S_ℓ la riflessione lungo la retta ℓ e sia α l'angolo tra ℓ ed il semiasse positivo delle x. Dimostrare che

$$S_\ell = R_{2\alpha} \cdot S_{\text{ascisse}}.$$

(2.R) Sia n un intero positivo, sia R la rotazione con centro $\mathbf{0}$ ed angolo $2\pi/n$ e sia S la riflessione lungo l'asse delle ascisse. Dimostrare che

$$D_n = \{R^i S^j : 0 \le i \le n-1 \text{ e } 0 \le j \le 1\}$$

e

$$(R^i S^j)(R^{i'} S^{j'}) = \begin{cases} R^{i+i'} S^{j'}, & \text{se } j = 0, \\ R^{i-i'} S^{j'+1} & \text{se } j = 1. \end{cases}$$

Questo modo di scrivere gli elementi di D_n è molto conveniente per fare calcoli.

(2.S) Una trasformazione *affine* di $\mathbb{R}$ è una applicazione $A : \mathbb{R} \longrightarrow \mathbb{R}$ data da

$$x \mapsto ax + b$$

con $a \in \mathbb{R}^*$ e $b \in \mathbb{R}$.

(i) Dimostrare che le trasformazioni affini di $\mathbb{R}$ formano un gruppo con la composizione.

(ii) È un gruppo commutativo?

(2.T) Dimostrare che ci sono 48 trasformazioni isometriche dello spazio $\mathbb{R}^3$ che trasformano un dato cubo in se stesso.

(i) Dimostrare che queste trasformazioni formano un gruppo.

(ii) Quante trasformazioni isometriche di $\mathbb{R}^3$ trasformano un icosaedro in se stesso?

(2.U) 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.

(2.V) * Gli *Ottetti di Cayley* $\mathbb{O}$ sono espressioni della forma

$$\alpha + \beta\ell$$

dove $\alpha, \beta \in \mathbb{H}$ ed ℓ è un "simbolo. Definiamo una *addizione* ed una *moltiplicazione* per gli ottetti come segue:

$$\begin{aligned} (\alpha + \beta\ell) + (\gamma + \delta\ell) &= (\alpha + \gamma) + (\beta + \delta)\ell, \\ (\alpha + \beta\ell) \cdot (\gamma + \delta\ell) &= (\alpha\gamma - \overline{\delta}\beta) + (\delta\alpha + \beta\overline{\gamma})\ell. \end{aligned}$$

(Il coniugato $\overline{x}$ di un quaternione x è stato definito nell'Eserc.(2.H)). Definiamo inoltre

$$\overline{\alpha + \beta\ell} = \overline{\alpha} - \beta\ell, \qquad \mathrm{N}(x) = x\overline{x}, \qquad (\alpha,\, \beta \in \mathbb{H}, \quad x \in \mathbb{O}).$$

(i) Dimostrare che gli ottetti con l'addizione formano un gruppo abeliano.

(ii) Dimostrare che l'insieme $\mathbb{O}$ degli ottetti non zero con la moltiplicazione soddisfa le condizioni G_0, G_2 e G_3, ma non G_1 nè G_4.

(iii) Dimostrare

$$\begin{aligned} \overline{x + y} &= \overline{x} + \overline{y}, \\ \overline{xy} &= \overline{yx}, \\ \mathrm{N}(xy) &= \mathrm{N}(x)\mathrm{N}(y). \end{aligned}$$

Le sfere n-dimensionali $S^n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1} : x_0^2 + x_1^2 + \ldots + x_n^2 = 1\}$ hanno certe notevoli proprietà geometriche solo per le dimensioni $n = 1, 3$ e 7. Si possono spiegare queste proprietà con le proprietà algebriche di $\mathbb{C}$, $\mathbb{H}$ e $\mathbb{O}$ di dimensione rispettivamente $2, 4$ e 8. Si veda Hirzebruch, F.: *Divisionsalgebren und Topologie* in Ebbinghaus, H.-D. et al: *Zahlen*, Grundwissen Mathematik I, Springer-Verlag, Berlin 1983.

(2.W) (*Il gruppo di Rubik*). Si può, in modo naturale, associare un gruppo R al noto cubo di Rubik: gli elementi di R sono le mosse che si possono fare ruotando le facce. La composizione AB di due mosse A e B è semplicemente la mossa "prima fare B e poi A. Verificare che R con la composizione è un gruppo. Si può dimostrare che R ha 43252003274489856000 elementi.

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*) Sia n un intero positivo. L'insieme H delle rotazioni in D_n è un sottogruppo del gruppo diedrale D_n. Questo segue dal Teorema 3.3(*ii*) e dal fatto che l'inverso di una rotazione è una rotazione e il prodotto di due rotazioni è una rotazione.

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

(*v*) 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.L)) 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 positivi 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. □

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) $\{\pm1,\pm i\}\subset\mathbb{C}^*$

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

(v) $D_d\subset D_n$ per d un divisore positivo di $n\in\mathbb{Z}_{>0}$,

(vi) $\{x\in\mathbb{Q}^*:$ esistono $a,b\in\mathbb{Q}$ tali che $x=a^2+b^2\}$,

(vii) Le rotazioni con centro $\mathbf{0}$ in $O_2(\mathbb{R})$.

(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) Sia $G = \{f_{a,b} : a \in \mathbb{R}^*, b \in \mathbb{R}\}$ dove $f_{a,b}(x) = ax + b$ è detta trasformazione affine di $\mathbb{R}$ (si veda l'Eserc. (2.S)). Dimostrare che l'applicazione $F : G \longrightarrow \mathbb{R}^*$ data da $F(f_{a,b}) = a$ è un omomorfismo. Determinare l'immagine ed il nucleo.

(3.L) (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.M) Provare che

$$(\mathbb{Z}/12\mathbb{Z})^* \cong V_4 \cong D_2 \cong P(X)$$

dove $P(X)$ è l'insieme dei sottoinsiemi dell'insieme X di due elementi. (Si veda l'Eserc. (2.K).)

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

(3.O) Sia Δ_3 il triangolo equilatero con baricentro $\mathbf{0}$ dell'Esempio 2.18. Sia X l'insieme dei tre vertici 1,2,3 di Δ_3. Ogni elemento $A \in D_3$ induce una permutazione dei vertici di Δ_3. Questo definisce un'applicazione

$$D_3 \longrightarrow S_3.$$

Dimostrare che si tratta di un isomorfismo.

(3.P) 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.Q) (i) Dimostrare che

$$\mathbb{R}^* \cong \mathbb{R}_{>0} \times \{\pm 1\}.$$

(Sugg. Utilizzare l'Eserc.(3.P))

(ii) Dimostrare che l'applicazione data da $\mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x$ è un isomorfismo.

(iii) Dimostrare che

$$\mathbb{R}^* \cong \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}.$$

(Sugg. Utilizzare (i) e (ii))

(iv) Sia $G = \mathbb{R}^* \cup \{ix : x \in \mathbb{R}^*\} \subset \mathbb{C}$. Dimostrare che G è un gruppo moltiplicativo. Dimostrare

$$G \cong \mathbb{R} \times \mathbb{Z}/4\mathbb{Z}.$$

(3.R) Sia n un intero positivo e *dispari.* Dimostrare che

$$D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}.$$

(Sugg. Utilizzare l'Eserc.(3.P))

(3.S) (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

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

(3.T) (*Teorema cinese generalizzato*) Siano $n_1, n_2, \ldots, n_t \in \mathbb{Z}_{>0}$ tali che $\mathrm{mcd}(n_i, n_j) = 1$ per $i, j \in \{1, 2, \ldots, t\}$ e $i \neq j$ e siano $a_1, a_2, \ldots a_t \in \mathbb{Z}$. Mostrare che esiste un $x \in \mathbb{Z}$ tale che $x \equiv a_i \bmod n_i$ per ogni $i \in \{1, 2, \ldots, t\}$. L'intero x è unico modulo $n_1 n_2 \cdots n_t$.

(3.U) * Siano $n, m \in \mathbb{Z}$ positivi. Far vedere che

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/\mathrm{mcd}(n,m)\mathbb{Z}) \times (\mathbb{Z}/\mathrm{mcm}(n,m)\mathbb{Z})\,.$$

(3.V) * (*Simmetrie del cubo.*) Sia G il gruppo delle isometrie di $\mathbb{R}^3$ che trasformano un cubo con centro di gravità in $\mathbf{0}$ in se stesso. Sia $H \subset G$ l'insieme $\{\mathrm{id}_{\mathbb{R}^3}, \sigma\}$, dove σ è la trasformazione $\mathbf{x} \mapsto -\mathbf{x}$ e sia H' il sottoinsieme delle trasformazioni che rispettano l'*orientazione* di $\mathbb{R}^3$ (Siccome le isometrie sono mappe lineari A, questa equivale a dire che $H' = \{A : \det(A) > 0\}$).

(i) Dimostrare che H e H' sono sottogruppi. Dimostrare che $G \cong H \times H'$.

(ii) Ogni elemento $g \in G$ induce una permutazione delle 4 diagonali interne del cubo. Così otteniamo un'applicazione

$$f : G \longrightarrow S_4.$$

Dimostrare che f è un omomorfismo. Dimostrare che la restrizione di f al gruppo H' è un isomorfismo.

(iii) Dimostrare che

$$G \cong S_4 \times \mathbb{Z}/2\mathbb{Z}.$$

4 Permutazioni

In questo paragrafo discuteremo i gruppi *simmetrici* S_n introdotti nell'Esempio 2.16. Gli elementi di S_n sono le biiezioni da $\{1,2,\dots,n\}$ a $\{1,2,\dots,n\}$. Esse vengono dette *permutazioni dell'insieme* $\{1,2,\dots,n\}$.

4.1 Proposizione. . La cardinalità di S_n è $n!$

Dimostrazione. Dobbiamo determinare quante sono le biiezioni σ dall'insieme $\{1,2,\dots,n\}$ a $\{1,2,\dots,n\}$. Per $\sigma(1)$ ci sono n possibilità. Dopo aver scelto l'immagine $\sigma(1)$ di 1, ci sono ancora $n-1$ possibiltà per $\sigma(2)$. Dopo aver scelto l'immagine $\sigma(2)$ di 2, ci sono ancora $n-2$ possibiltà per $\sigma(2)$. ... ecc. Ci sono dunque $n(n-1)(n-2)\cdot\ldots = n!$ biiezioni, come richiesto. □

4.2 Cicli. Prima di studiare i gruppi S_n, introduciamo una notazione efficiente per gli elementi di S_n.

4.3 Definizione. Una permutazione $\sigma \in S_n$ si dice un *ciclo* se esistono $a_1, a_2, \dots, a_k$ distinti in $\{1,2,\dots,n\}$ tali che

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \dots \ \sigma(a_{k-1}) = a_k, \quad \sigma(a_k) = a_1, \quad \sigma(x) = x \quad \text{se } x \notin \{a_1, a_2, \dots, a_k\}.$$

La notazione per il ciclo σ è $\sigma = (a_1\, a_2\, \dots\, a_k)$. L'intero k si dice la *lunghezza* di σ. Si dice anche che σ è un *k-ciclo.* I 2-cicli si dicono anche *trasposizioni.* L'elemento neutro di S_n si indica con (1). Per convenzione (1) è un 1-ciclo.

4.4 Esempio. Prendiamo $n = 4$. La biiezione σ data da

$$1 \mapsto 2 \qquad 2 \mapsto 3 \qquad 3 \mapsto 1 \qquad 4 \mapsto 4$$

è un ciclo. Infatti, $\sigma = (1\,2\,3)$. La notazione non è unica. Per esempio è anche che $\sigma = (2\,3\,1)$ oppure $\sigma = (3\,1\,2)$. La lunghezza di σ è 3. Non ogni permutazione è un ciclo. Per esempio la biiezione τ data da

$$1 \mapsto 2 \qquad 2 \mapsto 1 \qquad 3 \mapsto 4 \qquad 4 \mapsto 3$$

non è un ciclo ma un prodotto di due cicli: $\tau = (1\,2)(3\,4)$. I cicli $(1\,2)$ e $(3\,4)$ sono *disgiunti.*

4.5 Definizione. Due cicli $(a_1\, a_2\, \dots\, a_s)$ e $(b_1\, b_2\, \dots\, b_t)$ si dicono *disgiunti* se $a_i \neq b_j$ per ogni $i \in \{1,2,\dots,s\}$ e $j \in \{1,2,\dots,t\}$.

In generale, se $\sigma, \tau \in S_n$, non è vero che $\sigma\tau = \tau\sigma$. Questo si vede, per esempio, prendendo $\sigma = (1\,2\,3)$ e $\tau = (1\,2)$. Per σ e τ cicli disgiunti invece vale $\sigma\tau = \tau\sigma$ (si veda l'Eserc. (4.F)).

4.6 Teorema . Ogni $\sigma \in S_n$ è un prodotto di cicli disgiunti in modo unico a meno dell'ordine.

Dimostrazione. Se $n = 1$ abbiamo che $\sigma = (1)$ e non c'è niente da dimostrare. Procediamo per induzione su n. Scegliamo $x \in \{1,2,\dots,n\}$ e consideriamo il sottoinsieme

$$Y = \{x, \sigma(x), \sigma^2(x), \dots\}.$$

Siccome $Y \subset \{1, 2, \ldots, n\}$, l'insieme Y è finito. Abbiamo perciò $\sigma^l(x) = \sigma^m(x)$, per certi $m > l \geq 0$. Applicando σ^{-l} troviamo $\sigma^{m-l}(x) = x$. L'intero $m - l$ è positivo. Sia k l'intero positivo minimo tale che $\sigma^k(x) = x$. Allora

$$Y = \{x, \sigma(x), \sigma^2(x), \ldots . \sigma^{k-1}(x)\}$$

e gli elementi $\sigma^i(x)$ sono, per $0 \leq i < k$, distinti. Siccome σ è una biiezione, essa rispetta il complemento Z di Y in $\{1, 2, \ldots, n\}$, cioè $\sigma(Z) = Z$. Quindi, dato che l'insieme Z ha meno di n elementi, la permutazione σ, *ristretta a* Z, è un prodotto $\pi_1\pi_2 \ldots \pi_t$ di cicli disgiunti π_i. Su Y la permutazione σ è data dal ciclo $(x\, \sigma(x) \ldots \sigma^{k-1}(x))$ e questo ciclo è disgiunto dai cicli π_i. Quindi σ è uguale al prodotto $(x\, \sigma(x) \ldots \sigma^{k-1}(x))\pi_1\pi_2 \ldots \pi_t$.

L'unicità della decomposizione segue facilmente dal fatto che σ è una biiezione. Questo dimostra Teorema 4.6. □

4.7 Esempio. Utilizzando la nostra notazione è facile moltiplicare permutazioni. Prendiamo, per esempio, $n = 6$ e le permutazioni $\sigma = (1\,2\,5\,3\,4)$ e $\rho = (1\,6\,2\,5\,4\,3)$ in S_6. Calcoliamo il prodotto

$$\sigma\rho = (1\,2\,5\,3\,4)(1\,6\,2\,5\,4\,3).$$

Prima consideriamo il primo elemento: 1. Si vede che ρ manda 1 in 6 e poi σ manda 6 in 6. Allora $(\sigma\rho)(1) = 6$. Poi consideriamo 6. Si vede che $\rho(6) = 2$ e $\sigma(2) = 5$. Allora $(\sigma\rho)(6) = 5$. Poi consideriamo 5. Abbiamo $\rho(5) = 4$ e $\sigma(4) = 1$. Concludiamo che $(\sigma\rho)(5) = 1$. Abbiamo trovato un ciclo: $(1\,6\,5)$. Per trovare tutto l'effetto di $\sigma\rho$ prendiamo il primo elemento che non abbiamo ancora incontrato: 2. Si controlla che $(\sigma\rho)(2) = \sigma(5) = 3$ e poi $(\sigma\rho)(3) = \sigma(1) = 2$. Un altro ciclo è $(2\,3)$. L'unico elemento che non abbiamo ancora incontrato è 4. Dovrebbe essere fissato. Controlliamo: $(\sigma\rho)(4) = \sigma(3) = 4$. Dunque 4 è fissato. Abbiamo trovato che $\sigma\tau$ è un prodotto di due cicli disgiunti:

$$\sigma\rho = (1\,6\,5)(2\,3).$$

4.8 Il segno. Allo scopo di definire il *segno* di una permutazione in S_n consideriamo l'insieme Ω delle funzioni da $\mathbb{Z}^n$ a $\mathbb{Z}$. Gli elementi di Ω sono dunque funzioni $h(X_1, \ldots, X_n)$ di n variabili intere $X_1, \ldots, X_n$. Per $h \in \Omega$ e $\sigma \in S_n$ definiamo $\sigma(h) \in \Omega$ mediante

$$(\sigma(h))(X_1, \ldots, X_n) = h(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Per esempio, per $n = 3$, $h = X_1^2 - X_2X_3$ e $\sigma = (1\,2\,3)$, abbiamo

$$(\sigma(h))(X_1, X_2, X_3) = h(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = X_{\sigma(1)}^2 - X_{\sigma(2)}X_{\sigma(3)} = X_2^2 - X_3X_1.$$

Una funzione importante in Ω è data da

$$D(X_1, \ldots, X_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j).$$

A meno del segno, ogni differenza $X_i - X_j$ appare nel prodotto esattamente una volta. Dunque, per ogni $\sigma \in S_n$, si ha

$$(\sigma(D))(X_1, \ldots, X_n) = \pm D(X_1, \ldots, X_n).$$

4.9 Definizione. Sia $\sigma \in S_n$. Il *segno* di σ è l'intero $\varepsilon(\sigma) \in \{+1, -1\}$ tale che

$$(\sigma(D))(X_1, \ldots, X_n) = \varepsilon(\sigma) D(X_1, \ldots, X_n).$$

Le permutazioni σ con $\varepsilon(\sigma) = 1$ si dicono *pari*, e quelle con $\varepsilon(\sigma) = -1$ *dispari*.

4.10 Esempio. Per esempio, per $n = 3$ abbiamo $D(X_1, X_2, X_3) = (X_1 - X_2)(X_1 - X_3)(X_2 - X_3)$. Per $\sigma = (1\,2) \in S_3$ si ha

$$(\sigma(D))(X_1, X_2, X_3) = D(X_2, X_1, X_3) = (X_2 - X_1)(X_3 - X_1)(X_3 - X_2) = -D(X_1, X_2, X_3)$$

e dunque $\varepsilon((1\,2)) = -1$.

4.11 Teorema. . Siano σ, τ due permutazioni in S_n. Allora

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

In altre parole, il segno $\varepsilon : S_n \longrightarrow \{+1, -1\}$ è un omomorfismo.

Dimostrazione. È banale verificare che per ogni $h \in \Omega$ ed ogni $\sigma, \tau \in S_n$ si ha

$$(\sigma\tau)(h) = (\sigma(\tau(h)).$$

Abbiamo perciò

$$\begin{aligned} \varepsilon(\sigma\tau)D &= (\sigma\tau)(D) \\ &= (\sigma(\tau(D)) \\ &= \sigma(\varepsilon(\tau)D) \\ &= \varepsilon(\tau)\sigma(D) = \varepsilon(\tau)\varepsilon(\sigma)D. \end{aligned}$$

Siccome D non è la funzione nulla, concludiamo che $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$, come richiesto. □

4.12 Teorema. Sia n un intero positivo.

(*i*) Sia $(a_1\, a_2\, \ldots\, a_k) \in S_n$ un k-ciclo. Allora

$$(a_1\, a_2\, \ldots\, a_k) = (a_1\, a_2)(a_2\, a_3) \ldots (a_{k-1}\, a_k)$$

(*ii*) Per ogni trasposizione τ si ha $\varepsilon(\tau) = -1$. In generale, per ogni k-ciclo τ si ha $\varepsilon(\tau) = (-1)^{k-1}$.

(*iii*) Ogni permutazione è un prodotto di trasposizioni. Se σ è il prodotto di k trasposizioni allora $\varepsilon(\sigma) = (-1)^k$.

Dimostrazione. Consideriamo la permutazione

$$\sigma = (a_1\, a_2)(a_2\, a_3)\dots(a_{k-1}\, a_k).$$

Ovviamente, se $x \notin \{a_1, a_2, \dots, a_k\}$, si ha $\sigma(x) = x$. Si verifica facilmente che $\sigma(a_i) = a_{i+1}$ per $1 \le i < k$ e che $\sigma(a_k) = a_1$. Concludiamo che σ ha lo stesso effetto del ciclo $(a_1\, a_2\, \dots\, a_k)$. In altre parole si ha $\sigma = (a_1\, a_2\, \dots\, a_k)$ come richiesto.
(ii) Sia $a \in \{1, 2, \dots, n\}$ e sia $\sigma = (a\, a+1)$. Si vede che $\sigma(i) < \sigma(j)$ se e soltanto se $i < j$, eccetto nel caso $i = a$ e $j = a+1$. Si conclude che solo il fattore $X_{\sigma(a)} - X_{\sigma(a+1)} = X_{a+1} - X_a$ "ha i termini in ordine sbagliato. Dunque $\varepsilon(\sigma) = -1$. Adesso sia $\sigma = (a\, b)$ una trasposizione qualsiasi. Per $b = a+1$ abbiamo gia visto che $\varepsilon(\sigma) = -1$. Se $b \neq a+1$, allora

$$(a\, b) = (b\, a+1)(a\, a+1)(b\, a+1)$$

e dunque

$$\varepsilon((a\, b)) = \varepsilon((b\, a+1))\varepsilon((a\, a+1))\varepsilon((b\, a+1)) = \varepsilon((a\, a+1))\varepsilon((b\, a+1))^2 = -1.$$

Questo dimostra la parte *(ii)* per $k = 2$.

Sia ora $k > 0$ un intero qualsiasi e sia $\sigma = (a_1\, a_2\, \dots\, a_k)$ un k-ciclo. Per il Teorema 4.11, la parte *(i)* e il caso $k = 2$ visto sopra, si ha

$$\varepsilon(\sigma) = \varepsilon((a_1\, a_2)) \cdot \varepsilon((a_2\, a_3)) \cdot \ldots \cdot \varepsilon((a_{k-1}\, a_k)) = (-1)^{k-1},$$

come richiesto.
(iii) Per il Teorema 4.6 ogni permutazione è un prodotto di cicli disgiunti e per la parte *(i)* ogni ciclo è un prodotto di trasposizioni. Il resto segue dal fatto che ε è un omomorfismo. Questo conclude la dimostrazione del teorema. □

4.13 Definizione. Sia n un intero positivo. Definiamo gruppo *alterno* il gruppo delle permutazioni pari di S_n:

$$A_n = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}.$$

Per il Teorema 3.11 l'insieme $A_n = \ker(\varepsilon)$ è un sottogruppo di S_n, che, per il Teorema 4.12, non contiene trasposizioni. Vale il seguente teorema:

4.14 Teorema. Sia n un intero positivo. Ogni $\sigma \in A_n$ è un prodotto di 3-cicli.

Dimostrazione. Sia $\sigma \in A_n \subset S_n$. Per il Teorema 4.12, σ è un prodotto di un numero *pari* di trasposizioni. Per dimostrare il teorema, basta dunque dimostrare che ogni prodotto di *due* trasposizioni diverse è un prodotto di 3-cicli. Per fare questo distinguiamo due casi:

Le due trasposizioni non sono digiunte. In questo caso abbiamo un prodotto del tipo $(a\, b)(b\, c)$ con a, b, c distinti. Siccome $(a\, b)(b\, c) = (a\, b\, c)$ questo caso è completo.
Le due trasposizioni sono disgiunte. Ora abbiamo un prodotto del tipo $(a\, b)(c\, d)$ con a, b, c, d distinti. Si verifica che $(a\, b)(c\, d) = (c\, a\, d)(a\, b\, c)$ e la dimostrazione è completa. □

Concludiamo questo paragrafo con un noto teorema di Cayley, che mostra che, in un certo senso, i gruppi simmetrici sono gruppi abbastanza generali.

4.15 Teorema. (*A. Cayley*) Ogni gruppo finito G è isomorfo a un sottogruppo di S_n per un certo intero postitivo n.

Dimostrazione. Sia $S(G)$ l'insieme delle biiezioni $G \longrightarrow G$ dell'Esempio 2.16. Definiamo una applicazione $I : G \longrightarrow S(G)$ per $I(g) = T_g$ dove $T_g(h) = gh$ per $h \in G$. Verifichiamo che l'applicazione I è ben definita, cioè che T_g è una biiezione. Siano $h, h' \in G$. Se $T_g(h) = T_g(h')$ allora $gh = gh'$ e dunque $h = h'$. Questo dimostra che T_g è una iniezione e, essendo G finito, una biiezione.

L'applicazione I è un omomorfismo perché

$$I(gg')(h) = T_{gg'}(h) = gg'h = T_g(g'h) = T_g(T_{g'}(h)) = I(g)(I(g')(h)) = (I(g) \cdot I(g'))(h).$$

L'omomorfismo I è iniettivo perché se $g \in \ker(I)$ allora $I(g) = \mathrm{id_G}$, cioè $T_g = \mathrm{id_G}$. Questo vuole dire che $gh = h$ per ogni $h \in G$ e prendendo $h = e$ si vede che $g = e$. Vediamo dunque che $\ker(I) = \{\mathrm{Id}_G\}$ e che I è iniettiva.

Ovviamente $S(G) \cong S_n$ per $n = \#G$. Identificando $S(G)$ con S_n troviamo un'omomorfismo iniettivo

$$I : G \hookrightarrow S_n.$$

Sia H l'immagine di I in S_n. Lasciamo al lettore la verifica che l'applicazione $I : G \longrightarrow H$ è un isomorfismo. Questo dimostra il Teorema 4.15. □

4.16 Esempio. Come esempio applichiamo il Teorema 4.15 al gruppo V_4 di Klein (Esempio 2.12). Identificando l'insieme $\{e, a, b, c\}$ con $\{1, 2, 3, 4\}$ troviamo che

$$V_4 \cong \{(1),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\} \subset S_4.$$

Spesso la precedente è data come definizione di V_4.

Esercizi.

(4.A) Dimostrare che $(a_1\, a_2\, \ldots\, a_k)^{-1} = (a_k\, \ldots\, a_2\, a_1)$.

(4.B) Esprimere le seguenti permutazioni in S_9 come prodotti di cicli disgiunti. Calcolare gli inversi.

(i)
$$\sigma_1 \begin{cases} 1 \mapsto 9, & 4 \mapsto 1, & 7 \mapsto 2, \\ 2 \mapsto 7, & 5 \mapsto 3, & 8 \mapsto 5, \\ 3 \mapsto 8, & 6 \mapsto 4, & 9 \mapsto 6. \end{cases}$$

(ii)
$$\sigma_2 \begin{cases} 1 \mapsto 8, & 4 \mapsto 6, & 7 \mapsto 9, \\ 2 \mapsto 2, & 5 \mapsto 5, & 8 \mapsto 1, \\ 3 \mapsto 3, & 6 \mapsto 4, & 9 \mapsto 7. \end{cases}$$

(4.C) Esprimere il seguente prodotto come prodotto di cicli disgiunti:

$$(1\,9\,6\,4\,3\,8\,7)(1\,3\,7\,4\,8\,6\,2).$$

(4.D) Dimostrare che
$$S_3 = \{(1),\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2)\}.$$
Determinare $\varepsilon(\sigma)$ per ogni $\sigma \in S_3$.

(4.E) Siano $k, n \in \mathbb{Z}$, con $0 < k < n$. Definiamo
$$H = \{\sigma \in S_n : 1 \leq \sigma(i) \leq k \quad \text{per ogni } i \in \{1, 2, \ldots, k\}\}.$$
Far vedere che H è un sottogruppo di S_n, isomorfo a $S_k \times S_{n-k}$.

(4.F) Siano $\sigma, \tau \in S_n$ due cicli disgiunti. Far vedere che σ e τ commutano, cioè $\sigma\tau = \tau\sigma$.

(4.G) Siano $\sigma, \tau \in S_n$.

(i) Sia $a \in \{1, 2, \ldots, n\}$ e sia $a' = \tau(a)$. Far vedere che $\sigma\tau\sigma^{-1}$ manda $\sigma(a)$ a $\sigma(a')$.

(ii) Se $\tau = (a_1\, a_2\, \ldots\, a_k)$ è un k-ciclo, allora $\sigma\tau\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2)\, \ldots\, \sigma(a_k))$. (Sugg. Utilizzare (i).)

(iii) Far vedere che $\sigma^{-1}\tau\sigma$ è un ciclo e calcolarlo.

(4.H) Siano $\sigma, \tau \in S_n$. Se $\sigma\tau$ è un prodotto di t cicli disgiunti di lunghezze $k_1, k_2, \ldots, k_t$, allora questo è vero anche per $\tau\sigma$.

(4.I) Sia n un intero positivo e siano σ, $\tau \in S_n$. Provare che:

(i) $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

(ii) $\varepsilon(\tau\sigma\tau^{-1}) = \varepsilon(\sigma)$.

(4.J) Sia n un intero positivo.

(i) Siano $1 < a < b \leq n$. Calcolare $(1\,a)(1\,b)(1\,a)$.

(ii) Far vedere che si può scrivere ogni permutazione come prodotto di trasposizioni del tipo $(1\,a)$.

(4.K) Sia n un intero positivo e sia p un numero primo con $n/2 < p \leq n$. Provare: se $\sigma \in S_n$ soddisfa $\sigma^p = (1)$ ma $\sigma \neq (1)$, allora σ è un p-ciclo.

(4.L) Sia $\sigma = (1\,2\,\ldots\,n) \in S_n$. Far vedere: se $\tau \in S_n$ sodisfa $\tau\sigma = \sigma\tau$ allora τ è una potenza di σ.

(4.M) Sia $n \neq 2$. Dimostrare che il centro di S_n è banale.

(4.N) Dimostrare che S_n contiene un sottogruppo isomorfo a D_n.

(4.O) Trovare il più piccolo intero n tale che S_n contiene un sottogruppo isomorfo a $\mathbb{Z}/6\mathbb{Z}$.

(4.P) (*Il teorema di Cayley per il gruppo Q dei quaternioni.*) Sia n un intero positivo e supponiamo che $H \subset S_n$ sia un sottogruppo isomorfo al gruppo Q dei quaternioni (Es.2.11). Sia τ la permutazione in H a cui corrisponde l'elemento $-1 \in Q$ tramite l'isomorfismo.

(i) Sia $x \in \{1, 2, \ldots, n\}$. Dimostrare: se $\tau(x) \neq x$ allora $\sigma(x) \neq x$ per ogni permutazione non banale $\sigma \in H$.

(ii) Dimostrare che $n \geq 8$.

(4.Q) (i) Il famoso puzzle di *Sam Lloyd* (1841–1911, statunitense noto per i suoi rompicapo) consiste in 15 blocchetti, numerati da 1 a 15, in un telaio. Utilizzando l'unica posizione vuota, essi si possono spostare orizzontalmente o verticalmente. Lo scopo del gioco è di ordinare i blocchetti da 1 a 15 per righe. Far vedere che questo è impossibile a partire dalla configurazione rappresentata a destra.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

(ii) Lo stesso gioco come in (i). In Trentino sanno ordinare i blocchetti cominciando dalla configurazione rappresentata a sinistra. Come mai?

33	tren	tini	an
da	va	no	per
Trento	tut	ti	33
trot	do	tan	

5 Generatori, ordine e indice

5.1 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.

5.2 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.

5.3 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.

5.4 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.(5.F) 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.

5.5 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 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.

5.6 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.

5.7 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 $\{e\}$ 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.5.6, 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 5.7. □

5.8 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. □

5.9 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.

5.10 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.

5.11 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 5.11. □

5.12 Si potrebbe dire che il Teorema 5.11 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.

5.13 Vale un analogo del Teorema 5.11 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 $ab^{-1} \in H$.

5.14 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! □

5.15 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.

5.16 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.(5.R) per il fatto che $[G : H]$ è anche uguale al numero delle classei laterali destre di H.

5.17 Esempio.

(*i*) Nell'esempio 5.10(*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 5.10(*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 $[G : H] = 3$.

5.18 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 5.11 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 5.14 ogni classe laterale ha la stessa cardinalità di H. Concludiamo che

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

come richiesto. □

5.19 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'. □

5.20 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 5.19(*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 5.6 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. □

5.21 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 5.7(*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. □

5.22 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:

5.23 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.5.20 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. □

5.24 Lista. Concludiamo questo paragrafo con la lista dei gruppi di ordine al più 15. Non diamo una dimostrazione della completezza della lista. Tutti i gruppi sono distinti, cioè non isomorfi.

$\#G$	comm.	non comm.
1	$\{e\}$	
2	C_2	
3	C_3	
4	C_4, $C_2 \times C_2$	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	D_4, Q
9	C_9, $C_3 \times C_3$	
10	C_{10}	D_5
11	C_{11}	
12	C_{12}, $C_6 \times C_2$	D_6, A_4, B
13	C_{13}	
14	C_{14}	D_7
15	C_{15}	

Abbiamo scritto C_n per il gruppo $\mathbb{Z}/n\mathbb{Z}$. Ci sono diversi isomorfismi con altri gruppi: il gruppo V_4 di Klein è isomorfo a $C_2 \times C_2$ (Si veda l'esempio subito dopo il Teorema 3.12). Il gruppo simmetrico S_3 è isomorfo al gruppo diedrale D_3 (Eserc.(3.N)). Per l'Eserc.(3.Q) abbiamo $D_6 \cong D_3 \times C_2 \cong S_3 \times C_2$. La struttura del gruppo B di 12 elementi è descritta nell'Esercizio (5.S).

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.

(5.A) Dimostrare

(i) $D_n =< R, S >$, (Si veda l'Eserc.(2.R).)

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

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

(iv) $S_n =< (1\,2), (1\,2\,\ldots\,n) >$.

(5.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.

(5.C) Calcolare gli ordini degli elementi dei cinque gruppi Q, D_4, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ e $\mathbb{Z}/8\mathbb{Z}$.

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

(5.E) Calcolare $\max_{\sigma\in S_n} \mathrm{ord}(\sigma)$ per $1 \le n \le 8$.

(5.F) (*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) Far vedere 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

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

(5.G) Sia G un gruppo abeliano e siano $\alpha, \beta \in G$ di ordine finito a e b, rispettivamente. Far vedere che

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

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

(5.H) 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.

(5.I) 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 $\mathrm{mcm}(a,b)$.

(5.J) Siano G e G' due gruppi e sia $f : G \longrightarrow G'$ un omomorfismo. Far vedere 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 $g \in G$.

(5.K) Dimostrare che

$$Q \ncong D_4, \qquad S_4 \ncong D_{12}, \qquad A_4 \ncong S_3 \times \mathbb{Z}/2\mathbb{Z}.$$

(5.L) (i) Sia p un primo e sia $a \in \mathbb{Z}$. Far vedere 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 $a \in \mathbb{Z}$.

(5.M) Sia n un intero positivo e sia H il sottogruppo di S_n definito nell'Eserc.(4.E). Far vedere che l'ordine di H è $k!(n-k)!$. Concludere che $k!(n-k)!$ divide $n!$.

(5.N) Dimostrare: ogni numero n tale che $\mathrm{mcd}(n,10) = 1$ divide un intero non nullo che ha tutte le cifre uguali. Per esempio: 219 divide 33333333.

(5.O) Far vedere: per ogni primo $p > 5$, l'espansione decimale di $1/p$ è periodica con periodo un divisore di $p-1$. Calcolare il periodo di $1/83$.

Esempi:

$$\begin{aligned}
7^{-1} &= 0,14285714285714\ldots \\
11^{-1} &= 0,09090909090909\ldots \\
13^{-1} &= 0,07692307692307\ldots \\
17^{-1} &= 0,0588235294117647058823529411764705\ldots \\
19^{-1} &= 0,0526315789473684210526315789473684210 5\ldots \\
23^{-1} &= 0,0434782608695652173913043478260869565217391304 3\ldots \\
29^{-1} &= 0,0344827586206896551724137931034482758620689655172 41\ldots \\
31^{-1} &= 0,0322580645161290322580645161290 3\ldots \\
37^{-1} &= 0,02702702702702702\ldots \\
41^{-1} &= 0,0243902439024390243902\ldots
\end{aligned}$$

(5.P) (*Numeri di Mersenne.*) Sia $p > 2$ un primo e sia $M_p = 2^p - 1$ un numero di Mersenne. (Si veda l'Eserc.(1.Q).) Dimostrare che ogni divisore di M_p è congruente a $1 \bmod 2p$. (Sugg. Sia l un divisore primo di M_p. Calcolare l'ordine di $\overline{2}$ in $(\mathbb{Z}/l\mathbb{Z})^*$.)

(5.Q) (*Numeri di Fermat.*) Sia k un intero non negativo e sia $F_k = 2^{2^k} + 1$ un numero di Fermat. (Si veda l'Eserc.(1.S).)

(i) Dimostrare che ogni divisore di F_k è congruente a $1 \bmod 2^{k+1}$. (Sugg. Sia l un divisore primo di F_k. Calcolare l'ordine di $\overline{2}$ in $(\mathbb{Z}/l\mathbb{Z})^*$.)

(ii) Sia $k \geq 2$ e $\alpha = 2^{2^{k-2}}$. Sia l un divisore primo di F_k. Dimostrare che $\alpha \in (\mathbb{Z}/l\mathbb{Z})^*$ sodisfa $(\alpha + \alpha^{-1})^2 = 2$. Concludere che $l \equiv 1 \bmod 2^{k+2}$.

(5.R) 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.

(5.S) 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 con questa moltiplicazione. Far vedere che B è un gruppo non abeliano. Far vedere che $B \ncong A_4$ e $B \ncong D_6$.

(5.T) Sia G un gruppo e X un sottoinsieme di G.

(i) Dimostrare: se $\#X > \#G/2$ allora $G =< X >$. Far vedere: Per ogni $g \in G$ esistono $x, y \in X$ tali che $g = xy$.

(ii) Sia p il più piccolo divisore primo di $\#G$. Far vedere che se $\#X > \#G/p$ allora $G =< X >$.

(5.U) 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.V) Sia X un insieme e sia

$$S'(X) = \{\sigma \in S(X) : \sigma(x) = x \text{ per ogni } x \in X, \text{ tranne un numero finito}\}.$$

Dimostrare che $S'(X)$ è un sottogruppo di $S(X)$ e far vedere che $S'(X)$ contiene un sottogruppo di indice 2.

6 Sottogruppi normali e gruppi quoziente

6.1 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.

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

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

6.3 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 $ghg^{-1} \in Z(G)$.

(*iv*) Il sottogruppo delle permutazioni pari A_n di S_n è normale: sia $\sigma \in A_n$ e sia $\tau \in S_n$, allora $\varepsilon(\tau\sigma\tau^{-1}) = \varepsilon(\tau)\varepsilon(\sigma)\varepsilon(\tau)^{-1} = \varepsilon(\tau)\varepsilon(\tau)^{-1} = 1$. Quindi $\tau\sigma\tau^{-1} \in A_n$.

6.4 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. □

6.5 Esempio. Nell'Esempio 5.10(*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 6.4 concludiamo che H non è un sottogruppo normale di S_3.

6.6 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 6.4. □

6.7 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. □

6.8 Esempi.

(*i*) Consideriamo il gruppo diedrale D_n di ordine $2n$. Le n rotazioni in D_n formano un sottogruppo H. Siccome H ha indice 2 in D_n il sottogruppo H è normale per il Teorema 6.6.

(*ii*) Sia $n \geq 6$ un intero *pari* e sia D_n il gruppo diedrale. Consideriamo l'insieme X delle diagonali del n-gono regolare. Siccome n è pari, l'insieme X ha cardinalità $n/2$. Ogni elemento $A \in D_n$ induce una permutazione di X. In questo modo otteniamo un omomorfismo

$$f : D_n \longrightarrow S(X).$$

È facile verificare che il nucleo di f contiene soltanto l'identità e la rotazione R_π con centro **O** e angolo π. Per il Teorema 6.7, il gruppo $\{\mathrm{id}, R_\pi\}$ è un sottogruppo normale di D_n.

6.9 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 5, 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 5.11).

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 5.11 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 $[G : N]$.

6.10 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 latterale, cioè $x = gN$ per un certo $g \in G$. Allora $x = \pi(g)$ e perciò π è suriettivo. Abbiamo $g \in \ker(\pi)$ se e soltanto se $\overline{g} = N$, cioè $gN = N$ e questo vale se e soltanto se $g \in N$. □

6.11 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 7.5 che $\mathbb{R}/\mathbb{Z}$ è, in un certo senso, una circonferenza.

6.12 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.(6.S) per un esempio.

6.13 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.

(6.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.

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

(i) G è abeliano.,

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

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

(6.C) Sia $V_4 \subset S_4$ il sottogruppo $\{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ dato in Esempio 4.16. Far vedere che $V_4 \subset A_4$. Dimostrare che V_4 è un sottogruppo normale di S_4. (Sugg. considerare gli ordini degli elementi in A_4.)

(6.D) 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.

(6.E) Sia G un gruppo e siano N, M due sottogruppi normali di G che soddisfano $N \cap M = \{e\}$. Far vedere:

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

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

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

(6.F) Sia G un gruppo e sia $N \subset G$ un sottogruppo normale di ordine 2. Far vedere che $N \subset Z(G)$.

(6.G) Dimostrare che ogni sottogruppo del gruppo Q dei quaternioni è normale in Q.

(6.H) Determinare i sottogruppi normali del gruppo diedrale D_4.

(6.I) Dare un esempio di un gruppo G e di sottogruppi $H, N \subset G$ tali che

$$\begin{array}{l} H \subset N \subset G, \\ N \text{ è un sottogruppo normale di } G, \\ H \text{ è un sottogruppo normale di } N, \\ H \textit{ non} \text{ è un sottogruppo normale di } G. \end{array}$$

(6.J) 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. Far vedere che N è "massimale, cioè, se $M \subset H$ è un sottogruppo normale di G, allora $M \subset N$.

(6.K) Sia n un intero positivo. Dimostrare che $[S_n, S_n] = A_n$. (Sugg. Utilizzare il Teorema 4.14).

(6.L) Determinare la struttura di D_4/N per ogni sottogruppo normale N del gruppo diedrale D_4.

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

(6.N) 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.

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

(6.P) Sia $\mathrm{N} : \mathbb{H}^* \longrightarrow \mathbb{R}^*$ l'applicazione "norma dell'Eserc.(2.H). 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) $[\mathbb{H}^*, \mathbb{H}^*] = \ker(N) = \{x \in \mathbb{H}^* : x\overline{x} = 1\}$.

(6.Q) Sia $n \geq 2$ un intero. Dimostrare che

$$\begin{array}{lll} [A_2, A_2] & = \{(1)\} & \\ [A_3, A_3] & = \{(1)\} & \\ [A_4, A_4] & = V_4 & \text{si veda l'Eserc.(6.C),} \\ [A_n, A_n] & = A_n & \text{per } n \geq 5. \end{array}$$

(6.R) 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 $N \subseteq H$.

(6.S) 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

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

Far vedere 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 $\mathbb{Z}/3\mathbb{Z}$.)

(6.T) 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.U) Trovare un gruppo G con sottogruppi normali N_1, N_2 tali che

$$N_1 \cong N_2 \qquad G/N_1 \ncong G/N_2.$$

(6.V) Dimostare che S_n e $A_n \times \mathbb{Z}/2\mathbb{Z}$ sono gruppi non isomorfi per $n \geq 3$.

7 Teoremi di isomorfismo

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

7.1 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

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

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. □

7.2 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 7.1 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).

7.3 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 7.1 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.

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

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

Dimostrazione. Immediata dal Teorema 7.3. □

7.5 Esempio. Come esempio studiamo il sottogruppo $S = \{z \in \mathbb{C}^* : z\overline{z} = 1\}$ di $\mathbb{C}^*$ (Si veda l'Eserc.(2.F) 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 7.4:

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

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

7.6 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 7.1.

7.7 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 6.13,

abbiamo $[G,G] \subset \ker(f)$. Adesso il Teorema 7.1 con $N = [G,G]$ ha come consequenza il risultato. □

7.8 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 $a = h_1n_1 \in HN$ e $b = h_2n_2 \in HN$. Siccome N è un sottogruppo normale abbiamo

$$h_2(n_1n_2^{-1})h_2^{-1} = n_3 \in N.$$

Dunque, $ab^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1}n_3 \in HN$. 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 7.4. □

7.9 Applicazione. Diamo una applicazione del Teorema 7.8. Sia G il gruppo simmetrico S_4 e sia $N = V_4$ il sottogruppo dato da

$$\{(1),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$$

Si veda l'Eserc.(6.C) per una dimostrazione dal fatto che N è un sottogruppo normale di G. Sia H l'insieme delle permutazioni che fissano l'elemento 4:

$$H = \{\sigma \in S_4 : \sigma(4) = 4\}.$$

L'insieme H è un sottogruppo di G. Abbiamo che $H \cong S_3$. Applichiamo il Teorema 7.8:

$$H/(N \cap H) \cong NH/N.$$

Poiché solo l'elemento neutro di V_4 ha punti fissi, segue che $N \cap H = \{(1)\}$ e quindi $H/(N \cap H) \cong H$. Abbiamo che

$$N \subset NH \subset S_4.$$

L'indice $[NH : N] = \#H = 6$. D'altra parte, per il Teorema di Lagrange 5.18 l'indice $[S_4 : N]$ è uguale a 24/4=6. Concludiamo che $NH = S_4$. Sostituiamo tutto questo e troviamo

$$S_3 \cong H \cong S_4/V_4.$$

Abbiamo dunque calcolato la struttura del gruppo quoziente S_4/V_4. Si veda l'Eserc.(7.L) per una interpretazione geometrica di questo isomorfismo.

7.10 Teorema. (Terzo teorema di isomorfismo).
Sia G un gruppo e siano N, N' due sottogruppi normali di G tali che

$$N \subset N' \subset G.$$

Allora N'/N è un sottogruppo normale di G/N ed ogni sottogruppo normale di G/N ha la forma M/N dove M è un sottogruppo normale con $N \subset M \subset G$. Abbiamo

$$(G/N)/(N'/N) \cong G/N'.$$

Dimostrazione. Si veda l'Esercizio (6.R) per il fatto che N'/N è un sottogruppo di G/N e che ogni sottogruppo di G/N ha la forma M/N per un sottogruppo M di G con $N \subset M \subset G$. Basta quindi far vedere che M/N è normale in G/N se e soltanto se M è normale in G. Questo è immediato: supponiamo che M sia un sottogruppo normale di G. Sia $\overline{m} = mN \in M/N$ e sia $\overline{g} \in G/N$. Abbiamo $\overline{g}\,\overline{m}\,\overline{g}^{-1} = \overline{gmg^{-1}}$. Siccome M è normale abbiamo $gmg^{-1} \in M$, cioè $\overline{gmg^{-1}} \in M/N$ come richiesto. Il viceversa si dimostra in modo simile.

Adesso dimostriamo l'isomorfismo. Consideriamo l'applicazione *canonica* $\pi : G \longrightarrow G/N'$. Applichiamo il Teorema 7.1 al sottogruppo normale $N \subset N'$. Questo ci dà un omomorfismo

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

con $h(gN) = f(g) = gN'$.

Siccome l'applicazione canonica $G \longrightarrow G/N'$ è suriettiva, anche la mappa h è suriettiva. Adesso il corollario 7.4 ci dà un isomorfismo

$$(G/N)/\ker(h) \cong G/N'.$$

Calcoliamo il nucleo $\ker(h)$: una classe gN è nel nucleo di h se e soltanto se $gN' = N'$, cioè $g \in N'$. Dunque

$$\ker(h) = \{gN : g \in N'\} = N'/N$$

come richiesto. □

7.11 Esempio. Come esempio di applicazione del Teorema 7.10, sia H il sottogruppo $\{\overline{0}, \overline{3}\}$ di $\mathbb{Z}/6\mathbb{Z}$. (Si veda il Teorema 3.6). Si potrebbe calcolare la struttura di $(\mathbb{Z}/6\mathbb{Z})/H$ così: sia $G = \mathbb{Z}$, sia $N' = 3\mathbb{Z}$ e sia $N = 6\mathbb{Z}$. Il gruppo N'/N è uguale a

$$\{\ldots, -3, 0, 3, 6\ldots\}/6\mathbb{Z} = \{\overline{0}, \overline{3}\} \subset \mathbb{Z}/6\mathbb{Z}.$$

Il Teorema 7.10 ci dà

$$(\mathbb{Z}/6\mathbb{Z})/(\{\overline{0}, \overline{3}\}) \cong \mathbb{Z}/3\mathbb{Z}.$$

Esercizi.

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

(7.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 $< g >$. Far vedere che F è iniettiva se e soltanto se g ha ordine infinito. Se F non è iniettiva, utilizzare il Teorema 7.3 per dimostrare che $\mathbb{Z}/n\mathbb{Z} \cong < g >$ dove n è l'ordine di g.

(7.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 $(G/N_1) \times (G/N_2)$.

(7.D) Sia $n \geq 2$ un intero. Determinare tutti gli omomorfismi $S_n \longrightarrow \mathbb{C}^*$.

(7.E) Dimostrare che l'insieme $H = \{\overline{1}, \overline{11}\}$ è un sottogruppo di $(\mathbb{Z}/15\mathbb{Z})^*$. Far vedere 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.

(7.F) Una trasformazione *affine* di $\mathbb{R}$ è una applicazione $A : \mathbb{R} \longrightarrow \mathbb{R}$ data da

$$A : x \mapsto ax + b$$

con $a \in \mathbb{R}^*$ e $b \in \mathbb{R}$. Sia G il gruppo delle trasformazioni affine di $\mathbb{R}$. (Si veda l'Eserc.(2.S).) Dimostrare che $f : G \longrightarrow \mathbb{R}^*$ data da $f(A) = a$ è un omomorfismo suriettivo. Sia $T = \{A \in G : A(x) = x + b, \text{ per un certo } b \in \mathbb{R}\}$ il sottogruppo delle traslazioni di $\mathbb{R}$. Far vedere che

$$G/T \cong \mathbb{R}^*$$

(7.G) Sia G un gruppo e siano N_1, N_2 due sottogruppi normali di G con $N_1 \cap N_2 = \{e\}$ e $N_1N_2 = G$. Far vedere 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 $g \mapsto (gN_1, gN_2)$).

(7.H) Dimostrare:

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

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

(7.I) Dimostrare che il gruppo diedrale D_n contiene D_d se e soltanto se d divide n. Far vedere che, per n pari, il gruppo $D_{n/2}$ è un sottogruppo normale di D_n. Dimostrare che, per n pari e n non divisibile per 4, si ha

$$D_n \cong D_{n/2} \times \mathbb{Z}/2\mathbb{Z}.$$

(7.J) (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 $N = \{(\overline{0}, \overline{0}),\ (\overline{2}, \overline{2})\}$.

(7.K) * Sia G il gruppo delle trasformazioni isometriche di $\mathbb{R}^3$ che rispettano un cubo con baricentro $\mathbf{0}$ (si veda l'Eserc.(2.T)). Sia

$$G \longrightarrow S_4$$

l'applicazione che associa a una isometria la permutazione indotta sulle diagonali del cubo.

(i) Dimostrare che questa applicazione è un isomorfismo.

(ii) Sia

$$F : G \longrightarrow S_3$$

l'applicazione che associa a una isometria la permutazione indotta sulle 3 coppie di lati opposti. Far vedere che F è un omomorfismo suriettivo. Provare che il nucleo di F è uguale al sottogruppo V_4.

(iii) Far vedere che

$$S_4/V_4 \cong S_3.$$

(7.L) * Sia G il gruppo delle 48 trasformazioni isometriche di $\mathbb{R}^3$ che rispettano un cubo con baricentro $\mathbf{0}$ (Si veda l'Eserc.(2.T)). Sia

$$F : G \longrightarrow S_4$$

l'applicazione che associa a una isometria la permutazione indotta sulle diagonali del cubo.

(i) Far vedere che F è un omomorfismo suriettivo. Determinarne il nucleo.

(ii) Sia H il sottogruppo di G delle isometrie che rispettano l'orientazione di $\mathbb{R}^3$ (quelle che hanno il determinante uguale a $+1$). Dimostrare che l'applicazione F ristretta ad H è un isomorfismo fra H e S_4.

(iii) Dimostrare che $G \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$.

8 Anelli

In questo paragrafo studiamo gli *anelli*. Diamo diversi esempi importanti di anelli ai quali faremo continuamente riferimento in seguito.

8.1 Definizione. Un anello R è un insieme fornito di due composizioni, *l'addizione* "$+$ e la *moltiplicazione* "$\cdot$, e di due elementi speciali, lo zero $0 \in R$, e l'identità $1 \in R$, in modo che valgano i seguenti assiomi:

(R_1) (*Gruppo additivo*) L'insieme R è un gruppo *abeliano* rispetto all'addizione e con elemento neutro 0.

(R_2) (*Associatività*) Per ogni $x, y, z \in R$

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

(R_3) (*L'identità*) Per ogni $x \in R$

$$1 \cdot x = x \cdot 1 = x.$$

(R_4) (*Distributività*) Per ogni $x, y, z \in R$

$$x \cdot (y + z) = x \cdot y + x \cdot z, \qquad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Questi assiomi definiscono precisamente una struttura di anello. In generale su un anello R non valgono gli assiomi (R_5) e (R_6):

(R_5) (*Commutatività*) Per ogni $x, y \in R$

$$x \cdot y = y \cdot x.$$

(R_6) (*Inverso moltiplicativo*) Per ogni $x \in R$, $x \neq 0$ esiste $x^* \in R$ tale che

$$x \cdot x^* = x^* \cdot x = 1.$$

Se per un anello R vale (R_5), l'anello R si dice *commutativo*. Se vale (R_6) e se R non è l'anello banale (si veda l'Esempio 8.3), l'anello R si dice *un anello con divisione*. Un anello commutativo con divisione si dice un *campo* oppure un *corpo*.

Come al solito, scriveremo spesso ab per il prodotto $a \cdot b$.

8.2 Esempio. Con l'addizione e la moltiplicazione introdotte nel primo paragrafo gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ sono anelli. Lasciamo al lettore la facile verifica. Gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono commutativi. Gli anelli $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ sono anelli con divisone (si vedano gli Esempi 2.9 e 2.10). Siccome la moltiplicazione in $\mathbb{H}$ non è commutativa, solo gli anelli $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono campi.

8.3 Esempio. (*L'anello banale*) Di solito, in un anello R gli elementi 0 e 1 sono distinti. Se invece $0 = 1$, ogni elemento di R è 0 perché per $x \in R$ vale

$$x = 1 \cdot x = 0 \cdot x = 0.$$

Per l'ultima uguaglianza si veda l'Eserc.(8.C). Dunque, se $0 = 1$, l'anello R è uguale a $\{0\}$. Questo anello si chiama *l'anello banale*.

8.4 Esempio. Con l'addizione dell'Esempio 2.13 e la moltiplicazione data da

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

l'insieme $\mathbb{Z}/n\mathbb{Z}$ ottiene la struttura di anello commutativo. Lasciamo le verifiche al lettore.

8.5 Esempio. (*L'anello degli interi di Gauss*) Sia $\mathbb{Z}[i]$ il sottoinsieme di $\mathbb{C}$ dato da

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : \ a, b \in \mathbb{Z}\}.$$

È facile verificare che $\mathbb{Z}[i]$ con l'addizione e la moltiplicazione di $\mathbb{C}$ è un anello commutativo.

8.6 Definizione. Sia R un anello. Un elemento $x \in R$ tale che esiste $x^* \in R$ con

$$x \cdot x^* = x^* \cdot x = 1$$

si dice un'*unità* di R. L'elemento x^* è l'unico elemento di R che soddisfa $x \cdot x^* = x^* \cdot x = 1$ (si veda l'Eserc. (8.D)) e si dice *l'elemento inverso di* x. Si scrive x^{-1} per l'elemento x^*. L'insieme delle unità di R si indica con R^*.

8.7 Osservazione. È da notare che le notazioni $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ e $\mathbb{H}^*$ coincidono con quelle del paragrafo 2. Anche la notazione $(\mathbb{Z}/n\mathbb{Z})^*$ coincide: nell'Esempio 2.14 abbiamo già dimostrato che il sottoinsieme $\{\overline{a} : \mathrm{mcd}(a, n) = 1\}$ di $\mathbb{Z}/n\mathbb{Z}$ è un gruppo moltiplicativo. Ogni elemento di questo gruppo ha dunque un inverso moltiplicativo. Viceversa, se $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ha un inverso moltiplicativo $\overline{b}$, allora $\overline{a}\,\overline{b} = \overline{1}$, cioè

$$ab = 1 + kn, \qquad \text{per un } k \in \mathbb{Z}.$$

Dunque, ogni divisore comune di a e n divide 1. Concludiamo che $\mathrm{mcd}(a,n)=1$ e quindi che $\overline{a}\in(\mathbb{Z}/n\mathbb{Z})^*$.

8.8 Proposizione. Sia R un anello. Le unità di R formano un gruppo moltiplicativo.

Dimostrazione. Ovviamente vale l'assioma dell'associatività. L'identità 1 è l'elemento neutro di R^*. Se $a,b\in R^*$ allora

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

e dunque $ab\in R^*$. Finalmente $a^{-1}\in R^*$ se $a\in R^*$. Concludiamo che R^* è un gruppo moltiplicativo. □

8.9 Esempio. Per esempio, il gruppo $\mathbb{Z}^*$ è uguale a $\{+1,-1\}$. Si veda l'Eserc.(8.L) per una dimostrazione che $\mathbb{Z}[i]^*=\{\pm1,\pm i\}$.

8.10 Proposizione. Sia n un intero positivo. L'anello $\mathbb{Z}/n\mathbb{Z}$ è un campo se e soltanto se n è un numero primo.

Dimostrazione. L'anello $\mathbb{Z}/n\mathbb{Z}$ è un campo se e soltanto se ogni $\overline{x}\in\mathbb{Z}/n\mathbb{Z}-\{0\}$ ha un inverso moltiplicativo. Cioè $\mathbb{Z}/n\mathbb{Z}$ è un campo se e soltanto se

$$(\mathbb{Z}/n\mathbb{Z})^*=\mathbb{Z}/n\mathbb{Z}-\{0\}.$$

Equivalentemente, ogni $a\in\mathbb{Z}$ con $0<a<n$ ha la proprietà $\mathrm{mcd}(a,n)=1$. Questo è possibile se e soltanto se n è un numero primo, come richiesto. □

8.11 Esempio. Visto che 11 è un primo, l'anello $\mathbb{Z}/11\mathbb{Z}$ è un campo. Gli inversi degli elementi di $\mathbb{Z}/11\mathbb{Z}$ sono:

$$\overline{1}^{-1}=\overline{1},\quad \overline{2}^{-1}=\overline{6},\quad \overline{3}^{-1}=\overline{4},\quad \overline{5}^{-1}=\overline{9},\quad \overline{7}^{-1}=\overline{8},\quad \overline{10}^{-1}=\overline{10}.$$

e, ovviamente, $\overline{4}^{-1}=\overline{3}$ etc. La verifica è facile, per esempio $\overline{5}\cdot\overline{9}=\overline{45}=\overline{1}$ quindi $\overline{5}^{-1}=\overline{9}$ e $\overline{9}^{-1}=\overline{5}$. In 2.14 si è spiegato come usare l'algoritmo di Euclide 1.18 per determinare l'inverso di un elemento diverso da $\overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$.

8.12 Definizione. Sia R un anello. Un elemento $a\in R$ si dice un *divisore di zero sinistro* se $a\neq0$ e se esiste $b\in R$ con $b\neq0$ e $ab=0$. L'elemento $a\in R$ si dice un *divisore di zero destro* se $a\neq0$ e se esiste $b\in R$ con $b\neq0$ e $ba=0$. L'elemento $a\in R$ si dice un *divisore di zero* se è un divisore di zero sia destro che sinistro.

8.13 Esempi. Negli anelli soliti $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ non ci sono divisori di zero. Ma esistono in altri anelli. Per esempio, in $\mathbb{Z}/6\mathbb{Z}$ si ha $\overline{2}\cdot\overline{3}=\overline{6}=\overline{0}$.

8.14 Proposizione. Un'unità di un anello R non può essere un divisore di zero.

Dimostrazione. Supponiamo che a sia un'unità ed anche un divisore di zero. Dunque esistono elementi $b, c \in R$ con

$$ab = 1, \qquad ca = 0, \quad (c \neq 0).$$

Abbiamo

$$0 = 0 \cdot b = (ca) \cdot b = c \cdot (ab) = c \cdot 1 = c,$$

contraddicendo $c \neq 0$. □

8.15 Dunque, gli anelli con divisione non possiedono divisori di zero, perché ogni elemento non nullo è un'unità. Più generalmente, ogni sottoanello (si veda l'Esempio 8.18) di un anello con divisione non contiene divisori di zero. L'anello $\mathbb{Z}$ e l'anello degli interi di Gauss $\mathbb{Z}[i]$ ne sono esempi.

8.16 Definizione. Un anello non banale che è commutativo e non possiede divisori di zero si dice un *dominio di integrità*.

8.17 Esempi. I campi sono esempi di domini di integrità. Come abbiamo visto sopra, anche i sottoanelli dei campi sono domini di integrità. Per esempio $\mathbb{Z} \subset \mathbb{R}$ e l'anello degli interi di Gauss $\mathbb{Z}[i] \subset \mathbb{C}$ sono domini di integrità.

Per ottenere altri esempi di anelli, consideriamo adesso diversi metodi per costruire nuovi anelli a partire da anelli dati.

8.18 Sottoanelli. Sia R un anello. Un *sottoanello di* R è un sottoinsieme di R il quale è, con la stessa addizione e moltiplicazione di R e con gli stessi elementi neutri 0 e 1, un anello. Per verificare che un sottoinsieme S di un anello R è un sottoanello basta verificare che $0, 1 \in S$, che $(S, +, 0)$ è un sottogruppo di $(R, +, 0)$ e che $a, b \in S$ implica $ab \in S$.

8.19 Esempio. $\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$. Il campo $\mathbb{Q}$ è un sottoanello di $\mathbb{R}$. Abbiamo le seguenti inclusioni di anelli:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}.$$

8.20 Prodotti. Siano R_1 e R_2 due anelli. Il *prodotto* $R_1 \times R_2$ *di* R_1 *per* R_2 è definito da

$$R_1 \times R_2 = \{(r, s) : r \in R_1 \text{ e } s \in R_2\}.$$

Con l'addizione data da $(r, s)+(r', s') = (r+r', s+s')$ e la moltiplicazione data da $(r, s)\cdot(r', s') = (r \cdot r', s \cdot s')$, il prodotto $R_1 \times R_2$ diventa un anello.

Se $R_1, R_2 \neq \{0\}$, il prodotto $R_1 \times R_2$ ha divisori di zero perché si ha

$$(r, 0) \cdot (0, s) = (0, 0) \qquad \text{per ogni } r \in R_1,\ s \in R_2.$$

8.21 Esempio. (*Anelli dei polinomi*) Sia R un anello. Un *polinomio a coefficienti in* R è una "espressione del tipo

$$a_0 + a_1X + a_2X + \ldots + a_nX^n$$

dove $a_0, a_1, a_2, \ldots, a_n \in R$ e la lettera X è soltanto un "simbolo. Gli elementi a_i si dicono *i coefficienti* del polinomio. Equivalentemente, un polinomio è un'espressione

$$\sum_{i=0}^{\infty} a_i X^i$$

dove gli elementi a_i appartengono ad R e sono quasi tutti zero, cioè, esiste $n \in \mathbb{Z}_{\geq 0}$ tale che $a_i = 0$ per ogni $i > n$. Si veda l'Eserc.(9.V) per una definizione più formale dei polinomi.

Per definizione, due polinomi $\sum_{i=0}^{\infty} a_i X^i$ e $\sum_{i=0}^{\infty} b_i X^i$ sono uguali *se e soltanto se* $a_i = b_i$ per ogni $i \geq 0$.

Al posto di X si utilizzano anche altre lettere, come Y, Z, X_0, X_1, etc. Di solito, non si scrivono gli zeri e si scrive X per $1 \cdot X$ e $-aX^i$ per $(-a)X^i$. Spesso si scrive il polinomio in ordine opposto. Per esempio $Y^3 - 2Y + 1$ è il polinomio $1 + (-2) \cdot Y + 0 \cdot Y^2 + 1 \cdot Y^3$.

Il *grado* $\deg(f)$ (inglese: degree) di $f = \sum_{i=0}^{\infty} a_i X^i$ è il più grande indice n tale che $a_n \neq 0$. Per *il polinomio zero* $0 = \sum_{i=0}^{\infty} 0 \cdot X^i$, il grado non è definito. Ogni tanto si trova $\deg(0) = -1$ oppure $\deg(0) = -\infty$. Un polinomio $f = \sum_{i=0}^{\infty} a_i X^i$ di grado n si dice *monico* se $a_n = 1$.

Adesso introduciamo *l'anello* $R[X]$ *dei polinomi a coefficienti in* R:

$$R[X] = \left\{ \sum_{i=0}^{\infty} a_i X^i : a_i \in R \right\}$$

con l'addizione data da

$$\left(\sum_{i=0}^{\infty} a_i X^i \right) + \left(\sum_{i=0}^{\infty} b_i X^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

e la moltiplicazione implicata dalle regole della distributività e da

$$(a_i X^i) \cdot (b_j X^j) = a_i b_j X^{i+j},$$

cioè

$$\left(\sum_{i=0}^{\infty} a_i X^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i \right) = \sum_{k=0}^{\infty} \Big(\sum_{\substack{i,j \\ i+j=k}} a_i b_j \Big) X^k.$$

Questa è la moltiplicazione di polinomi usuale; per esempio:

$$\begin{aligned} (5 - 3X^2) \cdot (3 + 4X + X^3) &= 5 \cdot (3 + 4X + X^3) - 3X^2 \cdot (3 + 4X + X^3) \\ &= 15 + 20X + 5X^3 - 9X^2 - 12X^3 - 3X^5 \\ &= 15 + 20X - 9X^2 - 7X^3 - 3X^5. \end{aligned}$$

Il polinomio $0 = \sum_{i=0}^{\infty} 0 \cdot X^i$ è l'elemento neutro per l'addizione e il polinomio $1 = 1 + 0 \cdot X + 0 \cdot X^2 + \ldots$ è l'identità di $R[X]$. Lasciamo al lettore la verifica che $R[X]$ è un anello.

L'anello $R[X]$ è commutativo se e soltanto se R è commutativo. Si considera R come il sottoanello dei polinomi *costanti* di $R[X]$: per $\alpha \in R$ si ha

$$\alpha = \alpha + 0 \cdot X + 0 \cdot X^2 + \ldots \in R[X].$$

Se R è un dominio, anche $R[X]$ lo è (si veda l'Eserc.(8.P)). In questo caso il grado ha la seguente proprietà:

$$\deg(fg) = \deg(f) + \deg(g) \qquad \text{per ogni } f, g \in R[X] - \{0\}.$$

Induttivamente, si definisce *l'anello dei polinomi in n variabili su R*:

$$R[X_1, X_2, \ldots, X_n] = (R[X_1, X_2, \ldots, X_{n-1}])[X_n].$$

Gli elementi di $R[X_1, X_2, \ldots, X_n]$ sono somme finite del tipo

$$\sum_{i_1=0}^{\infty} \sum_{i_2=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} a_{i_1 i_2 \ldots i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}.$$

8.22 Esempio. (*Campi quozienti).* Sia R un dominio. A partire da R costruiamo un campo $Q(R)$, detto il *campo quoziente di R.* Esso contiene R ed "è generato da R nel senso che ogni $x \in Q(R)$ ha la forma xy^{-1} ,per certi $x, y \in R$.

Sia

$$\Omega = \{(a, r) \in R \times R : \ r \neq 0\}.$$

Innanzitutto, sull'insieme Ω definiamo una relazione *di equivalenza* mediante

$$(a, r) \sim (b, s) \quad \text{se e soltanto se} \quad as = br.$$

Verifichiamo che si tratta di una relazione di equivalenza: è facile vedere che $(a, r) \sim (a, r)$ e che $(a, r) \sim (b, s)$ se e soltanto se $(b, s) \sim (a, r)$. La relazione è dunque riflessiva e simmetrica. Per controllare la transitività utilizziamo la commutatività della moltiplicazione del dominio R: siano $(a, r) \sim (b, s)$ e $(b, s) \sim (c, t)$. Allora

$$ats = ast = brt = rbt = rcs = crs$$

e quindi $(at - cr)s = 0$. Siccome $s \neq 0$ ed R è un dominio, troviamo $at = cr$, cioè $(a, r) \sim (c, t)$.

Definiamo adesso $Q(R)$ come l'insieme delle classi di equivalenza della relazione $\sim$ su Ω. Scriveremo $\frac{a}{r}$ per la classe di (a, r). Con questa notazione abbiamo

$$\frac{a}{r} = \frac{b}{s} \quad \text{se e soltanto se} \quad as = br.$$

Definiamo l'addizione e la moltiplicazione su $Q(R)$ mediante

$$\frac{a}{r} + \frac{b}{s} = \frac{as + br}{rs}, \qquad \frac{a}{r} \cdot \frac{b}{s} = \frac{ab}{rs}.$$

Si noti che $rs \neq 0$ perché $r, s \neq 0$ ed R è un dominio.

Siccome l'addizione e la moltiplicazione sono definite in termini di rappresentanti delle classi di equivalenza, è necessario controllare che sono ben definite, cioè che la somma ed il prodotto non dipendono della scelta dei rappresentanti: supponiamo

$$\frac{a}{r} = \frac{a'}{r'} \quad \text{e} \quad \frac{b}{s} = \frac{b'}{s'},$$

cioè $ar' = a'r$ e $bs' = b's$. Abbiamo

$$\begin{aligned}(a's' + b'r')rs &= a's'rs + b'r'rs = (a'r)s's + (b's)r'r \\ &= ar's's + bs'r'r = (as + br)r's'\end{aligned}$$

e quindi, per definizione,

$$\frac{a's' + b'r'}{r's'} = \frac{as + br}{rs}.$$

Dunque l'addizione è ben definita. Similmente si controlla che la moltiplicazione è ben definita.

Lasciamo al lettore la verifica che, con questa addizione e moltiplicazione, $Q(R)$ è un *campo*. Per esempio, se $a \neq 0$, l'inverso moltiplicativo di $\frac{a}{r}$ è $\frac{r}{a}$. Consideriamo R come sottoanello di $Q(R)$ identificando $a \in R$ con $\frac{a}{1}$.

Per l'anello $R = \mathbb{Z}$ si trova un campo isomorfo al campo $\mathbb{Q}$ dei numeri razionali. Se K è un campo e $R = K[X]$ l'anello dei polinomi con coefficienti in K, allora R è un dominio. Scriviamo $K(X)$ per il campo quoziente di R. Questo campo si dice *il campo delle funzioni razionali in una variabile su* K. Gli elementi di $K(X)$ hanno la forma

$$\frac{f(X)}{g(X)} \qquad \text{dove } f(X), g(X) \in K[X].$$

8.23 Esempio. (*Endomorfismi).* Sia A un gruppo *additivo* e sia $\mathrm{End}(A)$ l'insieme degli endomorfismi di A (si veda il paragrafo 3). Per $f, g \in \mathrm{End}(A)$ definiamo la somma $f + g$ ed il prodotto fg:

$$(f+g)(a) = f(a) + g(a) \qquad \text{per ogni } a \in A, \qquad (fg)(a) = f(g(a)) \qquad \text{per ogni } a \in A.$$

Lasciamo al lettore la facile verifica che con quest'addizione e moltiplicazione $\mathrm{End}(A)$ diventa un anello; ossia *l'anello degli endomorfismi di* A. L'identità di $\mathrm{End}(A)$ è l'applicazione identica Id_A.

Per esempio, se $A = \mathbb{R}^n$, ogni matrice $n \times n$ definisce un endomorfismo di A. Lasciamo al lettore la dimostrazione che $\mathrm{End}(\mathbb{Z}) = \mathbb{Z}$ ed è generato dall'identità $\mathrm{Id}_{\mathbb{Z}}$. Similmente si ha, per ogni intero positivo n che $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ è isomorfo a $\mathbb{Z}/n\mathbb{Z}$, generato dall'applicazione identica.

8.24 Esempio. (*Funzioni.*) Sia X un insieme e sia R un anello. L'insieme R^X delle funzioni $X \longrightarrow R$ è un anello con le seguenti addizione e moltiplicazione: per $f, g : X \longrightarrow R$ definiamo

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x),$$

dove l'addizione e la moltiplicazione a destra sono quelle di R.

Si ottengono esempi importanti di anelli se si considerano funzioni che hanno particolari proprietà. Per esempio, sia X l'intervallo $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ e sia

$$C([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : \ f \text{ è continua}\}.$$

Lasciamo al lettore la verifica che $C([0,1])$ è un sottoanello di $\mathbb{R}^{[0,1]}$. Altri esempi sono l'anello delle funzioni derivabili

$$C^1([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : \ f \text{ è derivabile}\}.$$

e l'anello delle funzioni C^∞:

$$C^\infty([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : \ f \text{ è } \infty \text{ volte derivabile}\}.$$

Esercizi.

(8.A) Sia R un anello e sia $a \in R$. Dimostrare: se $ab = b$ per ogni $b \in R$ allora $a = 1$.

(8.B) Sia $2\mathbb{Z}$ l'insieme degli interi pari. Far vedere che con l'addizione e la moltiplicazione di $\mathbb{Z}$, l'insieme $2\mathbb{Z}$ soddisfa gli assiomi (R_1), (R_2) ed (R_4), ma non (R_3).

(8.C) Sia R un anello.

(i) Far vedere: per ogni $x \in R$ si ha $0 \cdot x = x \cdot 0 = 0$.

(ii) Sia -1 l'inverso additivo di $1 \in R$. Far vedere $(-1) \cdot (-1) = 1$.

(iii) * Siano $a, b, c, \ldots, z$ ventisei elementi di R. Dimostrare che

$$(x - a)(x - b) \cdots (x - z) = 0.$$

(8.D) Sia R un anello e sia $a \in R$ un'unità. Siano $b, c \in R$. Dimostrare che se $ba = ca$, allora $b = c$. Concludere che a ha un unico inverso moltiplicativo.

(8.E) Sia R un anello. Definiamo una nuova moltiplicazione "$\star$ su R:

$$a \star b = ba.$$

Far vedere che, con l'addizione originale e la moltiplicazione nuova, R è un anello. Questo anello si chiama *l'anello opposto di R.*

(8.F) Sia R un anello e sia

$$Z(R) = \{a \in R : \ ax = xa \text{ per ogni } x \in R\}$$

il *centro* di R. Dimostrare che $Z(R)$ è un sottoanello di R.

(8.G) (*Anello di Boole*) Sia X un isieme e sia $P(X)$ l'insieme dei sottoinsiemi di X. Definiamo per $A, B \in P(X)$

$$A + B = A \Delta B, \qquad \text{(si veda l'Eserc.(2.K))} \qquad A \cdot B = A \cap B.$$

Dimostrare che con quest'addizione e moltiplicazione $P(X)$ diventa un anello commutativo.

(8.H) Sia R un anello con la proprietà $x^3 = x$ per ogni $x \in R$. Dimostrare che $x+x+x+x+x+x = 0$ per ogni $x \in R$. Dare un esempio di un anello R siffatto.

(8.I) (i) Sia R un anello *finito*. Dimostrare che ogni $x \in R$ o è 0, o un divisore di zero oppure un'unità.

(ii) Dimostrare: un dominio di integrità finito è un anello di divisione.

(iii) Dare un esempio di un anello R che contiene un elemento $a \neq 0$, il quale non è un'unità e non è un divisore di zero.

(iv) Dare un esempio di un anello infinito con divisori di zero.

(8.J) Dimostrare che nessun anello R ha un gruppo additivo isomorfo a $\mathbb{Q}/\mathbb{Z}$.

(8.K) (*Il binomio di Newton*) Sia R un anello. Per ogni intero positivo n scriviamo n per l'elemento

$$\underbrace{1+1+\ldots+1}_{n \text{ volte}} \in R.$$

Questo vale in particolare per il coefficiente binomiale $\binom{n}{k}$.

(i) Dimostrare: se R è commutativo, allora

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

per ogni $a, b \in R$ ed ogni intero positivo n.

(ii) Far vedere che se $(*)$ vale per ogni $a, b \in R$ ed ogni intero positivo, allora R è commutativo.

(8.L) Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss. Siano $a, b \in \mathbb{Z}$ e sia $z = a + bi \in \mathbb{Z}[i]$. Far vedere che z è un'unità se e soltanto se $a^2 + b^2 = 1$. Calcolare $\mathbb{Z}[i]^*$.

(8.M) Sia H il sottoinsieme dell'insieme dei quaternioni $\mathbb{H}$ dato da

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

Dimostrare che H è un anello non commutativo. Dimostrare che H non contiene divisori di 0.

(8.N) Sia $m \in \mathbb{Z}$. Supponiamo che $m \in \mathbb{Z}$ non sia un quadrato.

(i) Dimostrare: l'insieme

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : \ a, b \in \mathbb{Z}\}$$

è un sottoanello di $\mathbb{C}$.

(ii) Sia $m = 7$. Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbb{Z}[\sqrt{7}]$. (Sugg. Verificare che $a+b\sqrt{7}$ è un'unità se e soltanto se $(a + b\sqrt{7})(a - b\sqrt{7}) = a^2 - 7b^2$ è uguale a ± 1.)

(iii) * Sia $m = 67$. Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbb{Z}[\alpha]$. (Sugg. Trovare soluzioni $X, Y \in \mathbb{Z}$ della equazione $X^2 - 67Y^2 = \pm 1$. Il più piccolo valore di X ha cinque cifre decimali.)

(8.O) Sia $m \in \mathbb{Z}$. Supponiamo che $m \equiv 1 \bmod 4$ e che m non sia un quadrato. Sia

$$\alpha = \frac{1 + \sqrt{m}}{2} \in \mathbb{C}.$$

(i) Dimostrare: l'insieme

$$\mathbb{Z}[\alpha] = \{a + b\alpha : \ a, b \in \mathbb{Z}\}$$

è un sottoanello di $\mathbb{C}$.

(ii) Fare un "disegno di $\mathbb{Z}[\alpha]$ per $m = -3$.

(iii) Sia $\alpha = \frac{1+\sqrt{13}}{2}$. Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbb{Z}[\alpha]$. (Sugg. Sia $\alpha' = \frac{1-\sqrt{13}}{2}$. Verificare che $a + b\alpha$ è un'unità se e soltanto se $(a + b\alpha)(a + b\alpha') = a^2 + ab - 3b^2$ è uguale a ± 1)

(iv) Sia

$$\alpha = \frac{1 + \sqrt{61}}{2}.$$

Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbb{Z}[\alpha]$. (Sugg. Trovare soluzioni $X, Y \in \mathbb{Z}$ della equazione $X^2 + XY - 15Y^2 = \pm 1$.)

(8.P) Sia R un anello senza divisori di zero.

(i) Dimostrare che neanche $R[X]$ ha divisori di zero.

(ii) Supponiamo che R sia commutativo. Far vedere che l'anello $R[X, Y, Z]$ è un dominio di integrità.

(iii) Siano $f, g \in R[X]$ polinomi non nulli. Far vedere che

$$\deg(f) + \deg(g) = \deg(fg).$$

(8.Q) (i) Sia R un anello senza divisori di zero. Dimostrare che $R[X]^* = R^*$.

(ii) Far vedere che $\overline{1} + \overline{5}X \in (\mathbb{Z}/25\mathbb{Z})[X]$ è un'unità.

(8.R) Siano R_1 e R_2 anelli.

(i) Dimostrare che
$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

(ii) Dimostrare: se $R_1 \times R_2$ è un dominio di integrità, allora uno degli anelli R_1, R_2 è l'anello banale.

(8.S) * (*Teorema di McCoy*) Sia R un anello commutativo e sia $f \in R[X]$, $f \neq 0$. Dimostrare: se f è un divisore di zero di $R[X]$, allora esiste $r \in R$, $r \neq 0$ tale che $rf = 0$. (Sugg. se $gf = 0$, diminuire il grado di g moltiplicando con certi coefficienti di f.)

(8.T) (i) Far vedere che l'anello $C([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : f \text{ è continua}\}$ ha divisori di zero.

(ii) * Far vedere che l'anello $C^\infty([0,1]) = \{f : [0,1] \longrightarrow \mathbb{R} : f \text{ è } \infty \text{ volte derivabile}\}$ ha divisori di zero.

(8.U) Sia A il gruppo additivo di $\mathbb{R}[X]$. Definiamo tre elementi $f, g, h \in \mathrm{End}(A)$:
$$\begin{aligned} f(a_0 + a_1X + \ldots + a_nX^n) &= a_1 + a_2X + \ldots a_nX^{n-1} \\ g(a_0 + a_1X + \ldots + a_nX^n) &= a_0X + a_1X^2 + \ldots a_nX^{n+1} \\ h(a_0 + a_1X + \ldots + a_nX^n) &= a_0 \end{aligned}$$

(i) Verificare che $fg = 1$ e $fh = 0$.

(ii) Dimostrare che f non è un'unità.

(8.V) (*Polinomi di Laurent*) Sia R un anello. Un *polinomio di Laurent* è un'espressione
$$\sum_{i \in \mathbb{Z}} a_i X^i \qquad \text{con } a_i \in R \text{ per ogni } i \in \mathbb{Z}.$$
con $a_i = 0$ per quasi tutti gli indici i.

(i) Con l'addizione e la moltiplicazione ovvie l'insieme dei polinomi di Laurent a coefficienti in R diventa un anello. Si indica l'anello ottenuto con $R[X, \frac{1}{X}]$.

(ii) Dimostrare: se R è un dominio di integrità, allora
$$R[X, \frac{1}{X}]^* = \{uX^i : u \in R^* \text{ e } i \in \mathbb{Z}\}.$$

(8.W) * (*Funzioni aritmetiche.*) Una *funzione aritmetica* è una funzione $f : \mathbb{Z}_{>0} \longrightarrow \mathbb{C}$. La somma di due funzioni aritmetiche f e g è definita da
$$(f + g)(n) = f(n) + g(n) \qquad \text{per ogni } n \in \mathbb{Z}_{>0}$$
ed il cosidetto *prodotto di convoluzione* $f \star g$ è di f e g è definito da
$$(f \star g)(n) = \sum_{d \text{ divide } n \atop d>0} f(d)g(\frac{n}{d}) \qquad \text{per ogni } n \in \mathbb{Z}_{>0}.$$

(i) Far vedere che, con queste addizione e moltiplicazione, l'insieme R delle funzioni aritmetiche è un dominio di integrità.

(ii) Far vedere che l'identità di R è la funzione e data da

$$e(n) = \begin{cases} 1; & \text{se } n = 1, \\ 0. & \text{se } n \neq 1. \end{cases}$$

(iii) Far vedere che $R^* = \{f \in R : \ f(1) \neq 0\}$.

(iv) Sia E la funzione aritmetica data da $E(n) = 1$ per ogni $n \in \mathbb{Z}_{>0}$. Calcolare $E \star E$.

(v) Sia "id la funzione $\mathrm{id}(n) = n$ per ogni $n \in \mathbb{Z}_{>0}$ e sia φ la funzione di Eulero dell'Esempio 2.14. Dimostrare che

$$\varphi = \mathrm{id} \star E^{-1}.$$

9 Omomorfismi ed ideali

In questo paragrafo introduciamo gli omomorfismi di anelli. Le immagini di omomorfismi sono sempre sottoanelli, ma i nuclei sono *ideali*. Studiamo quindi il concetto importante di *ideale* di un anello, introdotto dal matematico tedesco E. E. Kummer nel 1845.

9.1 Definizione. Siano R_1, R_2 due anelli. Un *omomorfismo (di anelli)* da R_1 a R_2 è una mappa

$$f : R_1 \longrightarrow R_2$$

che soddisfa

$$\begin{array}{lll} f(a+b) & = f(a) + f(b) & \text{per ogni } a, b \in R_1, \\ f(ab) & = f(a)f(b) & \text{per ogni } a, b \in R_1, \\ f(1) & = 1. & \end{array}$$

Un omomorfismo biiettivo si dice un *isomorfismo* o anche, se $R_1 = R_2$, un *automorfismo*. L'insieme

$$\ker(f) = \{x \in R_1 : f(x) = 0\}$$

si dice il *nucleo di* f.

9.2 Esempio.

(*i*) Sia n un intero positivo. L'applicazione canonica

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \qquad a \longmapsto a \bmod n$$

è un omomorfismo dall'anello $\mathbb{Z}$ all'anello $\mathbb{Z}/n\mathbb{Z}$.

(*ii*) Sia $\alpha \in \mathbb{R}$. L'applicazione

$$\Phi : \mathbb{R}[X] \longrightarrow \mathbb{R}, \qquad f \longmapsto f(\alpha)$$

è un omomorfismo di anelli. Lasciamo la verifica al lettore. È facile vedere che Φ è un omomorfismo suriettivo. In generale, per ogni anello *commutativo* R ed ogni $\alpha \in R$, l'applicazione $\Phi : R[X] \longrightarrow R$ data da $\Phi(f) = f(\alpha)$ è un omomorfismo. Questo non è più vero per anelli non commutativi. Si veda l'Eserc.(9.H).

(*iii*) Sia R un anello e sia R' un sottoanello di R. Allora l'inclusione $R' \hookrightarrow R$ è un omomorfismo di anelli.

(*iv*) Siano R_1 e R_2 due anelli. La *proiezione*

$$\pi_1 : R_1 \times R_2 \longrightarrow R_1$$

data da $\pi_1(r, s) = r$ è un omomorfismo. Anche l'altra proiezione $\pi_2 : R_1 \times R_2 \longrightarrow R_2$ data da $\pi_2(r, s) = s$ è un omomorfismo.

(*v*) Sia R un anello. L'applicazione $\mathbb{Z} \longrightarrow R$ data da $m \mapsto m$, cioè

$$m \longmapsto \begin{cases} \underbrace{1+1+\cdots+1}_{m \text{ volte}}; & \text{se } m > 0, \\ \underbrace{-1-1-\cdots-1}_{-m \text{ volte}}; & \text{se } m < 0. \\ 0; & \text{se } m = 0, \end{cases}$$

è un omomorfismo. Si controlli che questa applicazione è l'unico omomorfismo da $\mathbb{Z}$ a R.

9.3 Definizione. Sia R un anello. Un sottoinsieme $I \subset R$ si dice un *ideale sinistro di* R se I è un sottogruppo additivo di R con la proprietà

$$ra \in I \qquad \text{per ogni } r \in R \text{ ed ogni } a \in I.$$

Un sottoinsieme $I \subset R$ si dice un *ideale destro di* R se I è un sottogruppo additivo di R con la proprietà

$$ar \in I \qquad \text{per ogni } r \in R \text{ ed ogni } a \in I.$$

Un *ideale (bilaterale)* è un ideale sia sinistro che destro di R.

9.4 Esempi.

(*i*) (*Ideali banali*) Ogni anello R possiede i cosidetti ideali *banali* $\{0\}$ e R.

(*ii*) (*Nuclei*) Sia $f : R_1 \longrightarrow R_2$ un omomorfismo. Allora, il nucleo di f è un ideale di R_1. Infatti, per il Teorema 3.11, il nucleo di f è un sottogruppo additivo di R. Per vedere che $\ker(f)$ è un ideale di R prendiamo $r \in R$ e $x \in I$. Abbiamo $f(rx) = f(r)f(x) = f(r)\cdot 0 = 0$ e dunque $rx \in I$. Similmente si dimostra che $xr \in I$.

Un omomorfismo f di anelli è iniettivo se e soltanto se il nucleo di f è zero. Questo fatto segue dal Teorema 3.11.

(*iii*) (*Ideali principali*) Sia R un anello e sia $x \in R$. L'insieme

$$Rx = \{rx : r \in R\}$$

è un ideale sinistro di R. Similmente $xR = \{xr : r \in R\}$ è un ideale destro di R. Se R è commutativo gli ideali xR e Rx coincidono. Questo ideale si dice *l'ideale generato da* x e si scrive anche (x). Gli ideali di R generati da un elemento solo di R si dicono *ideali principali*.

(*iv*) Sia I un ideale di $\mathbb{Z}$. Questo significa, in particolare, che I è un sottogruppo additivo di $\mathbb{Z}$. Per il Teorema 3.6, ogni sottogruppo di $\mathbb{Z}$ ha la forma $d\mathbb{Z}$. Ogni ideale di $\mathbb{Z}$ è dunque principale. Ogni sottogruppo di $\mathbb{Z}$ è quindi anche un ideale di $\mathbb{Z}$.

(*v*) Sia R un anello commutativo e siano $a_1, a_2, \ldots, a_n$ elementi di R. Scriviamo $a_1R + a_2R + \cdots + a_nR$ oppure $(a_1, a_2, \ldots, a_n)$ per *l'ideale* I *generato da* $a_1, a_2, \ldots, a_n$. L'ideale I è definito da

$$I = \{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in R\}.$$

L'ideale I è il più piccolo ideale di R che contiene gli elementi $a_1, a_2, \ldots, a_n$.

9.5 Esempio. Per esempio consideriamo l'ideale $I = (2, X)$ generato dagli elementi 2 ed X nell'anello $\mathbb{Z}[X]$. L'ideale I non è principale. Per dimostrare questo fatto, supponiamo che $I = (f)$ per un certo polinomio $f \in \mathbb{Z}[X]$. Dunque

$$2 = h \cdot f, \qquad X = g \cdot f,$$

per certi polinomi $h, g \in \mathbb{Z}[X]$. Siccome $\mathbb{Z}$ è un dominio di integrità, il grado deg è additivo: $\deg(f) + \deg(h) = \deg(2) = 0$. Siccome $\deg(f) \geq 0$, abbiamo $\deg(f) = 0$, cioè f è un polinomio costante. Similmente, g è un polinomio di grado 1. Siccome $X = g \cdot f$, abbiamo, per un certo $\alpha \in \mathbb{Z}$, che $g = X + \alpha$ e $f = 1$ oppure $g = -X + \alpha$ e $f = -1$. In ogni caso troviamo che $1 \in I$, il che è impossibile perché I consiste di polinomi $\sum_{k \geq 0} a_k X^k$ con a_0 pari. Concludiamo che $I = (2, X)$ non è un ideale principale.

9.6 Proposizione. Sia R un anello e sia $I \subset R$ un ideale di R. Se I contiene un'unità, allora $I = R$.

Dimostrazione. Sia $a \in R^*$ in I. Allora $1 = a \cdot a^{-1} \in I$ e dunque $x = x \cdot 1 \in I$ per ogni $x \in R$. In altre parole $I = R$, come richiesto. □

9.7 Corollario. Sia R un anello con divisione.

(*i*) I soli ideali di R sono quelli banali.

(*ii*) Sia R' un anello non banale e sia $f : R \longrightarrow R'$ un omomorfismo. Allora f è iniettivo.

Dimostrazione. *(i)* Ogni elemento $x \neq 0$ di R è un unità. L'anello R ha quindi per la Prop.9.6 soltanto i due ideali $\{0\}$ e R.
(ii) Siccome $f(1) = 1$, l'elemento 1 non è contenuto nel nucleo di f. Dunque l'ideale $\ker(f)$ non è uguale a R e per la prima parte abbiamo $\ker(f) = 0$, come richiesto. □

9.8 Somme, prodotti e intersezioni di ideali. Sia R un anello e siano I, J ideali bilaterali di R. È facile vedere che l'intersezione $I \cap J$ è un ideale di R. L'ideale $I \cap J$ è il più grande ideale contenuto in sia I che J. L'unione di I e J non è, in generale, un ideale.

La *somma* $I + J$ *di* I *e* J è definita da

$$I + J = \{x + y : x \in I \text{ ed } y \in J\}.$$

Lasciamo al lettore la verifica che si tratta di un ideale. Ovviamente $I + J$ contiene gli ideali I e J. D'altra parte, ogni ideale che contiene I e J contiene anche la somma $I + J$. Dunque, $I + J$ è il più piccolo ideale di R che contiene sia I che J. Si dice che I e J sono *coprimi* oppure che *non hanno divisori comuni,* se $I + J = R$.

Il *prodotto* IJ *di* I *e* J è definito da

$$IJ = \left\{ \sum_{k=1}^{m} x_k y_k : \ m \in \mathbb{Z}_{>0}, \quad x_k \in I, \ y_k \in J \right\}.$$

Lasciamo al lettore la verifica che IJ è un ideale di R. In generale, l'insieme $\{xy : x \in I, y \in J\}$ non è un ideale; si veda l'Eserc.(9.R). L'ideale IJ è contenuto in sia I che J e quindi $IJ \subset I \cap J$. Abbiamo il seguente diagramma di ideali di R:

$$\begin{array}{ccccc} & & & & I & & & & \\ & & & \subset & & \subset & & & \\ IJ & \subset & I \cap J & & & & I + J & \subset & R \\ & & & \subset & & \subset & & & \\ & & & & J & & & & \end{array}$$

9.9 Esempio. Adesso vediamo che significato hanno questi ideali nel caso $R = \mathbb{Z}$. Siano I, J due ideali di $\mathbb{Z}$. Siccome ogni ideale di $\mathbb{Z}$ è principale, possiamo scrivere $I = n\mathbb{Z}$ e $J = m\mathbb{Z}$ per certi interi n, m.

L'intersezione $n\mathbb{Z} \cap m\mathbb{Z}$ consiste degli interi a che sono divisibili sia per n che per m. Dunque il *minimo comune multiplo* $\text{mcm}(n, m)$ di n ed m è contenuto nella intersezione $n\mathbb{Z} \cap m\mathbb{Z}$. D'altra parte, per l'Eserc.(1.G), ogni multiplo comune di n ed m è divisibile per $\text{mcm}(n, m)$. Concludiamo che

$$n\mathbb{Z} \cap m\mathbb{Z} = \text{mcm}(n, m)\mathbb{Z}.$$

La somma $n\mathbb{Z} + m\mathbb{Z}$ è, per definizione, uguale all'insieme $\{an + bm : a, b \in \mathbb{Z}\}$. Per il Teorema 1.7 esso contiene $\text{mcd}(n, m)$. È banale che ogni numero della forma $an + bm$ è divisibile per $\text{mcd}(n, m)$. Concludiamo che

$$n\mathbb{Z} + m\mathbb{Z} = \text{mcd}(n, m)\mathbb{Z}.$$

In particolare, $\mathrm{mcd}(n,m) = 1$ se e soltanto se $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. Questo spiega perché si dice che due ideali I, J di un anello arbitrario R, sono coprimi, oppure non hanno divisori comuni, quando $I + J = R$.

Per l'Eserc. (9.Q) il prodotto di $n\mathbb{Z}$ e $m\mathbb{Z}$ è dato da

$$(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z}.$$

9.10 Definizione. (*Anelli quoziente*). Sia R un anello e sia I un ideale di R. Se consideriamo soltanto la struttura *additiva,* vediamo che R è un gruppo abeliano e I un sottogruppo normale di R. Dunque, per la costruzione del paragafo 6, è definito il quoziente R/I. Come solito, scriviamo $\overline{x}$ per la classe laterale $x + I$ dell'elemento $x \in R$. Si ha $\overline{x} = \overline{y}$ se e soltanto se $x - y \in I$.

Per due elementi $\overline{x}, \overline{y} \in R/I$ definiamo

$$\overline{x} \cdot \overline{y} = \overline{xy}.$$

Con questa moltiplicazione R/I diventa un anello, *l'anello quoziente di R per I*. Verifichiamo prima che la moltiplicazione è ben definita. Prendiamo x, $x' \in R$ e y, $y' \in R$ tali che $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$. Dunque

$$x' = x + a \qquad \text{e} \qquad y' = y + b \qquad \text{per certe } a,\ b \in I$$

e, per la distributività di R,

$$x'y' = xy + xb + ay + ab.$$

Siccome I è un ideale, gli elementi xb, ay e ab sono tutti in I. Concludiamo che

$$\overline{x'y'} = \overline{xy}$$

e quindi la moltiplicazione è ben definita.

È molto facile verificare gli assiomi di anello per R/I: abbiamo già detto che vale (R_1). L'assioma (R_2) vale perché

$$(\overline{x}\,\overline{y})\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,\overline{yz} = \overline{x}(\overline{y}\,\overline{z})$$

per ogni $\overline{x}, \overline{y}, \overline{z} \in R/I$.

L'elemento $\overline{1}$ è l'identità dell'anello R/I e la distributività vale. Dunque, valgono anche gli assiomi (R_3) e (R_4).

9.11 Proposizione. Sia I un ideale di un anello R. L'omomorfismo canonico

$$\pi : R \longrightarrow R/I, \qquad x \longmapsto \overline{x}$$

è un omomorfismo suriettivo. Il nucleo di π è I.

Dimostrazione. Siccome $\pi(x) = \overline{x}$, la mappa π è suriettiva. Abbiamo $x \in \ker(\pi)$ se e soltanto se $\pi(x) = \overline{x} = \overline{0}$. Questo è equivalente a $x \in I$, come richiesto. □

9.12 Teorema. (Teorema di omomorfismo.) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli. Sia I un ideale di R e supponiamo che $I \subset \ker(f)$. Allora esiste un unico omomorfismo $h : R/I \longrightarrow R'$ tale che $h \circ \pi = f$, cioè tale da rendere commutativo il seguente diagramma.

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

Dimostrazione. Definiamo $h : R/I \longrightarrow R'$ mediante $h(\overline{x}) = f(x)$. La mappa h è ben definita perché se $\overline{x} = \overline{y}$, allora $y = x + a$ dove $a \in I$. Abbiamo dunque $f(y) = f(x+a) = f(x) + f(a) = f(x)$, perché $a \in I \subset \ker(f)$, e quindi $h(\overline{y}) = h(\overline{x})$.

Per costruzione la mappa h soddisfa $h(\pi(x)) = f(x)$. Lasciamo al lettore la verifica che h è un omomorfismo e che h è l'unico omomorfismo con questa proprietà. □

9.13 Esempio. Sia $R = \mathbb{R}[X, Y]$ e sia $(a, b) \in \mathbb{R}^2$. È facile verificare che la mappa

$$f : R = \mathbb{R}[X, Y] \longrightarrow \mathbb{R}, \qquad p \longmapsto p(a, b)$$

è un omomorfismo, detto omomorfismo di valutazione nel punto (a, b). Consideriamo l'ideale principale $I = (X^2 + Y^2 - 1) \subset \mathbb{R}[X, Y]$. Allora $I \subset \ker(f)$ se e solo se $a^2 + b^2 - 1 = 0$, cioè il punto (a, b) soddisfa l'equazione $X^2 + Y^2 - 1 = 0$. In questo caso dal Teorema 9.12 otteniamo un omomorfismo

$$h : R/I = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \longrightarrow \mathbb{R}, \qquad \overline{p} \longmapsto p(a, b).$$

Si noti che l'uguaglianza $\overline{X^2 + Y^2 - 1} = \overline{0} \in R/I$ e l'esistenza di un tale omomorfismo h implica che $h(\overline{X^2 + Y^2 - 1}) = h(\overline{0})$ cioè $a^2 + b^2 - 1 = 0$, quindi la condizione $a^2 + b^2 - 1 = 0$ è essenziale per l'esistenza di h.

9.14 Teorema. (Primo Teorema di Isomorfismo.) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli. Allora f induce un isomorfismo

$$R/\ker(f) \xrightarrow{\cong} f(R), \qquad \overline{x} \longmapsto f(x).$$

Dimostrazione. Consideriamo l'omomomorfismo

$$f : R \longrightarrow f(R).$$

Applicando il Teorema 9.12 con $I = \ker(f)$ troviamo che esiste unico un omomorfismo

$$h : R/\ker(f) \longrightarrow f(R)$$

con $h(\overline{x}) = f(x)$. Verifichiamo che si tratta di un isomorfismo: se $\overline{x} \in \ker(h)$, allora $h(\overline{x}) = f(x) = 0$. Quindi $x \in \ker(f)$, cioè $\overline{x} = \overline{0}$. Dunque, h è iniettivo. Sia $y = f(x)$ un elemento arbitrario di $f(R)$. Allora $h(\overline{x}) = f(x) = y$ e vediamo che h è una suriezione, quindi h è un isomorfismo come richiesto. □

9.15 I Teoremi 9.12 e 9.14 sono molto simili ai corrispondenti Teoremi 7.1 e 7.4 per i gruppi. Per il corrispondente del secondo Teorema di isomorfismo si veda l'Eserc. (9.L). Il prossimo Teorema è l'analogo del Teorema 7.10.

9.16 Teorema. (Terzo Teorema di Isomorfismo.) Sia R un anello e sia I un ideale di R.

(*i*) Ogni ideale dell'anello R/I é immagine di un ideale J di R. In altre parole, ogni ideale di R/I ha la forma J/I dove J è un ideale di R che contiene I.

(*ii*) Sia J un ideale di R che contiene I. Allora J/I è un ideale di R/I e

$$(R/I)/(J/I) \cong R/J.$$

Dimostrazione. La dimostrazione è simile a quella del Teorema 7.10 e la lasciamo al lettore. □

9.17 Esempio. Il Teorema 9.16 è commodo per capire $R/(a,b)$. Se prendiamo $I = (a)$, che è contenuto in $J = (a,b)$, troviamo:

$$R/(a,b) \cong (R/(a))/(\overline{b})$$

perchè J/I, l'immagine di J in R/I, è ovviamente generato da $\overline{b}$ in $R/(a)$.

9.18 Esempi.

(*i*) Sia R un anello e sia $\Phi : R[X] \longrightarrow R$ la mappa data da $\Phi(f) = f(0)$. Cioè $\Phi(a_0 + a_1X + \ldots + a_nX^n) = a_0$. È facile vedere che Φ è un omomorfismo suriettivo. Il nucleo di Φ consiste dei polinomi $a_0 + a_1X + \ldots + a_nX^n$ con $a_0 = 0$. Questi sono precisamente i polinomi divisibili per X. Dunque $\ker(\Phi) = XR[X]$. Il Teorema 9.14 implica adesso

$$R[X]/XR[X] \cong R.$$

(*ii*) Sia R un anello commutativo e sia $a \in R$. Consideriamo la mappa $\Psi : R[X] \longrightarrow (R/aR)[X]$ data da

$$\Psi(a_0 + a_1X + \ldots + a_nX^n) = \overline{a_0} + \overline{a_1}X + \ldots + \overline{a_n}X^n$$

dove per $b \in R$, si indica con $\overline{b}$ la classe di b modulo l'ideale aR. Lasciamo al lettore la verifica che Ψ è un omomorfismo suriettivo.

Sia $f(X) = a_0 + a_1X + \ldots + a_nX^n$ nel nucleo di Ψ. Allora tutti i coefficienti di f sono congruenti a 0 modulo aR, cioè sono divisibili per a. Scriviamo $a_i = ab_i$ con $b_i \in R$. Allora

$$f(X) = ab_0 + ab_1X + \ldots + ab_nX^n = a(b_0 + b_1X + \ldots + b_nX^n).$$

Concludiamo che $\ker(\Psi) = aR[X]$. Per il primo Teorema di isomorfismo abbiamo adesso

$$R[X]/aR[X] \cong (R/aR)[X].$$

(*iii*) Sia $J = (2, X) \subset \mathbb{Z}[X]$ l'ideale generato da 2 e X. Calcoliamo l'anello quoziente $\mathbb{Z}[X]/(2, X)$ utilizzando il terzo Teorema di isomorfismo e l'Esempio 9.17. Per un metodo che utilizza invece il primo Teorema di isomorfismo si veda l'Eserc. (9.N).

Sia I l'ideale generato da 2 in $\mathbb{Z}[X]$. Per il Teorema 9.16 abbiamo

$$\mathbb{Z}[X]/(2, X) \cong (\mathbb{Z}[X]/2\mathbb{Z}[X])/((2, X)/(2\mathbb{Z}[X]).$$

Per il secondo esempio abbiamo $\mathbb{Z}[X]/2\mathbb{Z}[X] \cong (\mathbb{Z}/2\mathbb{Z})[X]$ e l'immagine dell'ideale $(2, X)$ in questo anello è semplicemente l'ideale $(2, X)$ in $(\mathbb{Z}/2\mathbb{Z})[X]$, cioè l'ideale (X). Troviamo dunque

$$(\mathbb{Z}[X]/2\mathbb{Z}[X])/((2, X)/(2\mathbb{Z}[X]) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X).$$

Per il primo esempio, l'anello $(\mathbb{Z}/2\mathbb{Z})[X]/(X)$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

9.19 Si veda il paragrafo 10 per altri metodi per fare calcoli in anelli di polinomi.
Adesso dimostriamo una generalizzazione del Teorema 3.16.

9.20 Teorema. (Teorema Cinese del resto.) Sia R un anello commutativo e siano I ed J due ideali coprimi: $I + J = R$. Allora

(*i*) Si ha $IJ = I \cap J$.

(*ii*) C'è un isomorfismo di anelli

$$R/(IJ) \cong (R/I) \times (R/J).$$

Dimostrazione. *(i)* Si ha sempre $IJ \subset I \cap J$. Siccome $I + J = R$, esistono $x \in I$ ed $y \in J$ tali che $x + y = 1$. Prendiamo adesso $z \in I \cap J$; allora $z = z \cdot 1 = zx + zy$. Questo dimostra che $z \in IJ$.
(ii) Definiamo

$$\Psi : R \longrightarrow (R/I) \times (R/J)$$

mediante $\Psi(x) = (x \bmod I, x \bmod J)$. È facile vedere che Ψ è un omomorfismo. Ovviamente il nucleo di Ψ è l'ideale $I \cap J$. Per la parte *(i)* abbiamo anche $\ker(\Psi) = IJ$.

Siano $a, b \in R$ e sia $(a \bmod I, b \bmod J)$. Consideriamo l'elemento $z = ay + bx \in R$ dove, come sopra, $x \in I$, $y \in J$ e $x + y = 1$. Allora

$$z = ay + bx \equiv ay = a(1 - x) = a - ax \equiv a \bmod I,$$
$$z = ay + bx \equiv bx = b(1 - y) = b - by \equiv b \bmod J.$$

Quindi $\Psi(z) = (a \bmod I, b \bmod J)$. Questo dimostra che Ψ è un omomorfismo suriettivo. Il teorema segue adesso dal primo Teorema di isomorfismo. □

9.21 Corollario. Siano n, m due interi coprimi, cioè tali che $\mathrm{mcd}(n, m) = 1$.

(*i*) C'è un isomorfismo di anelli

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

(*ii*) C'è un isomorfismo di gruppi

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

(*iii*) Per interi positivi e coprimi n e m si ha

$$\varphi(nm) = \varphi(n)\varphi(m),$$

dove φ è la funzione di Eulero (si veda l'Esempio 2.14).

Dimostrazione. *(i)* Questo segue dal Teorema 9.20 e dal fatto che gli ideali $I = n\mathbb{Z}$ e $J = n\mathbb{Z}$ sono coprimi se e soltanto se $\mathrm{mcd}(n, m) = 1$.
(ii) Per l'Eserc.(8.R), il gruppo delle unità di un prodotto di anelli è isomorfo al prodotto dei gruppi delle unità dei fattori. Dunque, la parte *(ii)* segue da *(i)*.
(iii) Questo segue dalla parte *(ii)*, perché $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$. □

9.22 Corollario. Sia n un intero positivo. Allora la funzione di Eulero è data da:

$$\varphi(n) = n \prod_{p \text{ divide } n} \left(1 - \frac{1}{p}\right)$$

dove p varia tra i numeri primi che dividono n.

Dimostrazione. Consideriamo prima il caso $n = p^a$ con p un numero primo e $a \in \mathbb{Z}_{>0}$. Abbiamo

$$\begin{aligned} \varphi(p^a) &= \#(\mathbb{Z}/p^a\mathbb{Z})^* \\ &= \#\{x \in \mathbb{Z} : 1 \le x \le p^a,\ \mathrm{mcd}(x, p^a) = 1\} \\ &= p^a - \#\{x \in \mathbb{Z} : 1 \le x \le p^a,\ \mathrm{mcd}(x, p^a) > 1\} \end{aligned}$$

Siccome $\mathrm{mcd}(x, p^a) > 1$ se e soltanto se p divide x, basta determinare i numeri x divisibili per p con $1 \leq x \leq p^a$. Questi sono esattamente i numeri yp con $1 \leq y \leq p^{a-1}$. Ce ne sono p^{a-1}. Troviamo dunque

$$\varphi(p^a) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right).$$

In generale, scriviamo $n = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$ ove i p_i sono numeri primi distinti. Per il Cor 9.21(*iii*) abbiamo

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \dots \varphi(p_t^{a_t})$$

e quindi

$$\varphi(n) = p_1^{a_1} \left(1 - \frac{1}{p_1}\right) p_2^{a_2} \left(1 - \frac{1}{p_2}\right) \dots p_t^{a_t} \left(1 - \frac{1}{p_t}\right)$$

come richiesto.

Esercizi.

(9.A) Sia $f : R_1 \longrightarrow R_2$ un omomorfismo. Far vedere che l'immagine di f è un sottoanello di R_2.

(9.B) Sia R un anello. Far vedere che esiste unico un omomorfismo di anelli $\mathbb{Z} \longrightarrow R$. Far vedere che esiste unico un omomorfismo di anelli $R \longrightarrow \{0\}$.

(9.C) (i) Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ un omomorfismo di anelli. Far vedere che f è l'applicazione identica.

(ii) Sia $f : \mathbb{R} \longrightarrow \mathbb{R}$ un omomorfismo. Far vedere che $f(x) > 0$ se $x > 0$.

(iii) Sia $f : \mathbb{R} \longrightarrow \mathbb{R}$ un omomorfismo. Far vedere che f è l'applicazione identica.

(9.D) Far vedere che esiste un omomorfismo di anelli $f : \mathbb{C} \longrightarrow \mathbb{C}$ distinto dall'applicazione identica.

(9.E) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli.

(i) Dimostrare che f manda R^* in R'^* e l'applicazione $f^* : R^* \longrightarrow R'^*$, data da $f^*(\varepsilon) = f(\varepsilon)$, è un omomorfismo di gruppi.

(ii) Far vedere: f^* è iniettivo se f è iniettivo.

(iii) È vero che f^* è suriettivo se f è suriettivo?

(9.F) Siano R_1 ed R_2 due anelli.

(i) Siano $I_1 \subset R_1$ e $I_2 \subset R_2$ ideali. Far vedere che $I_1 \times I_2$ è un ideale di $R_1 \times R_2$.

(ii) Dimostrare che ogni ideale $I \subset R_1 \times R_2$ ha la forma $I = I_1 \times I_2$ dove $I_1 \subset R_1$ e $I_2 \subset R_2$ sono ideali.

(9.G) Sia R un anello e siano $I, J \subset R$ due ideali di R. Far vedere: $I \cup J$ è un ideale se e soltanto se $I \subset J$ o $J \subset I$.

(9.H) Sia R un anello. Sia $F_\alpha : R[X] \longrightarrow R$ l'applicazione data da $f \mapsto f(\alpha)$.

(i) Far vedere che F_α è un omomorfismo di anelli se α è contenuto nel centro di R. (Si veda l'Eserc.(8.F)).

(ii) Dimostrare: la mappa F_α è un omomorfismo per ogni $\alpha \in R$ se e soltanto se R è commutativo.

(iii) Sia $F : R[X] \to R$ un omomorfismo tale che $F(r) = r$ per ogni $r \in R$. Mostrare che $F = F_\alpha$ per un certo α nel centro di R.

(9.I) Sia R un anello. Far vedere che

$$I = \left\{ \sum_{k=0}^{\infty} a_k X^k \in R[X] : \, a_0 = a_1 = a_2 = 0 \right\}$$

è un ideale di $R[X]$ e che $I = (X^3)$.

(9.J) Sia A un gruppo abeliano. Far vedere che

$$\{f \in \mathrm{End}(A) : \, f(a) = 0 \text{ se } a \in A \text{ ha ordine finito}\}$$

è un ideale di $\mathrm{End}(A)$.

(9.K) Sia R un anello e sia $I = R - R^*$. Supponiamo che per ogni $x \in I$ esista un intero positivo tale che $x^n = 0$. Far vedere che I è un ideale di R. Far vedere che R/I è un anello con divisione.

(9.L) Sia R un anello, sia R' un sottoanello di R e si I un ideale di R.

(i) Far vedere che $R' \cap I$ è un ideale di R'.

(ii) Far vedere che $R' + I = \{r + x : \, r \in R' \text{ e } x \in I\}$ è un sottoanello di R.

(iii) Dimostrare che

$$R'/(R' \cap I) \cong (R' + I)/I.$$

(9.M) Far vedere che l'ideale (X, Y) nell'anello $\mathbb{Q}[X, Y]$ non è principale.

(9.N) (i) Far vedere che la mappa $\Psi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}$ data da $f \mapsto f(0) \bmod 2$ è un omomorfismo suriettivo.

(ii) Far vedere che $\ker(\Psi)$ è l'ideale $(2, X)$.

(iii) Dimostrare che

$$\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}.$$

(9.O) Sia R un anello e supponiamo che l'applicazione $f : R \longrightarrow R$ data da $f(x) = x^2$ sia un omomorfismo di anelli.

(i) Far vedere che R è un anello commutativo.

(ii) Far vedere che per ogni $x \in R$ si ha $x + x = 0$.

(iii) Dimostrare: se $x \in \ker(f)$, allora $1 + x \in R^*$.

(9.P) Sia n un intero senza fattori quadrati e sia R un anello con $\#R = n$. Dimostrare che R è isomorfo all'anello $\mathbb{Z}/n\mathbb{Z}$.

(9.Q) Sia R un anello commutativo.

(i) Far vedere che $(aR) \cdot (bR) = abR$ per $a, b \in R$.

(ii) Siano $a, b \in R$. Dimostrare: se R è un dominio e aR=bR, allora $a = \varepsilon b$ per un $\varepsilon \in R^*$.

(9.R) Sia $R = \mathbb{Z}[X]/(5X, X^2)$.

(i) Far vedere che per ogni elemento $f \in R$ esistono unici due elementi $a \in \mathbb{Z}$, $b \in \mathbb{Z}/5\mathbb{Z}$ tali che

$$f = a + bX \bmod (5X, X^2).$$

(ii) Dimostrare che $f = a + bX \in R^*$ se e soltanto se $a = \pm 1$. Determinare la struttura di R^* come gruppo abeliano.

(iii) Siano $\alpha = X$ e $\beta = 2X$. Far vedere che gli ideali (X) e $(2X)$ sono uguali, ma non esiste $\varepsilon \in R^*$ tale che $\alpha = \varepsilon\beta$.

(9.S) (i) Sia R un anello commutativo. Siano $I, J \subset R$ ideali. Supponiamo che almeno uno di I, J sia principale. Far vedere che

$$IJ = \{xy : x \in I,\ y \in J\}.$$

(ii) Sia $R = \mathbb{Z}[X]$ e sia I l'ideale $(2, X)$. Far vedere che $X^2 + 4 \in I \cdot I$, ma che non si può scrivere $X^2 + 4$ come xy con $x, y \in I$. Concludere che $\{xy : x, y \in I\}$ non è un ideale di R.

(9.T) Sia R un anello. Definiamo

$$[R, R] = \left\{ \sum_{I=1}^{n} r_i(x_i y_i - y_i x_i) : n \in \mathbb{Z}_{>0},\ r_i, x_i, y_i \in R \right\}.$$

(i) Dimostrare che $[R, R]$ è un ideale di R e che $R/[R, R]$ è un anello commutativo.

(ii) Dimostrare: se R' è un anello commutativo, e se $f : R \longrightarrow R'$ è un omomorfismo, allora esiste unico un omomorfismo $h : R/[R, R] \longrightarrow R'$ con $h(\overline{x}) = f(x)$.

(9.U) (*Numeri duali.*) Sia R un anello commutativo. *L'anello $R[\varepsilon]$ dei numeri duali su R* consiste delle espressioni $a + b\varepsilon$ con $a, b \in R$. L'addizione e moltiplicazione sono definite da

$$\begin{aligned}(a + b\varepsilon) + (c + d\varepsilon) &= (a + c) + (b + d)\varepsilon,\\ (a + b\varepsilon) \cdot (c + d\varepsilon) &= (ac) + (ad + bc)\varepsilon.\end{aligned}$$

(i) Far vedere che $\varepsilon^2 = 0$. Questa formula e le leggi della distributività implicano la formula generale per la moltiplicazione data sopra.

(ii) Dimostrare $R[\varepsilon] \cong R[X]/(X^2)$.

(iii) Se R è un campo, allora l'anello $R[\varepsilon]$ ha esattamente tre ideali distinti.

(iv) Sia R un campo. Far vedere che c'è un isomorfismo di gruppi

$$R[\varepsilon]^* \cong R^* \times R.$$

(9.V) (*Polinomi "ufficiali*) In questo esercizio diamo una definizione dell'anello dei polinomi su un anello R senza introdurre un "simbolo X. Sia R un anello. Sia Ω l'insieme delle successioni di elementi in R dato da

$$\Omega = \{(a_0, a_1, a_2, \ldots) : \ a_i \in R \text{ per ogni } i \in \mathbb{Z}_{\geq 0} \text{ e } a_i = 0 \text{ per quasi tutti i valori di } i\}$$

Per $x = (a_0, a_1, a_2, \ldots)$ e $y = (b_0, b_1, b_2, \ldots)$ definiamo

$$x + y = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots), \qquad x \cdot y = (a_0b_0, a_1b_0 + a_0b_1, a_2b_0 + a_1b_1 + a_0b_2, \ldots).$$

(i) Dimostrare che con quest'addizione e moltiplicazione Ω è un anello.

(ii) Far vedere che la mappa $F : \Omega \longrightarrow R[X]$ data da

$$F((a_0, a_1, a_2, \ldots)) = a_0 + a_1X + a_2X^2 + \ldots$$

è un isomorfismo di anelli.

(9.W) * (*Idempotenti.*) Sia R un anello. Un *idempotente* di R è un elemento $e \in R$ con $e^2 = e$. Per esempio, in ogni anello ci sono gli idempotenti "banali 0 ed 1. In questo esercizio vedremo che per un anello commutativo R, gli idempotenti corrispondono ai modi diversi di scrivere R come prodotto $R_1 \times R_2$ di due anelli R_1 e R_2.

(i) Calcolare gli idempotenti di $\mathbb{Z}/6\mathbb{Z}$.

(ii) Dimostrare: se e è un idempotente anche $1 - e$ lo è.

(iii) Dimostrare: se R è il prodotto di due anelli non banali R_1 e R_2, allora $e_1 = (1, 0)$ e $e_2 = (0, 1)$ sono idempotenti non banali. Far vedere che $e_2 = 1 - e_1$.

(iv) Sia e un idempotente di R. Far vedere che l'applicazione

$$R \longrightarrow R/eR \times R/(1 - e)R$$

data da $x \mapsto (x \bmod eR, x \bmod (1 - e)R)$ è un isomorfismo di anelli.

(9.X) Sia φ la funzione di Eulero.

(i) Calcolare $\varphi(1991), \varphi(1992), \varphi(1993)$.

(ii) Determinare tutti gli interi n tali che $\varphi(n) = 8$.

(iii) Far vedere che non esiste $n \in \mathbb{Z}_{>0}$ con $\varphi(n) = 14$.

(iv) Dimostrare: per ogni $a \in \mathbb{Z}$ esistono soltanto un numero finito di interi $n \in \mathbb{Z}_{>0}$ tali che $\varphi(n) = a$. Concludere che $\lim_{n\to\infty}\varphi(n) = \infty$.

(v) * Dimostrare che $0 \leq \frac{\varphi(n)}{n} \leq 1$. Dimostrare che

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1 \qquad \text{e} \qquad \liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0.$$

(Sugg: la somma $\sum_{p \text{ primo}} \frac{1}{p}$ diverge.)

(vi) * Dimostrare che l'insieme

$$\{\frac{\varphi(n)}{n} : n \in \mathbb{Z}_{>0}\}$$

è denso nell'intervallo $[0, 1]$.

10 Zeri di polinomi

10.1 In questo paragrafo studiamo più in dettaglio gli anelli di polinomi. Studiamo, in particolare, gli zeri dei polinomi. Come applicazione dimostriamo qualche proprietà classica e fondamentale del campo $\mathbb{Z}/p\mathbb{Z}$.

10.2 Teorema. (Divisione con resto). Sia R un anello e siano $f, g \in R[X]$. Supponiamo che

$$g = b_m X^m + b_{m-1}X^{m-1} + \ldots + b_1 X + b_0$$

con $b_m \in R^*$. Allora esistono unici $q, r \in R[X]$ tali che

$$f = qg + r, \qquad r = 0 \text{ oppure } \deg(r) < \deg(g).$$

Dimostrazione. Dimostriamo prima l'esistenza dei polinomi q e r. Se $f = 0$, basta prendere $q = r = 0$. Supponiamo dunque $f \neq 0$ e diamo la dimostrazione per induzione rispetto a $\deg(f)$.

Se $\deg(f) < \deg(g)$, basta prendere $q = 0$ e $r = f$. Se

$$f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

con $a_n \neq 0$ e $n \geq m$, introduciamo

$$f_1 = f - a_n b_m^{-1} X^{n-m} g = \left(a_{n-1} - a_n b_m^{-1} b_{m-1}\right) X^{n-1} + \ldots$$

Siccome $\deg(f_1) < \deg(f)$, abbiamo per induzione

$$f_1 = q_1 g + r_1, \qquad r_1 = 0 \text{ oppure } \deg(r_1) < \deg(g).$$

Quindi

$$f = f_1 + a_n b_m^{-1} X^{n-m} g = \left(q_1 + a_n b_m^{-1} X^{n-m}\right) g + r_1$$

con $r_1 = 0$ oppure $\deg(r_1) < \deg(g)$ come richiesto. Questo dimostra l'esistenza di q ed r.

Per dimostrarne l'unicità, supponiamo che $f = qg + r = q'g + r'$ con $\deg(r), \deg(r') < \deg(g)$ oppure r, $r' = 0$. Dunque

$$(q - q')g = r' - r.$$

Il primo coefficiente di g è un'unità. Dunque, se $q \neq q'$, il grado di $(q - q')g$ è almeno $\deg(g)$. D'altra parte, $\deg(r - r') < \deg(g)$ oppure $r - r' = 0$. Questa contraddizione implica $q = q'$ e quindi $r = r'$. □

10.3 Esempio. Dati i polinomi $f, g \in R[X]$ l'algoritmo di Euclide, simile a quello nel primo paragrafo, è un metodo efficiente per ottenere il quoziente q ed il resto r. Piuttosto che darne una descrizione precisa diamo un esempio esplicito con polinomi in $\mathbb{Z}[X]$. Siano

$$f = 6X^3 + 7X^2 + 2X + 3, \qquad g = -X^2 + 2X - 3.$$

Osserviamo che il primo coefficiente di g è l'unità $-1 \in \mathbb{Z}^*$.

$$\begin{array}{rcrcrcr|l}
\multicolumn{7}{l|}{6X^3 + 7X^2 + 2X + 3} & -X^2 + 2X - 3 \\
\cline{8-8}
6X^3 & + & -12X^2 & + & 18X & & & -6X - 19 \\
\cline{1-5}
0 & & 19X^2 & - & 16X & + & 3 & \\
 & & 19X^2 & - & 38X & + & 57 & \\
\cline{3-7}
 & & 0 & & 22X & - & 54 &
\end{array}$$

] Prima sottraiamo $-6X \cdot (-X^2 + 2X - 3) = 6X^3 - 12X^2 + 18X$ di f. In questo modo si cancella il termine di grado 3 e si trova la differenza $19X^2 - 16X + 3$. Poi sottraiamo $-19 \cdot (-X^2 + 2X - 3) = 19X^2 - 38X + 57$. Adesso si cancella il termine di grado 2 e si trova come differenza $22X - 54$. Concludiamo che $f = qg + r$ con

$$q = -6X - 19, \qquad r = 22X - 54.$$

Dimostriamo qualche corollario del Teorema 10.2.

10.4 Teorema. Sia K un campo. Allora ogni ideale dell'anello $K[X]$ è principale.

Dimostrazione. Sia I un ideale di $K[X]$. Se $I = \{0\}$, l'ideale è ovviamente principale. Supponiamo dunque $I \neq \{0\}$ e prendiamo $g \in I$, $g \neq 0$ di grado *minimale*.

Affermiamo che g genera I: sia $f \in I$. Per il Teorema 10.2 possiamo dividere f per g con quoziente q e resto r:

$$f = qg + r; \qquad r = 0 \text{ oppure } \deg(r) < \deg(g).$$

Siccome $r = f - qg \in I$, è impossibile che $\deg(r) < \deg(g)$ ed abbiamo $r = 0$, cioè $f = qg$. In altre parole f è contenuto nell'ideale (g) generato da g. Dunque $I = (g)$ come affermato. □

10.5 Proposizione. Sia R un anello commutativo e sia $\alpha \in R$. Allora

(*i*) Per ogni polinomio $f \in R[X]$ esiste $q \in R[X]$ tale che

$$f = q \cdot (X - \alpha) + f(\alpha)$$

(*ii*) L'applicazione

$$\Psi : R[X] \longrightarrow R, \qquad f \longmapsto f(\alpha)$$

è un omomorfismo suriettivo con nucleo $(X - \alpha)$.

(*iii*) C'è un isomorfismo di anelli, indotto da Ψ,

$$R[X]/(X - \alpha) \cong R, \qquad \overline{f} \longmapsto f(\alpha).$$

Dimostrazione. *(i)* Per il Teorema 10.2 si ha

$$f = q \cdot (X - \alpha) + r$$

dove $r = 0$ o $\deg(r) < 1$. In altre parole, $r \in R$. Per calcolare r, sostituiamo $X = \alpha$. Per l'Eserc.(9.H) abbiamo $f(\alpha) = q(\alpha)(\alpha - \alpha) + r$ e quindi $r = f(\alpha)$ come richiesto.
(ii) Per l'Eserc.(9.H), la mappa Ψ è un omomorfismo. Per la parte *(i)*, un polinomio f è in $\ker(\Psi)$ se e soltanto se f è divisibile per $X - \alpha$. Cioè, il nucleo di Ψ è $(X - \alpha)$. È ovvio che Ψ è suriettiva.
(iii) Questa parte segue dal Primo Teorema di Isomorfismo applicato all'omomorfismo Ψ e dalla parte *(ii)*. □

10.6 Proposizione. C'è un isomorfismo di anelli

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}.$$

Dimostrazione. Consideriamo la mappa

$$\Phi : \mathbb{R}[X] \longrightarrow \mathbb{C}, \qquad \Phi(f) = f(i).$$

È facile vedere che Φ è un omomorfismo suriettivo. Calcoliamo il nucleo di Φ: ovviamente $X^2 + 1$, e più generalmente, ogni multiplo di $X^2 + 1$ è contenuto in $\ker(\Phi)$. Viceversa, sia $f \in \ker(\Phi)$. Per il Teorema 10.2, si ha

$$f = q \cdot (X^2 + 1) + r; \qquad r = 0 \text{ oppure } \deg(r) < 2.$$

Sostituendo $X = i$, si trova $r(i) = 0$. Se r avesse grado 1, allora $r = c_1 X + c_0$ con $c_1, c_0 \in \mathbb{R}$ e $c_1 \neq 0$. Ma questo implicherebbe che $i = -c_0/c_1 \in \mathbb{R}$, che è assurdo. Allora, il polinomio r deve essere costante e quindi $r = 0$. Concludiamo che $f = q \cdot (X^2 + 1)$ e quindi $\ker(\Psi) = (X^2 + 1)$.

Un'applicazione del Primo Teorema di Isomorfismo all'omomorfismo Φ conclude adesso la dimostrazione. □

10.7 Osservazione. La Proposizione 10.6 ci dà un modo di costruire il campo dei numeri complessi $\mathbb{C}$ senza introdurre un simbolo i. La definizione dei numeri complessi di un algebrista puro è semplicemente

$$\mathbb{C} := \mathbb{R}[X]/(X^2+1).$$

In questa costruzione i è un modo di scrivere l'immagine di X nell'anello $\mathbb{R}[X]/(X^2+1)$.

10.8 Teorema. Sia R un anello commutativo e sia $g = b_nX^n + b_{n-1}X^{n-1} + \ldots + b_0 \in R[X]$ un polinomio di grado n con $b_n \in R^*$. Allora per ogni elemento $\overline{f} \in R[X]/(g)$ esiste un unico polinomio $r \in R[X]$ con $deg(r) < n$ oppure $r = 0$ tale $\overline{f} = \overline{r}$:

$$R[X]/(g) = \{\overline{r} : \ r = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0 \in R[X]\ \}.$$

Dimostrazione. Sia $\overline{f} \in R[X]/(g)$. Usando il Teorema 10.2 troviamo polinomi q e r, con $deg(r) < n$ oppure $r = 0$, tali che $f = qg + r$ e quindi

$$\overline{f} = \overline{qg + r} = \overline{r}$$

perchè la differenza $(qg + r) - r = qg$ appartiene all'ideale (g). L'unicità di tale r segue dal Teorema 10.2. □

10.9 Esempi. Per *ogni* r, $s \in R$ e $g = X^2 + rX + s \in R[X]$ gli elementi dell'anello $R[X]/(g)$ sono del tipo $\overline{aX + b}$ per a, $b \in R$. L'addizione di tali elementi è quella ovvia:

$$\overline{aX+b} + \overline{cX+d} = \overline{aX+b+cX+d} = \overline{(a+c)X + (b+d)}.$$

Il prodotto però dipende in modo essenziale dalla scelta di g. Per esempio:

$$\overline{X+1} \cdot \overline{X-1} = \overline{X^2-1} = \overline{0} \qquad (\in R[X]/(X^2-1)).$$

Quindi $R[X]/(X^2-1)$ è un anello con divisori di zero. Però, per esempio l'anello $\mathbb{R}[X]/(X^2+1)$ è un campo (vedi 10.6) e quindi non ha divisori di zero. Infatti $X^2 - 1 = X^2 + 1 - 2$ e perciò:

$$\overline{X+1} \cdot \overline{X-1} = \overline{X^2-1} = \overline{-2} \qquad (\in \mathbb{R}[X]/(X^2+1)).$$

Vedi anche l'Eserc. (9.U) per il caso $g = X^2$.

10.10 Definizione. Sia R un anello e sia $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polinomio in $R[X]$. Un elemento $\alpha \in R$ si dice uno *zero* di f se $f(\alpha) = 0$, cioè se

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

10.11 Teorema. Sia R un dominio di integrità e sia $f \in R[X]$. Supponiamo che f abbia n zeri distinti $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$. Allora esiste un polinomio $q \in R[X]$ tale che

$$f = q \cdot (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n).$$

Dimostrazione. Diamo la dimostrazione per induzione rispetto al numero n di zeri $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$. Se $n = 0$, il teorema vale. Supponiamo adesso che f abbia $n+1$ zeri distinti $\alpha_1, \ldots, \alpha_n, \alpha_{n+1} \in R$. Per la Prop.10.5 abbiamo

$$f = f_1 \cdot (X - \alpha_{n+1}).$$

Per ogni $1 \leq i \leq n$ abbiamo inoltre $0 = f(\alpha_i) = f_1(\alpha_i)(\alpha_i - \alpha_{n+1})$ per l'Esercizio (9.H). Siccome R è un dominio e $\alpha_i - \alpha_{n+1} \neq 0$ deve essere $f_1(\alpha_i) = 0$. Per ipotesi induttiva abbiamo allora

$$f_1 = q \cdot (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n)$$

per un certo polinomio $q \in R[X]$. Il risultato segue adesso dal fatto che $f = f_1 \cdot (X - \alpha_{n+1})$. □

10.12 Corollario. Sia R un dominio di integrità e sia $f \in R[X]$ un polinomio non nullo di grado d. Allora f ha al più d zeri distinti in R.

Dimostrazione. Supponiamo che f abbia n zeri distinti $\alpha_1, \ldots, \alpha_n \in R$. Per il Teorema 10.11 si ha

$$f = q \cdot (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$$

e, per l'additività del grado,

$$d = \deg(f) \geq \deg((X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)) = n$$

come richiesto. □

10.13 Può succedere che un polinomio f con coefficienti in un dominio R di grado n abbia esattamente n zeri distinti. Per esempio il polinomio $X^3 - 9X \in \mathbb{Z}[X]$ ha gli zeri $0, 3$ e -3. Però, in generale non è così. Per esempio $2X - 3 \in \mathbb{Z}[X]$ ha grado 1 ma non ha zeri in $\mathbb{Z}$. Un altro esempio è il polinomio $X^2 - 2 \in \mathbb{Q}[X]$, il quale non ha zeri in $\mathbb{Q}$ perché $\sqrt{2} \notin \mathbb{Q}$. Il polinomio $(X-1)^2 \in \mathbb{Z}[X]$ ha grado 2, ma soltanto uno zero in $\mathbb{Z}$. In questo caso si dice che lo zero ha molteplicità 2.

La Proposizione 10.11 e il suo Corollario 10.12 sono, in generale, falsi se R non è un dominio di integrità. Per esempio, il polinomio $X^2 - 1 \in (\mathbb{Z}/12\mathbb{Z})[X]$ ha i quattro zeri $\overline{1}, \overline{5}, \overline{7}$ e $\overline{11}$. Anche la commutatività di R è essenziale: il polinomio $X^2 + 1 \in \mathbb{H}[X]$ ha un numero *infinito* di zeri in $\mathbb{H}$ (Si veda l'Eserc (10.C)). Nella dimostrazione della Prop.10.11, la commutatività di R è stata assunta quando abbiamo utilizzato il fatto che la valutazione dei polinomi su un elemento di R è un omomorfismo da $R[X]$ a R (vedi Eserc. (9.H)).

Gli elementi $\pm i \in \mathbb{H}$ sono zeri di $X^2 + 1 \in \mathbb{H}[X]$ e $X^2 + 1 = (X - i)(X + i)$ nell'anello $\mathbb{H}[X]$ però $j^2 + 1 \neq (j - i)(j + i)$, infatti, $j^2 + 1 = 0$ e $(j - i)(j + i) = j^2 + ji - ij - i^2 =$

$-1+(-k)-k-(-1)=-2k$. In generale $f=gh$ (in $\mathbb{H}[X]$) *non* implica che $f(j)=g(j)h(j)$ cioè in generale la valutazione dei polinomi su un elemento di $\mathbb{H}$ *non* è un omomorfismo da $\mathbb{H}[X]$ a $\mathbb{H}$ (vedi Eserc. (9.H)).

10.14 Definizione. Sia R un dominio, sia $\alpha\in R$ e sia $f\in R[X]$. Se α è uno zero di f, si può, per il Teorema 10.11, scrivere $f=f_1\cdot(X-\alpha)$ dove $f_1\in R[X]$. Se anche $f_1(\alpha)=0$ si dice che α è uno zero doppio di f. Una seconda applicazione del Teorema 10.11 ci da

$$f=f_2\cdot(X-\alpha)^2$$

dove $f_2\in R[X]$.

Per studiare gli zeri doppi, introduciamo il polinomio *derivato*.

10.15 Definizione. Sia R un anello commutativo. Per un polinomio

$$f=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0\in R[X]$$

definiamo il polinomio *derivato*:

$$f'=na_nX^{n-1}+(n-1)a_{n-1}X^{n-2}+\ldots+a_1\in R[X].$$

Si noti che questa definizione del polinomio derivato ha senso su anelli commutativi qualsiasi. Non dipende cioè dall'analisi.

10.16 Proposizione. Sia R un anello commutativo. Siano $f,g\in R[X]$. Allora

$$\begin{aligned}\alpha' &= 0, \qquad \text{per ogni } \alpha\in R,\\ (f+g)' &= f'+g',\\ (f\cdot g)' &= f'g+fg'.\end{aligned}$$

Dimostrazione. Siano $f=a_nX^n+\ldots+a_1X+a_0$ e $g=b_mX^m+\ldots+b_1X+b_0$ in $R[X]$. Lasciamo al lettore la facile verifica che $\alpha'=0$ per $\alpha\in R$ e che $(f+g)'=f'+g'$. Dimostriamo che

$$(f\cdot g)'=f'g+fg'$$

per induzione rispetto al grado di f. Se f è costante, il risultato segue dalle seconda parte, perché in questo caso $f'=0$. Supponiamo che $\deg(f)=n>0$ e scriviamo $f=a_nX^n+f_1$ dove $\deg(f_1)<n$. Allora

$$(f\cdot g)'=(a_nX^n\cdot g)'+(f_1\cdot g)'.$$

Il secondo membro si ottiene dall'ipotesi induttiva. Per il primo membro vale:

$$\begin{aligned}(a_nX^n\cdot g)' &= (a_nb_mX^{n+m}+\ldots+a_nb_1X^{n+1}+a_nb_0X^n)'\\ &= (n+m)a_nb_mX^{n+m-1}+\ldots+(n+1)a_nb_1X^n+na_nb_0X^{n-1}\\ &= na_nX^{n-1}g+a_nX^ng'\end{aligned}$$

Concludiamo dunque

$$\begin{aligned}(f\cdot g)' &= na_nX^{n-1}g + a_nX^ng' + f_1'g + f_1g'\\ &= (na_nX^{n-1} + f_1')g + (a_nX^n + f_1)g'\\ &= f'g + fg'\end{aligned}$$

come richiesto. □

10.17 Proposizione. Sia R un dominio e sia $f \in R[X]$. Sia $\alpha \in R$ uno zero di f. Allora α è uno zero doppio di f se e soltanto se $f'(\alpha) = 0$.

Dimostrazione. Siccome α è uno zero di f abbiamo

$$f = f_1 \cdot (X - \alpha).$$

Per la Proposizione 10.16 abbiamo dunque

$$f' = f_1'(X - \alpha) + f_1.$$

Sostituendo $X = \alpha$ troviamo $f'(\alpha) = f_1(\alpha)$. Questo implica che $f'(\alpha) = 0$ se e soltanto se f ha α come zero doppio, come richiesto. □

10.18 Concludiamo questo paragrafo con un'applicazione.

10.19 Teorema. Sia p un primo. Allora nell'anello $\mathbb{Z}/p\mathbb{Z}[X]$ vale

$$\prod_{\overline{a}\in\mathbb{Z}/p\mathbb{Z}} (X - \overline{a}) = X^p - X.$$

Dimostrazione. Per il Teorema di Fermat (Cor.5.20(i)), abbiamo

$$\overline{a}^{p-1} = \overline{1} \qquad \text{per ogni } \overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*.$$

In altre parole, ogni $\overline{a} \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ è uno zero del polinomio $X^{p-1} - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$. Siccome $\mathbb{Z}/p\mathbb{Z}$ è un dominio, possiamo applicare il Teorema 10.11. Troviamo

$$X^{p-1} - \overline{1} = q \cdot (X - \overline{1})(X - \overline{2}) \cdot \ldots \cdot (X - \overline{p-1})$$

con $q \in \mathbb{Z}/p\mathbb{Z}[X]$. Considerando i gradi dei diversi polinomi, vediamo che q deve essere un polinomio costante. Siccome $X^{p-1} - \overline{1}$ è un polinomio monico, questa costante è uguale a 1. Moltiplicando l'equazione per X, otteniamo la tesi. □

10.20 Corollario. (Teorema di Wilson). Un intero p è un primo se e soltanto se

$$(p-1)! \equiv -1 \bmod p.$$

Dimostrazione. Sia p un primo. Se $p = 2$ l'affermazione si verifica facilmente. Per $p \neq 2$ utilizziamo il Teorema 10.19:

$$\prod_{i=1}^{p-1}(X - \overline{i}) = X^{p-1} - \overline{1}.$$

Guardando i termini noti si vede che

$$(-\overline{1})(-\overline{2}) \cdot \ldots \cdot (-(\overline{p-1})) = -\overline{1}.$$

Siccome p è dispari, abbiamo un numero *pari* di termini e il risultato segue. Per il viceversa si veda l'Eserc.(10.E). □

10.21 Proposizione. Sia $p > 2$ un numero primo. Le seguenti affermazioni sono equivalenti:

(*i*) Esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \bmod p$.

(*ii*) Il polinomio $X^2 + 1$ ha uno zero in $\mathbb{Z}/p\mathbb{Z}$.

(*iii*) $p \equiv 1 \bmod 4$.

Dimostrazione. Le parti *(i)* e *(ii)* sono soltanto traduzioni una dell'altra.
Supponiamo *(i)*: $x^2 \equiv -1 \bmod p$. Allora la classe $\overline{x}$ ha ordine 4 nel gruppo $(\mathbb{Z}/p\mathbb{Z})^*$. Quindi, per il Cor.5.19, l'ordine $p - 1$ di $(\mathbb{Z}/p\mathbb{Z})^*$ è divisibile per 4. Questo implica *(iii)*.
Supponiamo *(iii)*: $p \equiv 1 \bmod 4$. Segue dal'Esercizio (10.G) che esiste un $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \bmod p$. □

Esercizi.

(10.A) Siano dati i due polinomi $f = 2X^7 + 1$ e $g = X^2 + X + 1$. Determinare due polinomi $q, r \in \mathbb{Z}[X]$ tali che $f = qg + r$ e $\deg(r) < \deg(g) = 2$.

(10.B) (i) Quanti zeri ha il polinomio $X^2 - \overline{1} \in \mathbb{Z}/24\mathbb{Z}[X]$ in $\mathbb{Z}/24\mathbb{Z}$?

(ii) * Quanti zeri ha il polinomio $X^6 - \overline{1} \in \mathbb{Z}/504\mathbb{Z}[X]$ in $\mathbb{Z}/504\mathbb{Z}$?

(10.C) Sia $x = a + bi + cj + dk \in \mathbb{H}$ con $a, b, c, d \in \mathbb{R}$. Far vedere che le seguenti affermazioni sono equivalenti:

(i) x è uno zero di $X^2 + 1$.

(ii) $x\overline{x} = 1$ e $\overline{x} = -x$. (Si veda l'Eserc.(2.F))

(iii) $a = 0$ e $b^2 + c^2 + d^2 = 1$.

Concludere che gli zeri del polinomio $X^2 + 1$ in $\mathbb{H}$ sono infiniti.

(10.D) (*Formula di interpolazione di Lagrange*) Sia K un campo, sia $f \in K[X]$ un polinomio e siano $\alpha_0, \alpha_1, \ldots, \alpha_n$ elementi distinti di K.

(i) Far vedere: se $n \geq \deg(f)$, allora

$$f(X) = \sum_{i=0}^{n} f(\alpha_i) \frac{\prod_{j=0, j\neq i}^{n} (X - \alpha_j)}{\prod_{j=0, j\neq i}^{n} (\alpha_i - \alpha_j)}.$$

(ii) Siano $\beta_0, \beta_1, \ldots, \beta_n \in K$. Dimostrare che esiste un polinomio $g \in R[X]$, di grado al più n, tale che $g(\alpha_i) = \beta_i$ per ogni $0 \leq i \leq n$.

(10.E) Sia n un intero positivo.

(i) Far vedere: se n non è un primo allora $\mathrm{mcd}(n, (n-1)!) \neq 1$.

(ii) Dimostrare: se $(n-1)! \equiv -1 \bmod n$, allora n è primo.

(iii) Far vedere: se $(n-1)!$ non è congruo a 0 o a -1 modulo n, allora $n = 4$.

(10.F) Sia K un campo e sia $f \in K[X]$ un polinomio di grado $n \geq 1$. Dimostrare che ogni classe laterale dell'anello quoziente $K[X]/(f)$ contiene un unico rappresentante r con $\deg(r) < \deg(f)$. (In questo esercizio mettiamo $\deg(0) = -1$.)

(10.G) Sia $p \equiv 1 \bmod 4$ un numero primo. Far vedere che $z = \left(\frac{p-1}{2}\right)!$ soddisfa $z^2 \equiv -1 \bmod p$.

(10.H) Per ogni $n \in \mathbb{Z}_{\geq 0}$ calcolare

$$1^n + 2^n + \ldots + (p-1)^n \bmod p.$$

(10.I) Sia R un anello commutativo e siano $f, g \in R[X]$. Supponiamo che f sia contenuto nell'ideale g^k per un certo intero $k \geq 0$. Far vedere che $f' \in (g^{k-1})$.

(10.J) Sia $f \in (\mathbb{Z}/2\mathbb{Z})[X]$. Dimostrare che le seguenti affermazioni sono equivalenti:

(i) $f' = 0$.

(ii) f è della forma $f = \sum_{k=0}^{n} a_k X^{2k}$ con $a_k \in \mathbb{Z}/2\mathbb{Z}$.

(iii) Esiste $g \in (\mathbb{Z}/2\mathbb{Z})[X]$ tale che $f = g^2$.

Far vedere che $(f')' = 0$.

(10.K) (*Formula di Leibniz*) Sia R un anello commutativo e sia $f \in R[X]$. Per $k \in \mathbb{Z}_{\geq 0}$ definiamo induttivamente

$$f^{(0)} = f, \qquad f^{(k)} = (f^{(k-1)})' \qquad \text{per } k \geq 1.$$

Dimostrare che per $f, g \in R[X]$ ed $n \in \mathbb{Z}_{\geq 0}$ si ha

$$(f \cdot g)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}.$$

Qua $\binom{n}{k}$ indica il coefficiente binomiale usuale.

(10.L) Sia R un dominio e siano $f, g \in R[X]$ polinomi con $\deg(f) < \#R$ e $\deg(g) < \#R$. Dimostrare che

$$f = g \iff f(x) = g(x) \text{ per ogni } x \in R.$$

Concludere che per un dominio infinito si ha $f = g \Leftrightarrow f(x) = g(x)$ per ogni $x \in R$.

(10.M) Sia p un numero primo e siano $f, g \in (\mathbb{Z}/p\mathbb{Z})[X]$. Far vedere che

$$f(x) = g(x) \text{ per ogni } x \in \mathbb{Z}/p\mathbb{Z} \iff f - g \in (X^p - X)$$

(10.N) * In questo esercizio determiniamo la struttura dei gruppi $(\mathbb{Z}/2^n\mathbb{Z})^*$.

(i) Far vedere che $(\mathbb{Z}/2\mathbb{Z})^*$ è banale, che $(\mathbb{Z}/4\mathbb{Z})^*$ è ciclico di ordine 2 e che $(\mathbb{Z}/8\mathbb{Z})^*$ è isomorfo al gruppo V_4 di Klein.

(ii) Far vedere che l'elemento $5 \in (\mathbb{Z}/2^n\mathbb{Z})^*$ ha ordine 2^{n-2} se $n \geq 2$. (Sugg. Calcolare l'elemento $5^{2^{n-3}} = (1+4)^{2^{n-3}}$ in $(\mathbb{Z}/2^n\mathbb{Z})^*$ con il binomio di Newton).

(iii) Far vedere che gli elementi -1 e 5 generano $(\mathbb{Z}/2^n\mathbb{Z})^*$. Far vedere che $-1 \notin < 5 >$. Concludere che

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong < -1 > \times < 5 > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

(Sugg. Utilizzare l'Eserc.(3.P)).

(10.O) Sia n un numero dispari. Dimostrare che il polinomio $X^2 - \overline{1}$ ha 2^t zeri in $\mathbb{Z}/n\mathbb{Z}$, dove t è il numero dei primi distinti che dividono n (Sugg. Utilizzare l'Eserc.(10.M)). Concludere che gli unici elementi di $(\mathbb{Z}/n\mathbb{Z})^*$ di ordine 2 sono ± 1 se e soltanto se n è una potenza di un numero primo $p > 2$.

11 Ideali primi e massimali

11.1 In questo paragrafo consideriamo soltanto gli anelli commutativi. Generalizziamo il concetto di un numero primo in tre modi diversi: introduciamo gli *ideali primi*, gli *ideali massimali* e, per i domini di integrità, gli *elementi irriducibili*.

11.2 Definizione. Sia R un anello commutativo. Un ideale I di R si dice *un ideale primo* se $I \neq R$ e se per ogni $x, y \in R$ vale la proprietà:

$$\text{se } xy \in I, \text{ allora } x \in I \text{ oppure } y \in I.$$

11.3 Esempi.

(*i*) L'ideale $p\mathbb{Z}$ di $\mathbb{Z}$, generato da un numero primo p, è un ideale primo. Questo fatto è il contenuto della Proposizione 1.13.

(*ii*) Consideriamo l'ideale generato da $X-1$ nell'anello $\mathbb{R}[X]$. Per la Prop. 10.5, l'applicazione $\Psi : \mathbb{R}[X] \to \mathbb{R}$ data da $\Psi(f) = f(1)$ ha nucleo uguale a $(X-1)$. Cioè

$$(X-1) = \{f \in \mathbb{R}[X] : f(1) = 0\}.$$

Supponiamo che $f, g \in \mathbb{R}[X]$ soddisfino $fg \in (X-1)$. Allora $f(1)g(1) = 0$ e quindi, siccome $\mathbb{R}$ è un dominio di integrità, $f(1) = 0$ oppure $g(1) = 0$. In altre parole, $f \in (X-1)$ o $g \in (X-1)$. Concludiamo che l'ideale $(X-1)$ è primo.

L'ideale generato da $X^2 - 1$ invece, non è primo. Infatti, il prodotto $(X-1)(X+1)$ è contenuto in (X^2-1), ma non lo sono i fattori $X-1$ ed $X+1$. Questo segue dal fatto che, se h è contenuto in (X^2-1), allora $h = g(X^2-1)$ e dunque, per l'Eserc.(8.P), vale $h = 0$ oppure $\deg(h) = \deg(g) + 2 \geq 2$.

(*iii*) L'ideale banale R di un anello R, per definizione, non è mai un ideale primo. L'ideale $\{0\}$ invece, può essere primo. Questo significa che se $xy = 0$ per qualche $x, y \in R$, allora $x = 0$ oppure $y = 0$. In altre parole, R è un dominio di integrità.

Il prossimo teorema ci dà un modo efficiente per decidere se un dato ideale è un ideale primo o meno.

11.4 Teorema. Sia R un anello commutativo. Allora, un ideale I di R è primo se e soltanto se l'anello quoziente R/I è un dominio di integrità.

Dimostrazione. Supponiamo che I sia un ideale primo. Per definizione $I \neq R$ e quindi R/I non è l'anello zero. Supponiamo che x, $y \in R$ soddisfino $\overline{x} \cdot \overline{y} = \overline{0}$ in R/I. Questo significa che $xy \in I$. Abbiamo dunque $x \in I$ oppure $y \in I$, cioè $\overline{x} = \overline{0}$ oppure $\overline{y} = \overline{0}$. Concludiamo che R/I è un dominio.

Per dimostrare che I è un ideale primo se R/I è un dominio di integrità, basta leggere questa dimostrazione nel senso opposto. □

11.5 Definizione. Sia R un anello commutativo. Un ideale I di R si dice *un ideale massimale* se $I \neq R$ e se per ogni ideale J di R vale:

$$\text{se } I \subset J \subset R, \text{ allora } J = I \text{ oppure } J = R.$$

Prima di dare esempi di ideali massimali dimostriamo il Teorema 11.6 il quale ci dà un criterio molto utile per decidere se un dato ideale è massimale o meno.

11.6 Teorema. Sia R un anello commutativo. Allora un ideale I di R è massimale se e soltanto se l'anello quoziente R/I è un campo.

Dimostrazione. Supponiamo che I sia un ideale massimale. Per definizione $I \neq R$ e quindi R/I non è l'anello zero. Per dimostrare che R/I è un campo basta far vedere che ogni elemento

non nullo ha un inverso moltiplicativo. Sia $\overline{x} \in R/I$ un elemento non nullo, cioè $x \in R$ ma $x \notin I$. L'ideale $I + (x)$ soddisfa

$$I \underset{\neq}{\subset} I + (x) \subset R$$

e quindi $I + (x) = R$. In particolare $1 = y + rx$ per certi elementi $y \in I$ ed $r \in R$. Guardando questa relazione modulo I troviamo $\overline{r} \cdot \overline{x} = \overline{1}$. L'elemento $\overline{x}$ ha dunque un inverso moltiplicativo come richiesto.

Per dimostrare l'altra implicazione, sia J un ideale di R con $I \subset J \subset R$. Considerando queste inclusioni modulo l'ideale I vediamo che $J/I = \{\overline{y} : y \in J\}$ è un ideale di R/I. Siccome R/I è un campo, è anche un anello con divisione e, per la Prop.9.7, contiene soltanto ideali banali. Abbiamo dunque $J/I = \{\overline{0}\}$ oppure $J/I = R/I$. In altre parole $J = I$ oppure $J = R$. Questo conclude la dimostrazione del teorema. □

11.7 Corollario. Un ideale massimale di un anello commutativo R è anche un ideale primo.

Dimostrazione. Ogni campo è un dominio di integrità. Il risultato segue adesso dai Teoremi 11.4 e 11.6. □

11.8 Esempi.

(*i*) L'ideale banale $\{0\}$ di un anello R è massimale se e soltanto se R è un campo. Questo segue dal teorema prendendo $I = \{0\}$.

(*ii*) Per ogni numero primo p, l'ideale $p\mathbb{Z}$ di $\mathbb{Z}$ è massimale perchè l'anello quoziente $\mathbb{Z}/p\mathbb{Z}$ è un campo (Si veda la Prop. 8.10). Per l'esempio *(i)*, l'ideale $\{0\}$ di $\mathbb{Z}$ è primo. Esso non è, però, massimale:

$$\{0\} \underset{\neq}{\subset} 2\mathbb{Z} \underset{\neq}{\subset} \mathbb{Z}.$$

Vediamo dunque che esistono ideali primi che non sono massimali.

(*iii*) L'ideale $(X^2 + 1)$ di $\mathbb{R}[X]$ è massimale perché

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$$

come abbiamo visto nella Proposizione 10.6.

(*iv*) Sia I l'ideale $(Y - 1, X^2 + Y - 2) \subset \mathbb{Q}[X, Y]$. Calcoliamo l'anello quoziente $\mathbb{Q}[X, Y]/I$:

$$\begin{aligned}
\mathbb{Q}[X,Y]/(Y-1, X^2+Y-2) &\cong (\mathbb{Q}[X][Y]/(Y-1))/(X^2+Y-2) && \text{(per 9.16(}ii\text{))}\\
&\cong \mathbb{Q}[X]/(X^2+1-2) && \text{(per 10.5(}iii\text{))}\\
&\cong \mathbb{Q}[X]/(X-1) \times \mathbb{Q}[X]/(X+1) && \text{(per 9.20)}\\
&\cong \mathbb{Q} \times \mathbb{Q}. && \text{(per 10.5(}iii\text{))}
\end{aligned}$$

Abbiamo utilizzato il fatto che $X^2 - 1 = (X - 1)(X + 1)$ in $\mathbb{Q}[X]$.

Siccome l'anello $\mathbb{Q} \times \mathbb{Q}$ ha divisori di zero, l'anello $\mathbb{Q}[X, Y]/(Y - 1, X^2 + Y - 2)$ non è un dominio di integrità. Dunque I non è primo e non è massimale.

(v) Sia n un intero positivo e sia $R = \mathbb{R}[X_1, X_2, \ldots, X_n]$ l'anello dei polinomi in n variabili su $\mathbb{R}$. L'ideale generato da X_1 è primo perché

$$\begin{aligned} \mathbb{R}[X_1, X_2, \ldots, X_n]/(X_1) &\cong (\mathbb{R}[X_2, \ldots, X_n])[X_1]/(X_1) \qquad \text{(per 8.21)} \\ &\cong \mathbb{R}[X_2, \ldots, X_n] \end{aligned}$$

e questo anello è un dominio di integrità. Similmente, l'ideale (X_1, X_2) è primo perché

$$\begin{aligned} \mathbb{R}[X_1, X_2, \ldots, X_n]/(X_1, X_2)), &\cong (\mathbb{R}[X_2, X_3, \ldots, X_n]/(X_2))[X_1]/(X_1), \\ &\cong \mathbb{R}[X_3, \ldots, X_n]. \end{aligned}$$

In questo modo si dimostra che tutti gli ideali nella catena

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \ldots \subset (X_1, X_2, \ldots, X_n)$$

sono ideali primi. Solo l'ultimo ideale è un ideale massimale perché l'anello quoziente $\mathbb{R}[X_1, X_2, \ldots, X_n]/(X_1, X_2, \ldots, X_n)$ è isomorfo al campo $\mathbb{R}$.

11.9 Ci sono rapporti profondi fra la struttura algebrica di certi anelli commutativi e la geometria di varietà algebriche. Per esempio, l'anello $\mathbb{R}[X_1, X_2, \ldots, X_n]$ entra nella geometria dello spazio $\mathbb{R}^n$. Ad un punto $P = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ di $\mathbb{R}^n$ si può associare l'ideale

$$M_P = \{f \in \mathbb{R}[X_1, X_2, \ldots, X_n] : f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0\}.$$

L'ideale M_P è un ideale massimale perché è il nucleo dell'omomorfismo $\mathbb{R}[X_1, X_2, \ldots, X_n] \longrightarrow \mathbb{R}$ dato da $f \mapsto f(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Un'applicazione ripetuta della Prop. 10.5(*ii*) fa vedere che $M_P = (X - \alpha_1, X - \alpha_2, \ldots, X - \alpha_n)$.

La corrispondenza è quasi biiettiva. Basta sostituire ad $\mathbb{R}$ il campo $\mathbb{C}$. Come abbiamo visto nell'Esempio 9.13, c'è un legame stretto tra punti della circonferenza $X^2 + Y^2 = 1$ e omomorfismi suriettivi $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \to \mathbb{R}$. Il nucleo di un tale omomorfismo è un ideale massimale di $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$. La corrispondenza tra punti e ideali massimali diventa biiettiva se si sostituisce $\mathbb{R}$ con $\mathbb{C}$.

Le proprietà geometriche si traducono in termini dell'algebra dell'anello corrispondente e viceversa. Per esempio, il fatto che la figura in $\mathbb{R}^2$ data dalla equazione $x^2y - x = 0$ si spezza in due figure disgiunte (la retta di equazione $x = 0$ e l'iperbole di equazione $xy = 1$) significa per l'anello $\mathbb{R}[X, Y]/(X^2Y - X)$ che si spezza in un prodotto

$$\mathbb{R}[X, Y]/(X) \times \mathbb{R}[X, Y]/(XY - 1).$$

Nella *geometria algebrica* si studia questa reciprocità fra algebra e geometria. Infatti, il tentativo di vedere l'insieme dei numeri primi di anelli come $\mathbb{Z}$, come "punti di una curva algebrica è alla base dei teoremi più importanti nella teoria dei numeri degli ultimi 30 anni. Si veda il libro

di R. Hartshorne: *Algebraic Geometry,* Graduate Texts in Mat. **52**, Springer-Verlag, Berlin Heidelberg New York 1977.

Infine generalizziamo il concetto di numero primo in un terzo modo. Assumiamo ora che R non abbia divisori di zero.

11.10 Definizione. Sia R un dominio di integrità. Un elemento $\alpha \in R$ si dice *irriducibile* se $\alpha \neq 0$, se $\alpha \notin R^*$ e se per ogni $\beta, \gamma \in R$ vale

$$\text{se } \alpha = \beta\gamma \text{ allora } \beta \in R^* \text{ oppure } \gamma \in R^*.$$

11.11 Proposizione. Sia R un dominio di integrità e sia $\alpha \in R$ un elemento non zero. Allora, se l'ideale (α) è primo, l'elemento α è irriducibile.

Dimostrazione. Per definizione $(\alpha) \neq R$ e quindi $\alpha \notin R^*$. Siano $\beta, \gamma \in R$ tali che

$$\alpha = \beta\gamma.$$

allora $\beta\gamma \in (\alpha)$ e quindi $\beta \in (\alpha)$ oppure $\gamma \in (\alpha)$. Se $\beta \in (\alpha)$, abbiamo

$$\beta = r\alpha = r\beta\gamma \qquad \text{per un certo } r \in R$$

e dunque $\beta(1 - r\gamma) = 0$. Siccome R è un dominio e $\alpha \neq 0$, abbiamo $\beta \neq 0$ e quindi $1 - r\gamma = 0$, cioè $r\gamma = 1$. Concludiamo che γ è un'unità. In modo simile si dimostra che β è un'unità nel caso $\gamma \in (\alpha)$. Questo completa la dimostrazione della proposizione. □

11.12 Abbiamo quindi, per $\alpha \neq 0$ in un dominio di integrità R:

$$(\alpha) \text{ è massimale} \implies (\alpha) \text{ è primo} \implies \alpha \text{ è irriducibile.}$$

Abbiamo visto sopra che esistono ideali primi che non sono massimali. Per esempio l'ideale $\{0\}$ di $\mathbb{Z}$ è primo, però non è massimale. Similmente esistono anche elementi α irriducibili in certi domini tale che gli ideali (α) non sono primi. Diamo un esempio:

11.13 Esempio. Sia R l'anello $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. In altre parole, R è l'anello dato da

$$R = \mathbb{Z}[X]/(X^2 + 5).$$

La mappa $\Phi : \mathbb{Z}[X]/(X^2 + 5) \longrightarrow \mathbb{Z}[\sqrt{-5}]$ data da $\Phi(f) = f(\sqrt{-5})$ dà un isomorfismo fra le due descrizioni di R. Definiamo la *norma* N su R:

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \qquad \text{per } a, b \in \mathbb{Z}.$$

Lasciamo al lettore la verifica del fatto che la norma è moltiplicativa: $N(\alpha\beta) = N(\alpha)N(\beta)$ per $\alpha, \beta \in R$.

Consideriamo adesso l'elemento $2 \in \mathbb{Z}[\sqrt{-5}]$. Abbiamo

$$\begin{aligned}\mathbb{Z}[\sqrt{-5}]/(2) &\cong \mathbb{Z}[X]/(2, X^2+5),\\ &\cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2+\overline{1})\\ &\cong (\mathbb{Z}/2\mathbb{Z})[X]/((X+\overline{1})^2)\end{aligned}$$

Siccome l'anello $(\mathbb{Z}/2\mathbb{Z})[X]/((X+\overline{1})^2)$ ha divisori di zero: $(X+\overline{1})(X+\overline{1}) = 0$, l'ideale generato da $2 \in \mathbb{Z}[\sqrt{-5}]$ non è un ideale primo.

Per vedere che 2 è invece, irriducibile, supponiamo che abbiamo $2 = \beta\gamma$ per certi $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$. Per la moltiplicatività della norma abbiamo

$$4 = N(2) = N(\beta)N(\gamma).$$

Scriviamo $\beta = a + b\sqrt{-5}$ dove $a, b \in \mathbb{Z}$. La norma di β è uguale a a^2+5b^2. Siccome l'equazione $a^2+5b^2 = 2$ non ha soluzioni $a, b \in \mathbb{Z}$, dobbiamo avere che $N(\beta) = 1$ o $N(\gamma) = 1$. Se $N(\beta) = 1$, o equivalentemente $a^2+5b^2 = 1$ dobbiamo avere che $a = \pm 1$ e $b = 0$, cioè $\beta = \pm 1$. Similmente, se $N(\gamma) = 1$ si ha $\gamma = \pm 1$. Concludiamo che o β o γ è un'unità e quindi che 2 è irriducibile.

11.14 Per la dimostrazione del prossimo teorema abbiamo bisogno del cosiddetto *assioma della scelta* della teoria degli insiemi. Questo assioma è stato rilevato abbastanza recentemente da Beppo Levi (Torino 1902) e da E. Zermelo (Freiburg 1903). Noi utilizziamo l'assioma della scelta nella forma equivalente del *Lemma di Zorn* (Si veda il libro di P.R. Halmos: *Teoria elementare degli insiemi*, Feltrinelli, Milano 1970).

11.15 Lemma di Zorn. Sia Ω un insieme parzialmente ordinato. Se ogni catena in Ω ha un limite superiore in Ω, allora Ω contiene un elemento massimale.

11.16 Ricordiamo il significato di alcune parole: un'*ordine parziale* su l'insieme Ω è una relazione "$\leq$ con le proprietà

$$\text{se } x \leq y \text{ e } y \leq z \text{ allora } x \leq z,$$

$$\text{se } x \leq y \text{ e } y \leq x \text{ allora } x = y$$

per ogni $x, y, z \in \Omega$. Una *catena* è un sottoinsieme C di Ω con la proprietà che per ogni $x, y \in C$ si ha che $x \leq y$ oppure $y \leq x$. Un limite superiore della catena C è un elemento x con $y \leq x$ per ogni $y \in C$. Finalmente, un *elemento massimale* è un elemento $x \in \Omega$ tale che per ogni $y \in \Omega$ la relazione $x \leq y$ implica $x = y$.

11.17 Teorema. Sia R un anello commutativo.

(*i*) Se $R \neq \{0\}$, allora R contiene un ideale massimale.

(*ii*) Sia $I \neq R$ un ideale di R. Allora esiste un ideale massimale di R che contiene I.

Dimostrazione. *(i)* Utilizziamo il *Lemma di Zorn*. Sia Ω l'insieme degli ideali $I \neq R$ di R. L'insieme Ω è parzialmente ordinato per l'inclusione. Verifichiamo che ogni catena ha un limite superiore in Ω: sia $\{I_\alpha : \alpha \in A\}$ una catena di ideali $I_\alpha \in \Omega$. Sia

$$J = \cup_{\alpha \in A} I_\alpha.$$

Si verifica facilmente che J è un ideale di R: siano $x, y \in J$. Allora $x \in I_\alpha$ per un $\alpha \in A$ e $y \in I_\beta$ per un $\beta \in A$. Siccome $I_\alpha \subset I_\beta$ oppure $I_\beta \subset I_\alpha$ abbiamo $x, y \in I_\alpha$ oppure $x, y \in I_\beta$. Siccome I_α e I_β sono ideali di R contenuti in J, abbiamo dunque $x - y \in J$. È facile vedere che $rx \in J$ per ogni $x \in J$ ed ogni $r \in R$.

Per ogni $\alpha \in A$ vale $I_\alpha \neq R$ e quindi $1 \notin I_\alpha$. Allora $1 \notin J = \cup_{\alpha \in A} I_\alpha$ e quindi $J \in \Omega$. Ovviamente J è un limite superiore della catena. Per il lemma di Zorn, esiste un elemento massimale $M \in \Omega$, cioè un ideale $M \neq R$ di R che è massimale rispetto all'inclusione. Questo significa esattamente che M è un ideale massimale.

(ii) Per la Prop. 9.16(*i*), ogni ideale di R/I ha la forma J/I dove J è un ideale di R che contiene I. Applicando la parte *(i)* all'anello R/I, si ottiene un ideale $J \subset R$ tale che J/I è massimale in R/I. Quindi per la Prop. 9.16(*ii*) l'anello quoziente $R/J \cong (R/I)/(J/I)$ è un campo. Vediamo che J è massimale come richiesto. □

Esercizi.

(11.A) Sia R un dominio. Far vedere che l'ideale di $R[X, Y]$ generato da X e Y è uguale a

$$\{f \in R[X, Y] : f(0, 0) = 0\}$$

ed è un ideale primo di $R[X, Y]$.

(11.B) Far vedere che l'ideale generato da 5 in $\mathbb{Z}[i]$ non è un ideale primo.

(11.C) Sia K un campo e siano $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Far veder che l'ideale $(X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_n - \alpha_n)$ è un ideale massimale di $K[X_1, X_2, \ldots, X_n]$.

(11.D) Decidere se i seguenti ideali di $\mathbb{Z}[X]$ sono primi o massimali:

(i) $(X, 3)$;
(ii) $(X^2 - 3)$;
(iii) $(7, X^2 - 3)$.

(11.E) Decidere se i seguenti ideali di $\mathbb{Q}[X, Y]$ sono primi o massimali:

(i) $(X^2 + 1)$;
(ii) $(X - Y, Y^2 - Y)$;

(iii) (X^2+1, Y^2+1);

(iv) (X^2+1, Y^2-2).

(11.F) Sia R un anello commutativo e sia I un ideale di R.

(i) Sia J un ideale primo di R che contiene I. Far vedere che J/I è un ideale primo di R/I. Dimostrare che ogni ideale primo di R/I ha questa forma.

(ii) Sia J un ideale massimale di R che contiene I. Far vedere che J/I è un ideale massimale di R/I. Dimostrare che ogni ideale massimale di R/I ha questa forma.

(11.G) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli commutativi. Sia I' un ideale di R'.

(i) Far vedere che $I = f^{-1}(I')$ è un ideale di R. Dimostrare che R/I è isomorfo ad un sottoanello di R'/I'.

(ii) Far vedere: se I' è un ideale primo di R', allora $I = f^{-1}(I')$ è un ideale primo di R.

(iii) Far vedere che l'affermazione "se I' è un ideale massimale di R', allora $I = f^{-1}(I')$ è un ideale massimale di R è falsa.

(11.H) Sia R un anello di Boole (Si veda l'Eserc.(8.G)).

(i) Dimostrare che R è un dominio se e soltanto se R è un campo se e soltanto se $R \cong \mathbb{Z}/2\mathbb{Z}$.

(ii) Sia I un ideale di R. Far vedere che I è primo se e soltanto se I è massimale se e soltanto se $R/I \cong \mathbb{Z}/2\mathbb{Z}$.

(11.I) Sia R un anello commutativo e sia I un ideale di R con indice $[R : I]$ finito. Far vedere che I è primo se e soltanto se è massimale.

(11.J) Sia K un campo e sia $R = K \times K$. Determinare gli ideali primi e massimali di R.

(11.K) Sia R un anello commutativo e sia I un ideale di R. Supponiamo che per ogni $x \in R - I$ vale $x^2 - 1 \in I$.

(i) Dimostrare che $R/I \cong \mathbb{Z}/2\mathbb{Z}$ oppure $R/I \cong \mathbb{Z}/3\mathbb{Z}$.

(ii) Dimostrare che I è un ideale massimale.

(11.L) Sia R un anello commutativo con la proprietà che ogni ideale è primo. Far vedere che R è un campo.

(11.M) Sia $R = C([0,1])$ l'anello delle funzioni continue sull'intervallo $[0,1]$. Per ogni $x \in [0,1]$ definiamo

$$M_x = \{f \in C([0,1]) : f(x) = 0\}$$

(i) Far vedere che M_x è un ideale massimale di $C([0,1])$.

(ii) * Sia I un ideale di $C([0,1])$ tale che I non è contenuto in nessun ideale M_x. Far vedere che $I = R$. (Sugg. Per ogni $x \in [0,1]$ esiste dunque una funzione $f_x \in I$ tale che $f_x(x) \neq 0$. Far vedere che esistono $x_1, x_2, \ldots, x_m \in [0,1]$ tali che

$$\sum_{i=1}^{m} f_{x_i}(x)^2 > 0 \qquad \text{per ogni } x \in [0,1].$$

(Utilizzare il Teorema di Bolzano-Weierstrass o, equivalentemente, la compattezza dell'intervallo $[0,1]$.)

(iii) Far vedere che ogni ideale massimale M di $C([0,1])$ è uguale a M_x per un $x \in [0,1]$.

(11.N) Sia R un anello commutativo. L'anello R si dice *locale* se $R - R^*$ è un ideale di R.

(i) Dimostrare: R è locale se e soltanto se R ha esattamente un ideale massimale.

(ii) Sia R un anello locale e sia $x \in R$ con $x^2 = x$. far vedere che $x = 0$ oppure $x = 1$.

(11.O) Sia $R = \{a/b \in \mathbb{Q} : a, b \in \mathbb{Z}, b \not\equiv 0 \bmod 5\}$. Dimostrare che R è un anello locale. Determinare l'unico ideale massimale M di R. Far vedere che $R/M \cong \mathbb{Z}/5\mathbb{Z}$.

(11.P) Decidere se i seguenti elementi di $\mathbb{Z}[\sqrt{-3}]$ sono irriducibili o meno:

$$\sqrt{-3},\ 1,\ 2,\ 1+\sqrt{-3},\ 5.$$

(11.Q) Sia R un dominio di integrità.

(i) Far vedere che se $\alpha \in R$ è irriducibile allora $\varepsilon\alpha$ è irriducibile per ogni unità ε di R.

(ii) Si dice che due elementi $\alpha, \beta \in R$ sono *associati* se esiste un unità ε di R tale che $\alpha = \varepsilon\beta$. Far vedere che "essere associato è una relazione di equivalenza.

(11.R) Far vedere che l'elemento $\sqrt{-6}$ di $\mathbb{Z}[\sqrt{-6}]$ è irriducibile, ma che l'ideale $(\sqrt{-6})$ non è un ideale primo.

(11.S) * Sia R un anello commutativo e supponiamo che $a \in R$ abbia la proprietà che $a^n \neq 0$ per ogni $n \in \mathbb{Z}_{>0}$. Far vedere che R contiene un ideale primo I con $a \notin I$. (Sugg. Applicare il lemma di Zorn all'insieme degli ideali che non contengono nessuna potenza di a.)

(11.T) * Il *radicale* $\sqrt{0}$ di un anello commutativo è definito da

$$\sqrt{0} = \{a \in R : a^n = 0 \text{ per un intero positivo } n\}.$$

(i) Far vedere che $\sqrt{0}$ è un ideale di R.

(ii) Dimostrare che $\sqrt{0} = \cap_I I$ dove I varia fra gli ideali primi di R.

12 Fattorizzazione

In questo paragrafo studiamo certe classi di anelli speciali. Introduciamo gli *anelli a ideali principali*, gli *anelli Euclidei* e gli *anelli a fattorizzazione unica*. L'anello $\mathbb{Z}$ e l'anello $K[X]$ dei polinomi con coefficienti in un campo K ne sono esempi.

12.1 Definizione. Un dominio di integrità R si dice un *anello a ideali principali* se ogni ideale di R è un ideale principale.

12.2 Teorema. Sia R un anello a ideali principali. Sia $\alpha \in R$, $\alpha \neq 0$. Allora le seguenti affermazioni sono equivalenti:

(*i*) L'ideale (α) è massimale.

(*ii*) L'ideale (α) è primo.

(*iii*) L'elemento α è irriducibile.

Dimostrazione. Per il paragrafo 11, basta dimostrare che *(iii)* implica *(i)*. Per definizione α non è un'unità e quindi $(\alpha) \neq R$. Supponiamo che J sia un ideale di R con

$$(\alpha) \subset J \subset R.$$

Siccome R è un anello a ideali principali, c'è un elemento $\beta \in R$ tale che $J = (\beta)$. Abbiamo $\alpha = r\beta$ per un certo $r \in R$. Siccome α è irriducibile deve essere $\beta \in R^*$ oppure $r \in R^*$. Nel primo caso abbiamo $J = R$ e nel secondo caso $J = (\alpha)$. Questo prova che (α) è massimale come richiesto. □

12.3 Corollario. In un anello a ideali principali ogni ideale primo è massimale.

Dimostrazione. Sia R un anello a ideali principali. Ogni ideale primo I di R è principale. Per il Teorema 12.2 l'ideale I è dunque massimale.

12.4 Esempi. Ogni campo è un anello a ideali principali. Per l'Esempio 9.4(*iv*) l'anello $\mathbb{Z}$ è un anello a ideali principali. Se K è un campo, l'anello $K[X]$ è, per il Teorema 10.4, un anello a ideali principali. Tutti questi anelli sono, infatti, anelli *Euclidei*. In 12.6 introduciamo questo concetto e dimostriamo che ogni anello Euclideo è un anello a ideali principali.

12.5 Esempio. L'anello $\mathbb{Z}/2\mathbb{Z}$ è un campo (8.10) e quindi $R = (\mathbb{Z}/2\mathbb{Z})[X]$ è a ideali principali (10.4). Il polinomio $f = X^2 + X + \overline{1} \in R$ è irriducibile perchè non è prodotto di polinomi lineari in R. Quindi l'ideale $I = (f)$ è massimale (12.2) e perciò l'anello quoziente $K = R/I$ è un campo (11.6). Dal Teorema 10.8 segue che gli elementi di K sono:

$$\overline{0}, \quad \overline{1}, \quad \overline{X}, \quad \overline{1+X},$$

quindi K ha quattro elementi. Si noti che $\overline{X^2+X+1}=\overline{0}$ in K implica che $\overline{X}\cdot\overline{X+1}+\overline{1}=\overline{0}$ e quindi $\overline{X}$ è l'inverso moltiplicativo di $\overline{X+1}$ in K.

12.6 Definizione. Un dominio di integrità R si dice *Euclideo* se esiste una funzione

$$N : R-\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

con la proprietà: per ogni $x, y \in R$ con $y \neq 0$ esistono $q, r \in R$ con

$$x = qy + r \qquad r = 0 \quad \text{oppure } N(r) < N(y).$$

Si dice che R è Euclideo rispetto alla funzione N.

12.7 Esempi. Ogni campo K è un anello Euclideo rispetto alla funzione

$$N : K-\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

data da $f(x) = 0$ per ogni $x \in K^*$. Infatti, si può sempre dividere x per $y \neq 0$ con quoziente $x/y \in K$ e resto 0.

Nel Teorema 1.2 abbiamo dimostrato che $\mathbb{Z}$ è un anello Euclideo rispetto alla funzione

$$N : \mathbb{Z}-\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

data da $N(x) = |x|$. La dimostrazione, data soltanto per interi positivi, si estende facilmente al caso generale.

Il Teorema 10.2 afferma che l'anello $K[X]$, dove K è un campo, è un anello Euclideo rispetto alla funzione $N(f) = \deg(f)$.

12.8 Teorema. Ogni anello Euclideo è un anello a ideali principali.

Dimostrazione. Per definizione, R è un dominio di integrità. Sia I un ideale di R. Dobbiamo dimostrare che I è principale. Se $I = \{0\}$ questo è chiaro. Se $I \neq \{0\}$, l'insieme $\{N(y) : y \in I - \{0\}\} \subset \mathbb{Z}_{\geq 0}$ non è vuoto. Sia $y \in I$ tale che $N(y)$ è minimale. Affermiamo che $I = (y)$.

Per dimostrare che $I = (y)$, sia $x \in I$ un elemento arbitrario. Dividiamo x per y con quoziente q e resto r tali che

$$x = qy + r \qquad r = 0 \quad \text{oppure } N(r) < N(y).$$

Siccome $r = x - qy$ sta in I non è possibile che $N(r) < N(y)$ e quindi abbiamo $r = 0$. Questo implica che $x = qy$, cioè $x \in (y)$ come richiesto. □

12.9 Teorema. L'anello $\mathbb{Z}[i]$ degli interi di Gauss è un anello Euclideo rispetto alla funzione

$$N(a+bi) = a^2 + b^2 \qquad (a, b \in \mathbb{Z}).$$

Dimostrazione. Definiamo per ogni $a, b \in \mathbb{R}$ la norma di $a + bi \in \mathbb{C}$ per $N(a+bi) = (a+bi)(a-bi) = a^2+b^2$. Per l'Eserc.(2.F) la norma è moltiplicativa e quindi $N(\alpha/\beta) = N(\alpha)/N(\beta)$ per $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$.

Siccome $N(0) = 0$, possiamo anche dire che l'anello $\mathbb{Z}[i]$ è Euclideo se per ogni due elementi $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, esiste $q \in \mathbb{Z}[i]$ tale che $N(\alpha - q\beta) < N(\beta)$. Dividendo adesso per $N(\beta)$ si trova che l'anello $\mathbb{Z}[i]$ è Euclideo se per ogni elemento α/β nel campo quoziente di $\mathbb{Z}[i]$ esiste un elemento $q \in \mathbb{Z}[i]$ tale che

$$N(\frac{\alpha}{\beta} - q) < 1$$

(tale $q \in \mathbb{Z}[i]$ è una buona approssimazione di $\frac{\alpha}{\beta} \in \mathbb{Q}[i]$). Scriviamo $\frac{\alpha}{\beta} = a + bi$ con $a, b \in \mathbb{Q}$. Siano $n, m \in \mathbb{Z}$ tali che $|a - m| \leq 1/2$ e $|b - n| \leq 1/2$ e definiamo $q = m + ni$. Allora $\frac{\alpha}{\beta} - q = c + di$ con $|c| \leq 1/2$ e $|d| \leq 1/2$, quindi

$$N(\frac{\alpha}{\beta} - q) = N(c + di) \leq (1/2)^2 + (1/2)^2 = 1/2 < 1,$$

come desiderato. Questo conclude la dimostrazione. □

12.10 Esempio. Sia $\alpha = 5 + 4i$ e $\beta = 1 - 2i$. Allora

$$\frac{\alpha}{\beta} = \frac{5+4i}{1-2i} = \frac{(5+4i)(1+2i)}{(1-2i)(1+2i)} = \frac{-3+14i}{5} = (-1 + \frac{2}{5}) + (3 - \frac{1}{5})i$$

quindi l'approssimazione migliore di α/β in $\mathbb{Z}[i]$ è $q = -1 + 3i$. Poi troviamo

$$r = \alpha - \beta q = 5 + 4i - (1 - 2i)(-1 + 3i) = 5 + 4i - (5 + 5i) = -i.$$

Quindi abbiamo $\alpha = \beta q + r$ e davvero $1 = N(r) < N(\beta) = (-1)^2 + 2^2 = 5$.

12.11 Per il Teorema 12.8, l'anello $\mathbb{Z}[i]$ degli interi di Gauss è anche un anello a ideali principali. Questo fatto implica il seguente teorema classico sui numeri primi.

12.12 Corollario. Sia $p \neq 2$ un numero primo. Allora $p = a^2 + b^2$ per certi interi a, b se e soltanto se $p \equiv 1 \bmod 4$.

Dimostrazione. Se $p = a^2 + b^2$, allora $(a/b)^2 \equiv -1 \bmod p$. Per la Prop.10.21 abbiamo dunque $p \equiv 1 \bmod 4$.

Viceversa, se $p \equiv 1 \bmod 4$ esiste per la Prop.10.21 un intero $z \in \mathbb{Z}$ tale che $z^2 \equiv -1 \bmod p$. Possiamo scegliere z tale che

$$-\frac{p}{2} < z < \frac{p}{2}.$$

Consideriamo l'ideale $I = (p, z - i)$ di $\mathbb{Z}[i]$. Siccome $\mathbb{Z}[i]$ è un anello a ideali principali, esiste $a + bi \in \mathbb{Z}[i]$ tale che $I = (a + bi)$. Questo implica che $a + bi$ divide sia p che $z - i$. Per la moltiplicatività della norma troviamo quindi che $N(a + bi) = a^2 + b^2$ divide sia p^2 che $z^2 + 1$. Troviamo

$$a^2 + b^2 = 1,\ p,\ \text{ oppure } p^2.$$

Siccome $a^2 + b^2$ divide $z^2 + 1$, esso è al più $p^2/4 + 1$. Dunque non è possibile che $a^2 + b^2 = p^2$. Se fosse $a^2 + b^2 = 1$, allora $(a + bi)(a - bi) = 1$ e $a + bi$ sarebbe un'unità. Questo implicherebbe

che $I = \mathbb{Z}[i]$, e quindi ci sono α, $\beta \in \mathbb{Z}[i]$ tali che $\alpha p + \beta(z - i) = 1$. Moltiplicando per $z + i$ e usando $z^2 + 1 = pk$ per un certo $k \in \mathbb{Z}$ troviamo:

$$z - i = p\alpha(z - i) + \beta(z^2 + 1) = p(\alpha(z - i) + \beta k)$$

che è una contraddizione perchè $z - i$ non è un multiplo di p. Concludiamo che $I \neq \mathbb{Z}[i]$ e quindi che $a^2 + b^2 = p$ come richiesto. □

12.13 Un *anello a fattorizzazione unica* è un anello con la proprietà che ogni elemento si può scrivere in modo unico come prodotto di elementi irriducibili. Per esempio, il Teorema Fondamentale dell'Aritmetica (Teorema 1.14) afferma che $\mathbb{Z}$ è un anello a fattorizzazione unica. La fattorizzazione di numeri interi è unica solo a meno dell'ordine dei fattori e a meno di moltiplicazione per unità. Per esempio, non si consideriano le fattorizzazioni

$$-15 = -3 \cdot 5 = 3 \cdot -5 = 5 \cdot -3 = -5 \cdot 3$$

come essenzialmente distinte. Per trattare problemi di questo tipo diamo la seguente definizione:

12.14 Definizione. Sia R un anello commutativo. Due elementi $\alpha, \beta \in R$ si dicono *associati* se esiste un'unità $\varepsilon \in R^*$ tale che

$$\alpha = \varepsilon\beta.$$

Si verifica facilmente che la relazione "essere associato è una relazione di equivalenza (Si veda l'Eserc.(12.C)).

Due elementi associati hanno le stesse proprietà di divisibilità: se α e β sono associati, allora, per ogni $\gamma \in R$, α divide γ se e soltanto se β divide γ. In questioni di divisibilità, gli elementi associati non si distinguono in modo essenziale.

12.15 Definizione. Un dominio di integrità R si dice un *anello a fattorizzazione unica* se si può scrivere ogni elemento $x \in R$, $x \neq 0$, come prodotto di un'unità e di un numero finito di elementi irriducibili:

$$x = u \cdot \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_t$$

dove $u \in R^*$, $t \in \mathbb{Z}_{\geq 0}$ e gli elementi $\pi_i \in R$, sono irriducibili (e non necessariamente distinti). Questa fattorizzazione di x è unica nel senso che per un'altra fattorizzazione

$$x = u' \cdot \pi'_1 \cdot \pi'_2 \cdot \ldots \cdot \pi'_s$$

in elementi irriducibili π'_i, si ha $s = t$ e c'è una permutazione σ di $\{1, 2, \ldots, t\}$ tale che π'_i e $\pi_{\sigma(i)}$ sono associati.

Per i domini a fattorizzazione unica vale una versione debole del Teorema 12.2:

12.16 Proposizione. Sia R un dominio a fattorizzazione unica e sia $\pi \in R$. Allora π è irriducibile se e soltanto se l'ideale (π) è primo.

Dimostrazione. Se (π) è un ideale primo, l'elemento π è automaticamente irriducibile. Supponiamo che π sia irriducibile. Siano $\beta, \gamma \in R$ con $\beta\gamma \in (\pi)$. Scriviamo β e γ come prodotto di elementi irriducibili di R. Siccome questa fattorizzazione è unica, abbiamo che π occorre nella fattorizzazione di β o di quella di γ. In altre parole $\beta \in (\pi)$ o $\gamma \in (\pi)$. □

12.17 Teorema. Un anello a ideali principali è un anello a fattorizzazione unica.

Dimostrazione. Sia R un anello a ideali principali. Supponiamo che esista un elemento $x \in R$, $x \neq 0$ non uguale a un prodotto di un'unità e di un numero finito di elementi irriducibili. Costruiamo una successione di elementi x_i di R. Sia $x_1 = x$. Ovviamente x_1 non è un'unità e non è irriducibile. Sia $x_1 = \beta_1\gamma_1$ una fattorizzazione di x_1 con $\beta_1, \gamma_1 \notin R^*$. Almeno uno degli elementi β_1, γ_1, diciamo β_1, non si può scrivere come prodotto di un'unità ed un numero finito di elementi irriducibili. Poniamo $x_2 = \beta_1$. Siccome $\gamma_1 \notin R^*$ l'ideale (x_1) è strettamente contenuto nell'ideale (x_2). Sia $x_2 = \beta_2\gamma_2$ una fattorizzazione di x con $\beta_2, \gamma_2 \notin R^*$. Almeno uno degli elementi β_2, γ_2, diciamo β_2, non si può scrivere come prodotto di un'unità ed un numero finito di elementi irriducibili. Poniamo $x_3 = \beta_2$. Siccome $\gamma_2 \notin R^*$ l'ideale (x_2) è strettamente contenuto nell'ideale (x_3). Eccetera. Così otteniamo una successione di ideali di R:

$$(x_1) \underset{\neq}{\subset} (x_2) \underset{\neq}{\subset} (x_3) \underset{\neq}{\subset} \dots$$

L'unione $I = \cup_{i=1}^{\infty}(x_i)$ è un ideale di R ed è dunque principale. Sia α un generatore. Allora α è contenuto in (x_i) per un certo indice i. Ma questo implica che $x_{i+1} \in (\alpha) \subset (x_i)$, cioè $(x_{i+1}) = (x_i)$. Questa contraddizione dimostra l'esistenza di una fattorizzazione di x in elementi irriducibili.

Dimostriamo l'unicità per induzione rispetto al numero di fattori irriducibili nella fattorizzazione: se x ammette una fattorizzazione con 0 fattori irriducibili, allora x è un'unità. Quindi, se x avesse anche una fattorizzazione

$$x = u'\pi'_1 \cdot \pi'_2 \cdot \ldots \cdot \pi'_s$$

dove $u \in R^*$ e $\pi'_i \in R$ fossero irriducibili, si avrebbe $s = 0$ e $x = u$. Questo dimostra l'unicità nel caso in cui x ha zero fattori irriducibili.

Supponiamo adesso che x abbia due fattorizzazioni:

$$\begin{aligned} x &= u\pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_t \\ &= u'\pi'_1 \cdot \pi'_2 \cdot \ldots \cdot \pi'_s, \end{aligned}$$

dove $t > 0$. Allora $u^{-1}x = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_t \in (\pi'_1)$. Siccome R è un anello a ideali principali, l'ideale (π'_1) è primo e abbiamo $\pi_i \in (\pi'_1)$ per un certo indice i. Siccome π_i è irriducibile, questo implica che

$$\pi_i = \varepsilon\pi'_1$$

per un'unità $\varepsilon \in R^*$. Adesso dividiamo le due fattorizzazioni per $\pi_i = \varepsilon\pi'_1$. Così otteniamo l'elemento x/π_i che ha una fattorizzazione con un fattore irriducibile di meno. Per ipotesi

di induzione questo elemento ha una unica fattorizzazione. Dunque anche x ha una unica fattorizzazione e la dimostrazione è completa. □

12.18 Esempi. Gli anelli $\mathbb{Z}$ e $\mathbb{Z}[i]$ sono anelli a fattorizzazione unica. Campi K ed anelli di polinomi $K[X]$ sono anelli a fattorizzazione unica. Questo segue dal fatto che tutti questi anelli sono anelli a ideali principali.

12.19 L'anello $\mathbb{Z}[\sqrt{-5}]$ non ha fattorizzazione unica. Per esempio, l'elemento $6 \in \mathbb{Z}[\sqrt{-5}]$ ha le due fattorizzazioni

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Per vedere che queste fattorizzazioni sono essenzialmente diverse, utilizziamo la norma N (si veda l'ultimo esempio del paragrafo 11). Si vede facilmente che $\varepsilon \in \mathbb{Z}[\sqrt{-5}]$ è un'unità se e soltanto se $N(\varepsilon) = 1$. Dunque, se uno degli elementi 2, 3, $1 \pm \sqrt{-5}$ non fosse irriducibile, dovrebbero esistere fattori irriducibili $a + b\sqrt{-5}$ con la norma $a^2 + 5b^2$ uguale a 2 o 3. Siccome le equazioni $a^2 + 5b^2 = 2$ e $a^2 + 5b^2 = 3$ non hanno soluzioni $a, b \in \mathbb{Z}$, tali fattori non esistono. Concludiamo che gli elementi 2, 3, $1 \pm \sqrt{-5}$ sono irriducibili.

Si ha che $N(a+b\sqrt{-5}) = a^2+5b^2 = 1$ se e soltanto se $a = \pm 1$ e $b = 0$. Dunque, le uniche unità in $\mathbb{Z}[\sqrt{-5}]$ sono ± 1. Questo implica che i fattori 2, 3 non sono uguali a $1 \pm \sqrt{-5}$ moltiplicato per un'unità. Concludiamo che le due fattorizzazioni sono distinte e l'anello $\mathbb{Z}[\sqrt{-5}]$ non ha fattorizzazione unica.

12.20 Esempio. *(Elementi irriducibili di $\mathbb{Z}[i]$)*
Determiniamo tutti gli elementi irriducibili di $\mathbb{Z}[i]$. Ogni elemento irriducibile $\pi \in \mathbb{Z}[i]$ divide $\pi\overline{\pi} \in \mathbb{Z}$. Dunque, per trovare tutti gli elementi irriducibili di $\mathbb{Z}[i]$ basta fattorizzare gli interi $n \in \mathbb{Z}$ nell'anello di Gauss. Per fare questo basta fattorizzare i numeri primi $p \in \mathbb{Z}$.

Il primo 2 si fattorizza come

$$2 = (1 + i)(1 - i) = (1 + i)(-i)(1 + i) = (-i)(1 + i)^2.$$

L'elemento $-i$ è un'unità di $\mathbb{Z}[i]$ (si veda l'Eserc.(8.L)). L'elemento $1 + i$ è irriducibile perché la norma $N(i + 1)$ è uguale a 2 (si veda l'Eserc.(12.F)).

Sia $p \equiv 1 \bmod 4$ un primo. Per il Cor.12.12, $p = a^2 + b^2$ per certi interi $a, b \in \mathbb{Z}$. In altre parole, $p = \pi\overline{\pi}$ dove $\pi = a + bi$ ha norma p ed è dunque irriducibile. Per l'Eserc.(12.F) gli elementi π e $\overline{\pi}$ non sono associati. Essi sono, dunque, elementi irriducibili essenzialmente distinti. Sia finalmente $p \equiv 3 \bmod 4$ un primo. Se p non fosse irriducibile allora $p = \beta\gamma$ con $\beta, \gamma \notin \mathbb{Z}[i]^*$. Siccome $p^2 = N(p) = N(\beta)N(\gamma)$, questo implica, per l'Eserc.(8.F), che $N(\beta) = N(\gamma) = p$. Se scriviamo $\beta = a + bi$, troviamo $p = a^2 + b^2$ contraddicendo il Cor.12.12. Dunque, p è irriducibile in $\mathbb{Z}[i]$.

Concludiamo che i soli elementi irriducibili π in $\mathbb{Z}[i]$ sono, a meno di moltiplicazione per le

unità 1, -1, i e $-i$:

$$\begin{aligned} \pi &= 1+i \\ &= p \qquad \text{dove } p \text{ è un numero primo congruo a } 3 \bmod 4, \\ &= a \pm bi \qquad \text{dove } p = a^2+b^2 \text{ è un primo congruo a } 1 \bmod 4. \end{aligned}$$

Come esempio fattorizziamo i primi piccoli $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 \ldots$. Diamo i fattori irriducibili a meno di moltiplicazione per unità. Per esempio, il numero primo 5 è uguale al prodotto $(2+i)(2-i)$ degli elementi irriducibili $2+i$ e $2-i$. Diamo soltanto $2+i$ e non gli elementi irriducibili associati $-1+2i$, $-2-i$ e $1-2i$ e diamo solo $2-i$ e non gli elementi irriducibili associati $-1-2i$, $-2+i$ e $1+2i$.

Si trovano i seguenti fattori irriducibili: $1+i$, 3, $2+i$, $2-i$, 7, 11, $3+2i$, $3-2i$, $4+i$, $4-i$, 19, 23, $5+4i$, $5-4i$, 31, $6+i$, $6-i$, $5+4i$, $5-4i$, 43, $\ldots$

Ogni elemento di $\mathbb{Z}[i]$ è un prodotto di elementi irriducibili. Per esempio

$$180 + 1992i = -i(1+i)^4 \cdot 3 \cdot (3+2i) \cdot (36-29i).$$

Il fattore $3+2i$ è un divisore di 13 e il fattore $36-29i$ è un divisore del primo 2137.

12.21 In questo paragrafo abbiamo dimostrato le implicazioni

$$\begin{array}{ccccc} \text{Anello} \\ \text{Euclideo} \end{array} \quad \Longrightarrow \quad \begin{array}{c} \text{Anello a} \\ \text{ideali} \\ \text{principali} \end{array} \quad \Longrightarrow \quad \begin{array}{c} \text{Anello a} \\ \text{fattorizzazione} \\ \text{unica} \end{array}$$

Le implicazioni nell'altra direzione sono tutte e due false. Per esempio, l'anello

$$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$$

non è Euclideo, ma è a ideali principali. Con le tecniche della teoria algebrica dei numeri è abbastanza facile costruire altri esempi di anelli con queste proprietà. Si veda l'Eserc.(12.O) e (12.P) per una dimostrazione ad hoc del fatto che l'anello $\mathbb{Z}[(1+\sqrt{-19})/2]$ non è Euclideo, ma è a ideali principali.

Nel paragrafo 13 vedremo che l'anello $\mathbb{Z}[X]$ ha fattorizzazione unica, ma non è un anello a ideali principali.

Esercizi.

(12.A) Far vedere che il polinomio $X^2+3 \in \mathbb{Q}[X]$ è irriducibile. Dimostrare che l'anello

$$\mathbb{Q}[X]/(X^2+3)$$

è un campo.

(12.B) Trovare campi con 8, 9 e 25 elementi.

(12.C) Dimostrare che l'anello $\mathbb{Z}[\sqrt{-2}]$ è un anello Euclideo rispetto alla norma $N(a+b\sqrt{-2}) = a^2 + 2b^2$. Si veda l'Eserc.(8.N) per la definizione di $\mathbb{Z}[\sqrt{-2}]$. (Sugg. Generalizzare la dimostrazione del Teorema 12.9.)

(12.D) Trovare quoziente q e resto r della divisone di $5+\sqrt{-2}$ per $2+2\sqrt{-2}$ nell'anello $\in \mathbb{Z}[\sqrt{-2}]$ tale che $N(r) < N(2+2\sqrt{-2}) = 12$.

(12.E) Calcolare $\mathrm{mcd}(4+7i, 7-9i)$. Fattorizzare $4+7i$ e $7-9i$ in fattori irriducibili in $\mathbb{Z}[i]$.

(12.F) Siano $a, b \in \mathbb{Z}$ a sia $a+bi \in \mathbb{Z}[i]$.

(i) Dimostrare che $a+bi$ è irriducibile se a^2+b^2 è primo.

(ii) Far vedere che il viceversa della parte (i) è falso.

(iii) Dimostrare che gli elementi $a+bi$ e $a-bi$ sono associati se e soltanto se $a=0$, $b=0$ oppure $a = \pm b$.

(iv) Sia $\pi \in \mathbb{Z}[i]$ un elemento irriducibile. Far vedere: se π è associato a $\overline{\pi}$ allora π è associato a $1+i$ oppure a un numero primo $p \equiv 3 \bmod 4$.

(12.G) Sia p un primo congruo a $3 \bmod 4$. Far vedere che $\mathbb{Z}[i]/(p)$ è un campo finito di ordine p^2.

(12.H) Sia $\rho \in \mathbb{C}$ uno zero del polinomio X^2+X+1. Far vedere che l'anello $\mathbb{Z}[\rho]$ è un anello Euclideo ripetto alla norma $N(x) = x\overline{x}$.

(12.I) Sia $p \neq 3$ un numero primo. Dimostrare che le seguenti affermazioni sono equivalenti:

(i) $p \equiv 1 \bmod 3$.

(ii) Esiste $z \in \mathbb{Z}$ tale che $z^2+z+1 \equiv 0 \bmod p$.

(iii) Esistono $a, b \in \mathbb{Z}$ tali che $p = a^2+ab+b^2$.

(12.J) Sia m un intero positivo che non è un quadrato, e consideriamo l'anello $\mathbb{Z}[\sqrt{m}] = \{a+b\sqrt{-m} : a, b \in \mathbb{Z}\}$ dell'Eserc.(8.N). Sia

$$N : \mathbb{Z}[\sqrt{m}] \longrightarrow \mathbb{Z}_{\geq 0}$$

la funzione definita da $N(a+b\sqrt{m}) = |(a+b\sqrt{m})(a-b\sqrt{m})| = |a^2-mb^2|$.

(i) Far vedere che $N(\alpha\beta) = N(\alpha)N(\beta)$ per ogni $\alpha, \beta \in \mathbb{Z}[\sqrt{m}]$.

(ii) Concludere che la norma N sul campo quoziente di $\mathbb{Z}[\sqrt{m}]$ data da $N(\alpha/\beta) = N(\alpha)/N(\beta)$ è ben definita.

(iii) Far vedere che per ogni $\alpha, \beta \in \mathbb{Z}[\sqrt{m}]$ con $\beta \neq 0$ esiste $\gamma \in \mathbb{Z}[\sqrt{m}]$ tale che

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < \frac{1+|m|}{4}.$$

(iv) Dimostrare che $\mathbb{Z}[\sqrt{m}]$ è Euclideo per $m = -1$, 2, -2 e 3.

Nel 1950 Chatland e Davenport hanno dimostrato che l'anello $\mathbb{Z}[\sqrt{m}]$ è Euclideo se e soltanto se $m = -2, -1, 2, 3, 6, 7, 11$ e 19. Si veda Hardy, G.H. e Wright, E.M.: *An Introduction to the Theory of Numbers*, Oxford 1968, Cap. XIV.

(12.K) Sia R un anello Euclideo rispetto alla funzione N. Definiamo

$$N^*(x) = \min\{N(yx) : y \in R - \{0\}\}.$$

Far vedere che N^* ha le proprietà

(i) $N^*(xy) \geq N^*(x)$ per ogni $x, y \in R - \{0\}$.

(ii) * Per ogni $x, y \in R$ con $y \neq 0$ esistono $q, r \in R$ con

$$x = qy + r, \qquad r = 0 \text{ oppure } N^*(r) < N^*(y).$$

(Sugg. Considerare $z \in R$ tale che il resto r_z della divisione di xz per xy ha $N(r_z)$ minimale.)

(12.L) Sia p un primo e sia $R = \{r/s \in \mathbb{Q} : p \text{ non divide } s\}$. (Si veda l'Eserc.(11.O))

(i) Dimostrare che

$$R^* = \{r/s \in R : p \text{ non divide } r\}.$$

(ii) Far vedere che si può scrivere ogni elemento $x \in R$ come

$$x = u \cdot p^k$$

dove $u \in R^*$ e $k \in \mathbb{Z}_{\geq 0}$ e questo in modo unico.

(iii) Dimostrare che R è un anello Euclideo rispetto alla norma $N(x) = k$ per $x = u \cdot p^k$ come nella parte (ii).

(12.M) Sia R un anello commutativo. Sia $R[[X]]$ *l'anello delle serie formali*:

$$R[[X]] = \left\{ \sum_{i=0}^{\infty} a_i X^i : a_i \in R \right\}.$$

Si verifica che, con l'addizione e moltiplicazione delle serie usuale, $R[[X]]$ è un'anello commutativo.

(i) Dimostrare che $f = \sum_{i=0}^{\infty} \in R[[X]]^*$ se e soltanto se $a_0 \in R^*$.

(ii) Supponiamo che R sia un campo. Sia

$$N : R[[X]] - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

la funzione data da

$$N(\sum_{i=0}^{\infty} a_i X^i) = \min\{i : a_i \neq 0\}.$$

Far vedere che $R[[X]]$ è Euclideo rispetto alla norma N.

(12.N) Sia

$$\alpha = \frac{1+\sqrt{-19}}{2} \in \mathbb{C}$$

e sia $R = \mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$ l'anello dell'Eserc.(8.O). Definiamo la norma

$$N : R \longrightarrow \mathbb{Z}_{\geq 0}$$

per

$$N(a+b\alpha) = (a+b\alpha)(a+b\overline{\alpha}) = a^2 + ab + 5b^2.$$

(i) Far vedere che $\alpha^2 - \alpha + 5 = 0$.

(ii) Far vedere che $N(xy) = N(x)N(y)$ per $x, y \in R$.

(iii) Sia $x \in R$. Far vedere che $x \in R^*$ se e soltanto se $N(x) = 1$. Concludere che $R^* = \{\pm 1\}$.

(iv) Dimostrare che non esiste un omomorfismo di anelli

$$\varphi : R \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

e non esiste neanche un omomorfismo di anelli

$$\varphi : R \longrightarrow \mathbb{Z}/3\mathbb{Z}.$$

(Sugg. Dovrebbe essere $\varphi(\alpha)^2 - \varphi(\alpha) + 5 = 0$.)

(12.O) * Lo scopo di questo esercizio è di dimostrare che l'anello $R = \mathbb{Z}[\alpha]$ dell'Eserc.(12.N) *non* è Euclideo. Supponiamo che R sia Euclideo rispetto una funzione $N : R - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$. Sia $b \in R - \{0, 1, -1\}$ con $N(b)$ minimale.

(i) Far vedere che $b \notin R^*$ e che per ogni $x \in R$ esiste $\varepsilon \in \{0, 1, -1\}$ tale che $x \equiv \varepsilon \bmod (b)$.

(ii) Far vedere che

$$R/(b) \cong \mathbb{Z}/2\mathbb{Z} \quad \text{oppure} \quad \mathbb{Z}/3\mathbb{Z}.$$

(iii) Far vedere che la conclusione della parte (ii) contraddice l'Eserc.(12.N).(iv). Concludere che R non è Euclideo.

(12.P) * Lo scopo di questo esercizio è di dimostrare che l'anello $R = \mathbb{Z}[\alpha]$ dell'Eserc.(12.N) è a ideali principali. Sia N la funzione dell'Eserc.(12.N).

(i) Siano $x, y \in R \subset \mathbb{C}$, $y \neq 0$. Far vedere che esistono quoziente e resto $q, r \in R$ tali che

$$x = qy + r, \qquad r = 0 \quad \text{oppure } N(r) < N(y)$$

se e soltanto se l'elemento $x/y \in \mathbb{C}$ è contentuto in un cerchio di raggio 1 e con centro in R. In questo caso si dice che "si può dividere x per y con resto piccolo.

(ii) Siano $x, y \in R \subset \mathbb{C}$, $y \neq 0$. Dimostrare che se *non* si può dividere x per y con resto piccolo, allora si può dividere $2x$ e uno di αx e $(1-\alpha)x$ per y con resto piccolo. (Sugg. Fare un disegno.)

(iii) Dimostrare che l'ideale $(2, \alpha)$ è uguale a R. Dimostrare che l'ideale $(2, 1-\alpha)$ è uguale a R.

(iv) Far vedere che R è un anello a ideali principali (Sugg. seguire la dimostrazione del Teorema 10.4).

(12.Q) Sia $\alpha = a + bi \in \mathbb{Z}[i]$. Far vedere che $\mathrm{ord}_p(a^2 + b^2)$ è pari per ogni primo $p \equiv 3 \bmod 4$. Concludere che si può scrivere $n \in \mathbb{Z}_{>0}$ come somma di due quadrati se e soltanto se $\mathrm{ord}_p(n)$ è pari per ogni primo $p \equiv 3 \bmod 4$.

(12.R) * Sia $n \in \mathbb{Z}$. Definiamo

$$r_2(n) = \#\{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 = n\}.$$

Dunque, $r_2(n)$ è il numero di modi distinti per scrivere n come somma di due quadrati. Per esempio $r_2(2) = 4$ perché $2 = 1^2 + 1^2 = 1^2 + (-1)^2 = (-1)^2 + 1^2 = (-1)^2 + (-1)^2$.

(i) Calcolare $r_2(64)$, $r_2(65)$, $r_2(66)$ e $r_2(67)$.

(ii) Far vedere che

$$\left(\sum_{n\in\mathbb{Z}} X^{n^2}\right)^2 = \sum_{n\in\mathbb{Z}} r_2(n) X^n$$

(iii) Dimostrare

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} r_2(n) = \pi.$$

In altre parole, il valore medio di $r_2(n)$ è $\pi = 3,1415926\ldots$.

13 Fattorizzazione di polinomi

13.1 In questo paragrafo studiamo gli anelli di polinomi con coefficienti in un dominio a fattorizzazione unica. L'anello $\mathbb{Z}[X]$ è un esempio importante. Dimostriamo che tali anelli sono anelli a fattorizzazione unica. Diamo diversi metodi per fattorizzare polinomi e per decidere se sono irriducibili o meno.

13.2 Definizione. Sia R un anello a fattorizzazione unica e sia $x \in R$, $x \neq 0$. Per un elemento irriducibile $\pi \in R$ scriviamo $\mathrm{ord}_\pi(x)$ per il numero dei fattori π che occorrono nella fattorizzazione di x.

13.3 Questa definizione generalizza quella che abbiamo dato per gli interi usuali nel Paragrafo 1. La definizione ha senso perché R è un anello a fattorizzazione unica. Si noti che $\mathrm{ord}_\pi(x) = \mathrm{ord}_{\pi'}(x)$ per ogni $x \in R - \{0\}$ se gli elementi irriducibili π e π' sono associati.

Con la Prop.1.17*(iii)* in mente, definiamo adesso il *massimo comun divisore* di due elementi $x, y \in R$:

13.4 Definizione. Sia R un anello a fattorizzazione unica e siano $x, y \in R$ elementi non nulli. Allora

$$\mathrm{mcd}(x, y) = \prod_{\pi \text{ irr.}} \pi^{\min(\mathrm{ord}_\pi(x), \mathrm{ord}_\pi(y))}$$

dove π varia fra gli elementi irriducibili di R a meno di moltiplicazione per unità. Siccome gli elementi irriducibili che occorrono nelle fattorizzazioni di x ed y sono unici solo a meno di moltiplicazione per unità, il $\mathrm{mcd}(x, y)$ di x e y dipende dalla scelta degli elementi irriducibili. *Il massimo comun divisore è soltanto ben definito a meno di moltiplicazione per unità di R.* Siccome questo fatto non è importante per questioni di divisibilità, noi non faremo caso a quest'ambiguità.

Come al solito, mettiamo $\mathrm{mcd}(0, x) = \mathrm{mcd}(x, 0) = x$ se $x \neq 0$ e definiamo il mcd di più elementi in modo induttivo: $\mathrm{mcd}(x_1, x_2, \ldots, x_t) = \mathrm{mcd}(x_1, \mathrm{mcd}(x_2, \ldots, x_t))$.

13.5 Proposizione. Sia R un dominio a fattorizzazione unica e siano $x, y \in R$ elementi non nulli. Allora

(*i*) x divide y se e soltanto se $\mathrm{ord}_\pi(x) \leq \mathrm{ord}_\pi(y)$ per ogni elemento irriducibile π.

(*ii*) per ogni $z \in R$, $z \neq 0$ si ha

$$\mathrm{mcd}(zx, zy) = z \cdot \mathrm{mcd}(x, y).$$

(*iii*) Un massimo comun divisore $\mathrm{mcd}(x, y)$ divide sia x che y. Ogni divisore comune di x e y divide $\mathrm{mcd}(x, y)$.

Dimostrazione. Facile e lasciata al lettore. □

13.6 Definizione. Sia R un dominio a fattorizzazione unica e sia

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in R[X]$$

un polinomio non nullo. Definiamo il *contenuto* $\mathrm{cont}(f)$ di f come

$$\mathrm{cont}(f) = \mathrm{mcd}(a_n, a_{n-1}, \ldots, a_1, a_0).$$

Un polinomio $f \in R[X]$ con $\mathrm{cont}(f) = 1$ si dice *primitivo*.

13.7 Esempio. Il polinomio $-2X^5 + 4X^3 - 6 \in \mathbb{Z}[X]$ ha contenuto 2 (o anche -2). Il polinomio $6X^4 - 10X + 15 \in \mathbb{Z}[X]$ è primitivo. Ogni polinomio monico in $\mathbb{Z}[X]$ è anche primitivo.

13.8 Lemma. Sia R un dominio a fattorizzazione unica e sia K il suo campo quoziente. Allora, ogni polinomio $g \in K[X]$, $g \neq 0$. si può scrivere come

$$g = c \cdot g_0$$

dove $c \in K^*$ e $g_0 \in R[X]$ è un polinomio primitivo. Questo modo di scrivere è unico a meno di moltiplicazione per unità di R.

Dimostrazione. Sia $g \in K[X]$. Siccome K è il campo quoziente di R, i coefficienti di g sono frazioni α/β dove $\alpha, \beta \in R$ e $\beta \neq 0$. Esiste dunque un elemento $\gamma \in R$, $\gamma \neq 0$, tale che il polinomio $h = \gamma \cdot g$ ha coefficienti in R. Sia $\delta = \mathrm{cont}(h)$. Per la Prop.13.5(*ii*) abbiamo che

$$h = \delta \cdot g_0$$

dove $g_0 \in R[X]$ è un polinomio primitivo. Questo implica che $g = \delta/\gamma \cdot g_0$ come richiesto.

Per dimostrare l'unicità di questo modo di scrivere, supponiamo che

$$g = c \cdot g_0 = c' \cdot g_0'$$

dove $c, c' \in K^*$ e $g_0, g_0' \in R[X]$ sono polinomi primitivi. Moltiplicando per un elemento opportuno in R possiamo assumere che $c, c' \in R - \{0\}$. A meno di moltiplicazione per unità abbiamo

$$c = \mathrm{cont}(c \cdot g_0) = \mathrm{cont}(c \cdot g_0') = c'$$

e dunque anche $g_0 = g_0'$ come richiesto. □

13.9 Lemma. Sia R un dominio a fattorizzazione unica e siano $f, g \in R[X]$ due polinomi primitivi. Allora anche il polinomio $f \cdot g$ è primitivo.

Dimostrazione. Se $f \cdot g$ non fosse primitivo, ci sarebbe un elemento irriducibile $\pi \in R$ che divide ogni coefficiente di $f \cdot g$. In altre parole

$$f \cdot g \equiv 0 \quad \text{nell'anello } R/(\pi)[X].$$

Siccome R è un dominio a fattorizzazione unica, l'ideale (π) è, per la Prop.12.16, un ideale primo. Per il Teorema 11.4, l'anello $R/(\pi)$ è dunque un dominio di integrità e per l'Eserc.(8.P) anche l'anello $R/(\pi)[X]$ è un dominio di integrità. Concludiamo che

$$f \equiv 0 \quad \text{oppure} \quad g \equiv 0 \quad \text{nell'anello } R/(\pi)[X]$$

cioè π divide $\mathrm{cont}(f)$ o $\mathrm{cont}(g)$. Questa contraddizione conclude la dimostrazione del Lemma 13.9. □

Adesso mostriamo il risultato principale di questo paragrafo.

13.10 Teorema. Se R è un dominio a fattorizzazione unica, allora anche $R[X]$ è un dominio a fattorizzazione unica.

Dimostrazione. Sia $f \in R[X]$ un polinomio non nullo e sia K il campo quoziente di R. Come primo passo dimostriamo:

Affermazione. Si può scrivere f come

$$f = u \cdot \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_s \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_t$$

dove $u \in R^*$ e $s, t \in \mathbb{Z}_{\geq 0}$, dove $\pi_1, \pi_2, \ldots, \pi_s$ sono elementi irriducibili di R e $g_1, g_2, \ldots, g_t$ sono polinomi primitivi in $R[X]$ che sono irriducibili in $K[X]$. A meno di cambiare l'ordine e di moltiplicare per unità di R questo modo di scrivere f è unico.

Dimostrazione. *(dell'affermazione.)* Siccome l'anello $K[X]$ è un anello a fattorizzazione unica, si può scrivere

$$f = \alpha \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_t$$

dove $\alpha \in K^*$ e i polinomi $g_1, g_2, \ldots, g_t \in R[X]$ sono irriducibili in $K[X]$. Per il Lemma 13.8 possiamo, cambiando α, assumere che i polinomi g_i siano primitivi. Per il Lemma 13.9 anche il prodotto $g_1 \cdot g_2 \cdot \ldots \cdot g_t$ è primitivo e quindi, per il Lemma 13.8, la costante α appartiene a R ed è uguale a $\mathrm{cont}(f)$.

Siccome R è un dominio a fattorizzazione unica, possiamo scrivere

$$\alpha = u \cdot \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_s$$

dove $u \in R^*$ e gli elementi π_i sono irriducibili in R. Questo dimostra che si può fattorizzare f nel modo richiesto. Lasciamo al lettore la verifica che questo è l'unico modo a meno di cambiare l'ordine e moltiplicare per unità in R^*.

Per concludere la dimostrazione del Teorema 13.10, basta adesso far vedere che gli elementi irriducibili di $R[X]$ sono gli elementi irriducibili di R ed i polinomi primitivi in $R[X]$ che sono irriducibili in $K[X]$.

Sia f un elemento irriducibile di $R[X]$. Siccome f non è un'unità, si conclude dall'affermazione sopra che f è uguale a un elemento irriducibile π_i di R oppure a un polinomio primitivo g_i in $R[X]$ che è irriducibile in $K[X]$.

Viceversa, sia π un elemento irriducibile di R. Se π non fosse irriducibile in $R[X]$ questo contraddirebbe l'affermazione sopra. Similmente, sia g un polinomio primitivo in $R[X]$, che è irriducibile in $K[X]$. Se g non fosse irriducibile in $R[X]$, questo contraddirebbe l'unicità della fattorizzazione affermata sopra.

Questo conclude la dimostrazione del Teorema 13.10. □

13.11 Corollario. Sia n un intero positivo. Allora

(*i*) L'anello $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ è un anello a fattorizzazione unica.

(*ii*) Per ogni campo K l'anello $K[X_1, X_2, \ldots, X_n]$ è un anello a fattorizzazione unica.

Dimostrazione. Siccome l'anello $\mathbb{Z}$ è un anello a fattorizzazione unica la prima affermazione segue dal Teorema per induzione. Ogni campo è, in modo banale, un dominio a fattorizzazione unica. Dunque anche la seconda parte segue. □

13.12 Abbiamo visto nell'Esempio 9.5 che l'ideale $(2, X) \subset \mathbb{Z}[X]$ non è principale. L'anello $\mathbb{Z}[X]$ è dunque un anello a fattorizzazione unica, ma *non* è a ideali principali. Anche l'anello $K[X, Y]$ dove K è un campo, ha questa proprietà: l'ideale (X, Y) non è principale. Però, per il Cor.13.11, l'anello $K[X, Y]$ ha fattorizzazione unica.

In anelli R di questo tipo può succedere che $\mathrm{mcd}(a, b)$ di due elementi $a, b \in R$ non generi l'ideale generato da a e b. L'ideale generato da $\mathrm{mcd}(a, b)$ contiene ovviamente a e b e quindi l'ideale (a, b), ma i due ideali sono, in generale, distinti. Per esempio, siccome gli elementi X ed Y di $\mathbb{R}[X, Y]$ sono irriducibili e distinti, abbiamo che $\mathrm{mcd}(X, Y) = 1$, ma l'ideale (X, Y) contiene esattamente i polinomi $F(X, Y) \in \mathbb{R}[X, Y]$ con $f(0, 0) = 0$. Dunque $(X, Y) \neq \mathbb{R}[X, Y]$.

Concludiamo questo paragrafo con esempi e risultati utili per fattorizzare polinomi.

13.13 Esempio. *(Fattori di grado 1.)* Sia R un dominio di integrità. Per il Teorema 10.11, un polinomio $f \in R[X]$ ha un fattore $X - \alpha$ di grado 1 se e soltanto se f ha uno zero $\alpha \in R$. Dunque, trovare fattori di grado 1 di f in $R[X]$ è equivalente a trovare zeri di f in R. Per fare questo la prossima proposizione è utile.

13.14 Proposizione. Sia R un dominio a fattorizzazione unica e sia K il campo quoziente di R. Sia

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \quad \text{in } R[X]$$

con $a_n \neq 0$ e $a_0 \neq 0$.

(*i*) Ogni zero $\alpha \in K$ di f ha la forma $\alpha = u/v$ dove $u, v \in R$ soddisfano: u divide a_0 e v divide a_n.

(*ii*) Se f è monico, allora ogni zero $\alpha \in K$ di f sta in R e divide a_0.

Dimostrazione. *(i)* Sia $\alpha \in K$ uno zero di f. Scriviamo $\alpha = u/v$ con $u/v \in R$ e $\mathrm{mcd}(u, v) = 1$. Allora

$$f = (vX - u)g$$

dove $g = b_{n-1} X^{n-1} + b_{n-2} X^{n-2} + \ldots + b_1 X + b_0 \in K[X]$. Per il Lemma 13.8, si può scrivere $g = c \cdot g_0$ dove $c \in K^*$ e $g_0 \in R[X]$ è un polinomio primitivo. Siccome $f = c(vX - u)g_0$ è in $R[X]$, deve essere $c = \mathrm{cont}(f) \in R$ e quindi $g = c \cdot g_0 \in R[X]$. Questo significa per i coefficienti di f che

$$a_n = v b_{n-1}, \qquad a_0 = -u b_0.$$

Siccome b_{n-1}, b_0 stanno in R, la parte *(i)* segue.

(ii) La parte *(ii)* è il caso speciale della parte *(i)* dove $a_n \in R^*$. □

13.15 Esempio. Per esempio, sia $f = 2X^3 + X^2 - X + 3 \in \mathbb{Z}[X]$ e sia $u/v \in \mathbb{Q}$, dove $u, v \in \mathbb{Z}$ soddisfano $\mathrm{mcd}(u, v) = 1$, uno zero di f. Per la Prop. 13.14 può essere $u = \pm 1$ oppure ± 3 e $v = 1$ oppure 2. Si verifica infatti, che $\alpha = -3/2$ è uno zero di f.

13.16 Proposizione. Sia K un campo e sia $f \in K[X]$ un polinomio di grado 2 o 3. Allora f è irriducibile in $K[X]$ se e soltanto se f non ha zeri in K.

Dimostrazione. Se fosse $f = g \cdot h$ con $g, h \in K[X]$ polinomi non costanti, allora almeno uno fra g e h avrebbe grado 1. □

13.17 La Prop.13.16 è falsa se il grado di f è più grande. Per esempio, il polinomio X^4+5X^2+9 non ha zeri in $\mathbb{Q}$, ma non è irriducibile perché

$$X^4 + 5X^2 + 9 = (X^2 + 3)^2 - X^2 \; = \; (X^2 + X + 3) \cdot (X^2 - X + 3).$$

13.18 Teorema. (Lemma di Gauss.) Sia R un dominio a fattorizzazione unica, sia K il campo quoziente di R e sia $f \in R[X]$ un polinomio primitivo. Allora f è irriducibile in $R[X]$ se e soltanto se f è irriducibile in $K[X]$.

Dimostrazione. Scriviamo f come nell'affermazione del Teorema 13.10. Visto che f è primitivo abbiamo $f = u \cdot g_1 \cdot g_2 \ldots \cdot g_t$ dove $u \in R^*$ e i $g_i \in R[X]$ sono primitivi e irriducibili in $K[X]$ e $t \geq 1$ (perchè f primitivo implica che $deg(f) > 0$). Allora f è irriducibile in $R[X]$ se e soltanto se $t = 1$ (cioè, $f = ug_1$) se e soltanto se f è irriducibile in $K[X]$. □

13.19 Esempio. Per esempio, siccome $\sqrt{2} \notin \mathbb{Z}$, il polinomio $X^2 - 2 \in \mathbb{Z}[X]$ è irriducibile. Per il Lemma di Gauss, il polinomio $X^2 - 2$ è anche irriducibile nell'anello $\mathbb{Q}[X]$. In altre parole $\sqrt{2} \notin \mathbb{Q}$.

13.20 Corollario. Sia $f \in \mathbb{Z}[X]$ un polinomio monico, supponiamo che esista un numero primo p tale che $f \bmod p \in \mathbb{Z}/p\mathbb{Z}[X]$ è irriducibile; allora f è irriducibile in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$.

Dimostrazione. Per il lemma di Gauss, f è irriducibile in $\mathbb{Q}[X]$ se e soltanto se è irriducibile in $\mathbb{Z}[X]$. Se fosse $f = g \cdot h$ con $g, h \in \mathbb{Z}[X]$, allora $f \bmod p = (g \bmod p)(h \bmod p)$ sarebbe una fattorizzazione di f in $\mathbb{Z}/p\mathbb{Z}[X]$. □

13.21 Esempio. Sia $f = X^4 + 3X^3 - X^2 - X + 27 \in \mathbb{Z}[X]$. Prendiamo $p = 2$. Il polinomio $f \bmod 2 = X^4 + X^3 + X^2 + X + 1$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$ perché non ha zeri in $\mathbb{Z}/2\mathbb{Z}$ e non è divisibile per l'unico polinomio quadratico irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$, vale a dire $X^2 + X + 1$. Concludiamo che f è irriducibile in $\mathbb{Q}[X]$.

Anche se $f \bmod p$ non è irriducibile, la fattorizzazione di $f \bmod p$ in $\mathbb{Z}/p\mathbb{Z}[X]$ può dare informazioni: sia $f = X^4 - X^2 + X + 2$. Utilizzando la Prop.13.14, si verifica che f non ha zeri in $\mathbb{Q}$. Dunque, se f fosse irriducibile, allora sarebbe il prodotto di due fattori di grado 2. Quindi sarebbe anche possibile scrivere $f \bmod 2$ come prodotto di due fattori di grado 2 in $\mathbb{Z}/2\mathbb{Z}[X]$. Ma

$$X^4 - X^2 + X + 2 = X(X^3 + X + 1) \qquad \text{in } \mathbb{Z}/2\mathbb{Z}[X]$$

dove il polinomio $X^3 + X + 1$ è irriducibile. Concludiamo che f è irriducibile in $\mathbb{Z}[X]$ e $\mathbb{Q}[X]$.

13.22 Teorema. (Criterio di Eisenstein). Sia R un dominio a fattorizzazione unica e sia π un elemento irriducibile di R. Supponiamo che

$$f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \quad \text{in } R[X]$$

sia un polinomio primitivo che soddisfa

$$\begin{array}{ll} \pi & \text{non divide } a_n, \\ \pi & \text{divide } a_k \text{ per } k = 0, 1, 2, \ldots, n-1, \\ \pi^2 & \text{non divide } a_0. \end{array}$$

Allora f è irriducibile in $R[X]$.

Dimostrazione. Supponiamo che $f = g \cdot h$ sia una fattorizzazione non banale di f in $R[X]$. Siccome f è primitivo, deve essere $\deg(g), \deg(h) > 0$. Abbiamo dunque che

$$\overline{a_n} X^n = \overline{g} \cdot \overline{h}$$

in $R/(\pi)[X]$. Siccome $\overline{a_n} \neq \overline{0}$ e siccome $R/(\pi)$ è un dominio di integrità è facile mostrare che

$$g \equiv bX^k \bmod \pi \quad \text{e} \quad h \equiv cX^{n-k} \bmod \pi$$

per certi b, $c \in R$ e $k \in \mathbb{Z}_{>0}$. In particolare, i termini noti di g ed h sono divisibili per π. Ma questo implica che π^2 divide a_0. Questa contraddizione conclude la dimostrazione. □

13.23 Esempio. Per esempio, prendiamo $R = \mathbb{Z}$ e $f = X^5 + 2X^3 - 6$. Questo polinomio è irriducibile perché si tratta di un polinomio di Eisenstein rispetto al primo 2.

Prendiamo $R = \mathbb{R}[Y]$. Il polinomio $g = X^3 + (Y^4 - 1)X - (Y^2 + 1)$ è un polinomio di Eisenstein rispetto all'elemento irriducibile $\pi = Y^2 + 1$. Concludiamo che g è irriducibile nell'anello $\mathbb{R}[X, Y]$.

13.24 Trucchi. Ci sono tanti altri trucchi per fattorizzare polinomi. Per esempio, sia $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ con $a_n, a_0 \neq 0$. Si definisce il polinomio *reciproco* $f^* = a_0 X^n + a_1 X^{n-1} + \ldots + a_{n-1}X + a_n$. Si verifica facilmente che f è irriducibile se e soltanto se f^* è irriducibile. Per esempio, il polinomio $2X^5 - 4X^2 + 3 \in \mathbb{Z}[X]$ è irriducibile perché il polinomio reciproco è di Eisenstein rispetto al primo 2.

Sia K è un campo e siano $a, b \in K$, $a \neq 0$. Sia $f \in K[X]$, allora, per l'Eserc.(13.N), il polinomio $g(X) = f(aX + b)$ è irriducibile se e soltanto se f è irriducibile. Per esempio, il polinomio

$$f = X^5 + 2X^4 + 3X^3 + 4X^2 + 5X + 6 \quad \text{in } \mathbb{Q}[X]$$

è irriducibile perchè il polinomio

$$f(X + 1) = X^5 + 7X^4 + 21X^3 + 35X^2 + 35X + 21$$

è di Eisenstein rispetto a 7.

13.25 Se non si riesce a utilizzare uno dei metodi sopra, si può, per fattorizzare $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, scrivere che $f = (b_mX^m + \ldots + b_1X + b_0)(c_{n-m}X^{n-m} + \ldots + c_1X + c_0)$ e risolvere le equazioni dei coefficienti. Per esempio, supponiamo che $f \in \mathbb{Z}[X]$ sia un polinomio primitivo di grado 4 e che si sia già verificato, utilizzando la Prop.13.14, che f non ha zeri in $\mathbb{Q}$, allora si scrive

$$f = (b_2X^2 + b_1X + b_0)(c_2X^2 + c_1X + c_0)$$

e si risolvono le equazioni

$$\begin{aligned} b_2c_2 &= a_4, \\ b_2c_1 + b_1c_2 &= a_3, \\ b_2c_0 + b_1c_1 + b_0c_2 &= a_2, \\ b_1c_0 + b_0c_1 &= a_1, \\ b_0c_0 &= a_0. \end{aligned}$$

C'è soltanto un numero *finito* di possibilità per $b_2, c_2, b_0, c_0 \in \mathbb{Z}$ e dunque un numero finito di possibilità per il prodotto c_1b_1 e dunque per c_1 e b_1 ecc. Questo metodo è laborioso, ma, almeno nel caso dove $\deg(f) = 4$, dà la fattorizzazione di f in un numero finito di passi.

Esercizi.

(13.A) Sia R un dominio a fattorizzazione unica. Definiamo il *minimo comun multiplo* $\mathrm{mcm}(x, y)$ di $x, y \in R - \{0\}$ come

$$\mathrm{mcm}(x, y) = \prod_{\pi \text{ irr.}} \pi^{\max(\mathrm{ord}_\pi(x), \mathrm{ord}_\pi(y))},$$

dove π varia fra gli elementi irriducibili a meno di moltiplicazione per unità. Siano $x, y \in R - \{0\}$. Far vedere che xy e $\mathrm{mcm}(x, y) \cdot \mathrm{mcd}(x, y)$ sono elementi associati in R.

(13.B) (i) Determinare $\mathrm{cont}(f)$ di $f = 2X^3 - 4/3 \in \mathbb{Q}[X]$.

(ii) Sia $g(X, Y) = XY^2 + X^2Y + YX \in \mathbb{R}[X, Y]$. Calcolare il contenuto di g considerato come polinomio in X e coefficienti in $\mathbb{R}[Y]$. Calcolare il contenuto di g considerato come polinomio in Y e coefficienti in $\mathbb{R}[X]$.

(13.C) Dimostrare che $X^n - 3$ è irriducibile in $\mathbb{Z}[X]$ per ogni $n \in \mathbb{Z}_{>0}$.

(13.D) Fattorizzare i polinomi $X^8 - 16$ e $X^6 + 27$ in fattori irriducibili in $\mathbb{Q}[X]$.

(13.E) Sia p un primo.

(i) Far vedere che il polinomio

$$X^{p-1} + X^{p-2} + \ldots + X + 1$$

è irriducibile in $\mathbb{Q}[X]$.

(ii) Far vedere che il polinomio

$$\frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}$$

è irriducibile in $\mathbb{Q}[X]$ per ogni $n \in \mathbb{Z}_{\geq 1}$.

(13.F) Il polinomio $5X^4 + 10X + 10$ è di Eisenstein? È irriducibile in $\mathbb{Q}[X]$? In $\mathbb{Z}[X]$?

(13.G) (i) Trovare un polinomio irriducibile $f(X) \in \mathbb{Z}[X]$ tale che $f(X^2)$ non è irriducibile.

(ii) Sia $f \in \mathbb{Z}[X]$ un polinomio di Eisenstein. Far vedere che $f(X^2)$ è irriducibile in $\mathbb{Z}[X]$.

(13.H) Fattorizzare i seguenti polinomi in fattori irriducibili in $\mathbb{Q}[X]$ e in $\mathbb{Z}[X]$:

$$4X^2 + 4,$$
$$2X^{10} + 4X^5 + 3,$$
$$X^4 - 7X^2 + 5X - 3,$$
$$X^{111} + 9X^{74} + 27X^{37} + 27,$$
$$X^3 + X + 3.$$

(13.I) Fattorizzare i seguenti polinomi in fattori irriducibili in $\mathbb{Q}[X]$ e in $\mathbb{Z}[X]$:

$$\tfrac{1}{7}((X+1)^7 - X^7 - 1),$$
$$X^3 + 3X^2 + 6X + 9,$$
$$X^4 + 2X^3 + 3X^2 + 9X + 6,$$
$$X^{12} - 1,$$
$$X^4 - X^3 + X^2 - X + 1.$$

(13.J) Fattorizzare i seguenti polinomi in fattori irriducibili in $\mathbb{Q}[X, Y]$:

$$Y^4 + X^2 + 1,$$
$$Y^3 - (X+1)Y^2 + Y + X(X-1),$$
$$X^n + Y^3 + Y \qquad (n \geq 1),$$
$$X^4 + 4Y^4,$$
$$X^4 + 2X^3 + X^2 - Y^2 - 2Y - 1,$$
$$Y^n - 13X^4 \qquad (n \geq 1).$$

(13.K) Determinare tutti i polinomi irriducibili di grado al più 3 in $\mathbb{Z}/2\mathbb{Z}[X]$.

(13.L) Per ciascuno degli anelli

$$\mathbb{Z}[X], \quad \mathbb{Q}[X], \quad \mathbb{R}[X], \quad \mathbb{Z}/11\mathbb{Z}[X]$$

decidere se l'ideale generato da $(X^2 - 3)$ è massimale e se è primo.

(13.M) Provare che il polinomio $X^3 + X + 1$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$. Dimostrare che l'anello

$$\mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1)$$

è un campo. Quanti elementi ha questo campo?

(13.N) Sia R un dominio di integrità e siano $a \in R^*$ e $b \in R$.

(i) Far vedere che la mappa $\varphi : R[X] \longrightarrow R[X]$ data da

$$\varphi(f(X)) = f(aX + b)$$

è un isomorfismo di anelli.

(ii) Dimostrare che f è irriducibile in $R[X]$ se e soltanto se $f(aX + b)$ è irriducibile.

14 Campi

In questo paragrafo studiamo la teoria generale dei *campi*. Il risultato principale è il Teorema 14.18 che afferma l'esistenza e unicità, a meno di isomorfismo, di un *campo di spezzamento* di un polinomio f con coefficienti in un campo K. Questo risultato un po' tecnico ci servirà nei prossimi paragrafi.

Un omomorfismo di campi è semplicemente un omomorfismo di anelli. Per il Cor.9.7 ogni omomorfismo $f : K \longrightarrow L$ di campi è iniettivo. La mappa f induce una biiezione fra K e $f(K)$. Si verifica facilmente che $f(K)$ è un *sottocampo* di L, cioè un sottoanello che è un campo. Spesso si identifica K con il sottoinsieme $f(K)$ di L e si guarda f come un'inclusione. Se K è un sottocampo di L si dice anche che L è una *estensione* di K.

Sia K un campo. Si verifica facilmente che l'intersezione di due sottocampi di K è ancora un sottocampo di K. Ecco perché esiste un *campo primo* di K, cioè un sottocampo minimale che è contenuto in ogni sottocampo di K. Ci sono soltanto poche possibilità per la struttura dei campi primi.

14.1 Proposizione. Ogni campo primo è isomorfo a $\mathbb{Q}$ oppure a $\mathbb{Z}/p\mathbb{Z}$ per un numero primo p.

Dimostrazione. Sia K un campo. Consideriamo l'omomorfismo dell'Esempio 9.2(v):

$$\varphi : \mathbb{Z} \longrightarrow K$$

dato da $\varphi(m) = m$. Siccome ogni sottocampo di K contiene l'elemento identico, deve anche contenere l'immagine di φ. Adesso ci sono due possibilità:
(1) La mappa φ non è iniettiva. Allora c'è un intero $n \neq 0$ tale che $n\mathbb{Z}$ è il nucleo di φ. Per il Primo Teorema di Isomorfismo abbiamo che

$$\mathbb{Z}/n\mathbb{Z} \cong \varphi(\mathbb{Z}) \subset K.$$

Siccome K è un campo, non contiene divisori di 0. Questo implica che n deve essere primo. Per la Prop.8.10, l'anello $\mathbb{Z}/n\mathbb{Z}$ è un campo se n è primo. Quindi esso è il campo primo di K.
(2) La mappa φ è iniettiva. Definiamo

$$\Phi : \mathbb{Q} \longrightarrow K$$

per $\Phi(a/b) = \varphi(a)/\varphi(b)$ per $a, b \in \mathbb{Z}$, $b \neq 0$. Lasciamo al lettore la verifica che Φ è un omomorfismo ben definito. L'immagine di Φ è contenuta in ogni sottocampo di K. Siccome $\mathbb{Q}$ è un campo, Φ è iniettiva e $\Phi(\mathbb{Q})$ è un sottocampo di K isomorfo a $\mathbb{Q}$. Concludiamo che questo sottocampo è il campo primo di K, come richiesto. □

14.2 La caratteristica. La *caratteristica* $\mathrm{car}(K)$ di un campo K si dice p se il campo primo di K è isomorfo a $\mathbb{Z}/p\mathbb{Z}$. La caratteristica si dice 0 se il campo primo è isomorfo a $\mathbb{Q}$. Ogni campo di caratteristica p ammette un omomorfismo speciale:

14.3 Proposizione. Sia K un campo di caratteristica p. Allora la mappa $F : K \longrightarrow K$ data da

$$F(x) = x^p \qquad \text{per } x \in K$$

è un omomorfismo.

Dimostrazione. Ovviamente $F(1) = 1$. Siano $x, y \in K$. Siccome K è commutativo, si ha $F(xy) = F(x)F(y)$. Poi

$$F(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p = F(x) + F(y)$$

perché i coefficienti binominali soddisfano

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{i!}$$

e sono dunque, per $1 \leq i \leq p-1$, divisibili per p. Questo conclude la dimostrazione. □

14.4 Il Frobenius. L'omomorfismo F si dice l'*omomorfismo di Frobenius*. La mappa F è sempre iniettiva. Se F è suriettiva il campo K si dice *perfetto*. Anche i campi di caratteristica zero si dicono perfetti.

14.5 Spazi vettoriali. Uno *spazio vettoriale V su K* è un gruppo additivo (e quindi commutativo) fornito di una moltiplicazione $K \times V \longrightarrow V$ per elementi di K: per ogni $\lambda \in K$ ed ogni $\mathbf{v} \in V$ è definito il vettore $\lambda\mathbf{v} \in V$ tale che

(V_1) Per ogni $\lambda \in K$ e per ogni $\mathbf{v}, \mathbf{w} \in V$

$$\lambda(\mathbf{v} + \mathbf{w}) = \lambda\mathbf{v} + \lambda\mathbf{w}.$$

(V_2) Per ogni $\lambda, \mu \in K$ e per ogni $\mathbf{v} \in V$

$$(\lambda + \mu)\mathbf{v} = \lambda\mathbf{v} + \mu\mathbf{v}.$$

(V_3) Per ogni $\lambda, \mu \in K$ e per ogni $\mathbf{v} \in V$

$$(\lambda\mu)\mathbf{v} = \lambda(\mu\mathbf{v}).$$

(V_4) Per ogni $\mathbf{v} \in V$

$$1 \cdot \mathbf{v} = \mathbf{v}.$$

Ogni spazio vettoriale possiede una base $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \ldots \in V$ tale che per ogni $\mathbf{v} \in V$ esistono unici $\lambda_1, \lambda_2, \ldots \in K$ tali che

$$\mathbf{v} = \lambda_1\mathbf{e}_1 + \lambda_2\mathbf{e}_2 + \lambda_3\mathbf{e}_3 + \ldots$$

La cardinalità di una base dipende soltanto da V e si dice la *dimensione* $\dim_K(V)$ dello spazio. Per le dimostrazioni delle proprietà degli spazi vettoriali si veda il corso di Geometria I o un testo di algebra lineare.

Sia K un campo e sia L un'estensione di K. Utilizzando l'usuale moltiplicazione in L diamo a L la struttura di uno spazio vettoriale su K. Dagli assiomi dell'associatività e della distributività della moltiplicazione in L seguono gli assiomi (V_1), ..., (V_4).

14.6 Definizione. Siano $K \subset L$ campi. Il *grado* $[L : K]$ di L su K è definito come

$$[L : K] = \dim_K(L).$$

Se $[L : K]$ è finito, si dice che L *è un'estensione finita di* K.

14.7 Esempio. Per esempio, $\mathbf{e}_1 = 1$ e $\mathbf{e}_2 = i$ è una base di $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ come spazio vettoriale su $\mathbb{R}$. Dunque $\mathbb{C}$ è uno spazio vettoriale su $\mathbb{R}$ di dimensione 2 e $[\mathbb{C} : \mathbb{R}] = 2$.

14.8 Proposizione. Siano $K \subset F \subset L$ tre campi. Allora

$$[L : K] = [L : F][F : K].$$

Dimostrazione. Supponiamo che $d = [F : K] = \dim_K(F)$ e $e = [L : F] = \dim_F(L)$ siano finiti. Abbiamo dunque isomorfismi di spazi vettoriali: $F \cong K^d$ e $L \cong F^e$. Allora $L \cong (F^e)^d \cong F^{de}$ come spazi vettoriali su F. Se la dimensione d o e è infinita, si vede facilmente che anche $[L : K]$ è infinito. Questo conclude la dimostrazione. □

14.9 Definizione. Sia $K \subset L$ un'estensione di campi e sia $\alpha \in L$. Definiamo

$$K[\alpha] = \left\{ \sum_{i=0}^{<\infty} a_i \alpha^i : a_i \in K \right\},$$

$$K(\alpha) = \text{il più piccolo sottocampo di } L \text{ che contiene sia } K \text{ che } \alpha.$$

Si noti che $K[\alpha]$ è un sottoanello di L e di $K(\alpha)$. Più generalmente, si definisce per $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, il campo $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ come il più piccolo campo che contiene K e gli elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$.

14.10 Definizione. Sia $K \subset L$ un'estensione di campi e sia $\alpha \in L$. L'elemento α si dice *algebrico su* K se esiste un polinomio $f \in K[X]$, $f \neq 0$ tale che $f(\alpha) = 0$. Una estensione L di K si dice *algebrica* se ogni $\alpha \in L$ è algebrico su K. Un elemento non algebrico si dice *trascendente*.

14.11 Teorema. Sia K un campo e sia L un'estensione di K.

(*i*) Se il grado $[L : K]$ di L su K è finito, ogni elemento di L è algebrico su K.

(*ii*) Se $\alpha \in L$ è algebrico su K allora l'anello $K[\alpha]$ è un campo, $K[\alpha] = K(\alpha)$ e $[K(\alpha) : K]$ è finito.

Dimostrazione. *(i)* Sia $d = [L : K]$, la dimensione di L come spazio vettoriale su K. Allora per $\alpha \in L$ i $d+1$ "vettori $1, \alpha, \alpha^2, \ldots, \alpha^d$ sono necessariamente dipendenti. Esistono dunque a_0, $a_1, \ldots,$ a_d in K, non tutti nulli, tali che

$$a_0 + a_1\alpha + \ldots + a_d\alpha^d = 0.$$

In altre parole, il polinomio

$$f = a_d X^d + \ldots + a_1 X + a_0 \qquad (\in K[X])$$

non è nullo e soddisfa $f(\alpha) = 0$, quindi α è algebrico su K.
(ii) Si considera l'omomorfismo

$$\Phi : K[X] \longrightarrow L, \qquad \Phi(g) = g(\alpha).$$

L'immagine $\mathrm{im}(\Phi)$ di Φ è il sottoanello $K[\alpha]$ di L, per definizione di $K[\alpha]$. Siccome K è un campo, $K[X]$ è un anello a ideali principali per il Teorema 10.4, e quindi $\ker(\Phi) = (f)$ per un certo $f \in K[X]$. Dato che α è algebrico, $\ker(\Phi) \neq 0$ e quindi $f \neq 0$. Per il primo Teorema di isomorfismo 9.14,

$$K[\alpha] = \mathrm{im}(\Phi) \cong K[X]/\ker(\Phi) = K[X]/(f).$$

Visto che $K[\alpha]$ è un sottoanello del campo L, $K[\alpha]$ è un dominio. Essendo $K[\alpha]$ un dominio, l'ideale (f) è primo nell'anello a ideali principali $K[X]$ e quindi f è irriducibile per 12.2. Allora l'anello $K[\alpha] \cong K[X]/(f)$ è un campo perchè, sempre per 12.2, (f) è un ideale massimale in $K[X]$. Per definizione di $K(\alpha)$ abbiamo allora che $K(\alpha) = K[\alpha]$. La dimensione di $K[\alpha]$ su K è finito perchè dal Teorema 10.8 segue che una K-base di $K[\alpha]$ è dato da $\overline{1}$, $\overline{X}$, ..., $\overline{X^{d-1}}$ dove $d = deg(f)$. □

14.12 Corollario. Sia K un campo e sia L un'estensione di K. Allora l'insieme degli elementi in L che sono algebrici su K è un sottocampo di L che contiene K.

Dimostrazione. Sia F l'insieme degli elementi in L che sono algebrici su K. Ovviamente $K \subset F$. Sia $\alpha \in F$, allora il campo $K(\alpha)$ ha grado finito su K per 14.11(*ii*). Siccome $K(\alpha) = K(-\alpha) = K(1/\alpha)$ concludiamo che gli elementi $-\alpha$ e $1/\alpha$ sono algebrici su K per 14.11(*i*).

Siano α, $\beta \in F$. Allora $K(\alpha)$ ha grado finito su K. Siccome β è algebrico su K, questo elemento è, a fortiori, algebrico su $K(\alpha)$. Questo implica che la dimensione di $K(\alpha)(\beta)$ come spazio vettoriale su $K(\alpha)$ è finita. Quindi anche la dimensione di $K(\alpha)(\beta)$ come spazio vettoriale su K è finita. Siccome la somma $\alpha + \beta$ ed il prodotto $\alpha\beta$ sono elementi di $K(\alpha)(\beta)$, i campi $K(\alpha+\beta)$ e $K(\alpha\beta)$ hanno grado finito. Per il Teorema 14.11(*ii*) abbiamo dunque $\alpha+\beta$, $\alpha\beta \in F$. Adesso si conclude facilmente che F è un campo. □

14.13 Il campo

$$\{\alpha \in \mathbb{C} : \alpha \text{ è algebrico su } \mathbb{Q}\}$$

si dice semplicemente *il campo dei numeri algebrici.* Gli elementi si dicono spesso *numeri algebrici.* Esempi di numeri algebrici sono $\sqrt{2}$, $\sqrt[6]{-33}$, $\sqrt[8]{5} - 1/9 + 5^{-1/5}$ .... Con tecniche della teoria degli insiemi si sa dimostrare che, in un senso preciso, quasi tutti i numeri complessi sono trascendenti. Questo dimostrò Cantor nel 1873. Per la dimostrazione facile si veda il libro di P. Halmos: *Teoria elementare degli insiemi*, Feltrinelli, Milano 1970. È molto più difficile dimostrare che un numero specificamente dato sia trascendente o meno. Il matematico Francese Hermite dimostrò nel 1873 che il numero $e = 2,71828182845\ldots$ è trascendente. Nel 1882 Lindemann dimostrò che $\pi = 3,14159265358\ldots$ è trascendente. Il suo risultato implicava l'impossibilità della famosa "quadratura del cerchio. Si veda il libro di Ian Stewart: *Galois Theory*, Chapman and Hall, London New York 1989.

14.14 Il polinomio minimo. Sia K un campo e sia α un elemento algebrico su K, contenuto in un'estensione L di K. Mostriamo che esiste un polinomio irriducibile $f \in K[X]$ tale che $f(\alpha) = 0$. Esiste dunque, anche un polinomio *monico* con questa proprietà. Questo polinomio monico è unico e si dice il *polinomio minimo di α (rispetto a K).* Notazione: $f^{\alpha}_{\min}$ oppure $f^{\alpha}_{\min,K}$.

14.15 Teorema. Sia K un campo e sia L un'estensione di K. Sia $\alpha \in L$ algebrico su K. Allora esiste un unico polinomio monico irriducibile, scritto $f^{\alpha}_{\min}$, in $K[X]$ tale che $f^{\alpha}_{\min}(\alpha) = 0$.

In più:

$$K[X]/(f^{\alpha}_{\min}) \cong K(\alpha), \qquad \deg(f_{\min}) = [K(\alpha) : K].$$

Dimostrazione. Nella dimostrazione del Teorema 14.11(*ii*) abbiamo visto che il nucleo dell'omomorfismo $\Phi : K[X] \to L$ con $\Phi(g) = g(\alpha)$ è generato da un polinomio irriducibile f.

Se $g \in K[X]$ è un polinomio irriducibile tale che $g(\alpha) = 0$ allora $g \in \ker(\Phi) = (f)$ e perciò $g = hf$ per un certo $h \in K[X]$. Dato che f e g sono irriducibili, h è un unità, cioè $h \in K^*$. L'unicità del polinomio minimo segue adesso del fatto che questo deve anche essere monico. Il resto segue dal Teorema 14.11(*ii*) e dal fatto che $(f^{\alpha}_{\min}) = (f)$. □

14.16 Esempio. Sia $\beta \in \mathbb{R}$ con $\beta^3 = -2$ e sia $L = \mathbb{Q}(\beta)$. Visto che β è uno zero di $g = X^3 + 2 \in \mathbb{Q}[X]$ e che g è irriducibile (Criterio di Eisenstein per $p = 2$) e è monico, concludiamo che $g = f^{\beta}_{\min}$ e che $[L : \mathbb{Q}] = 3$. Una $\mathbb{Q}$-base dello spazio vettoriale L su $\mathbb{Q}$ è data da 1, β e β^2.

Sia $\alpha = \beta^2 + 1$. Per determinare il polinomio minimo $f^{\alpha}_{\min}$ di α consideriamo, come nella dimostrazione di 14.11(*i*), le potenze $\alpha^0 = 1$, $\alpha^1 = 1 + \beta^2, \alpha^2$, α^3. Dato che $[L : \mathbb{Q}] = 3$, questi quattro elementi sono linearmente dipendenti su $\mathbb{Q}$. Si ha:

$$\alpha^2 = \beta^4 + 2\beta^2 + 1 = 2\beta^2 - 2\beta + 1, \qquad \alpha^3 = \beta^6 + 3\beta^4 + 3\beta^2 + 1 = 3\beta^2 - 6\beta + 5.$$

Quindi vale la relazione lineare tra le potenze di α:

$$\alpha^3 - 3\alpha^2 + 3\alpha - 5 = 0$$

e α è dunque uno zero di $f = X^3 - 3X^2 + 3X - 5$.

Per mostrare che $f = f^{\alpha}_{\min}$, basta adesso mostrare che f è irriducibile in $\mathbb{Q}[X]$. Visto che f ha grado 3 questo vale se f non ha zeri in $\mathbb{Q}$. Usando 13.14, basta verificare che ± 1, ± 5 non sono zeri di f, che è facile.

14.17 Consideriamo ora un polinomio $f \in K[X]$ e cerchiamo un'estensione di K nel quale f abbia zeri. Se f è irriducibile e $\deg(f) > 1$, allora f non ha fattori lineari in $K[X]$ e quindi non ha zeri in K. D'altra parte, siccome f è irriducibile, l'ideale (f) è massimale in $K[X]$ per 10.4 e 12.2 e perciò $K[X]/(f)$ è un campo. Mostriamo in 14.18 che f ha uno zero proprio in questo campo! Trovare un campo che contiene tutti gli zeri di f poi non è molto difficile.

14.18 Teorema. Sia $f \in K[X]$ un polinomio irriducibile e sia $I = (f)$ l'ideale di $K[X]$ generato da f. Allora:

(*i*) il campo $L = K[X]/I$ è un'estensione di K e $[L : K] = \deg(f)$,

(*ii*) l'elemento $\alpha = X + I \in L$ è uno zero di f e $L = K(\alpha)$.

Dimostrazione. La composizione dell'inclusione $K \hookrightarrow K[X]$ e dalla mappa canonica $K[X] \to L$ è un omomorfismo $K \to L$ che è iniettivo per 9.7(*ii*). Quindi l'immagine è un sottocampo

di L, isomorfo a K, e questo permette di vedere L come estensione di K. Si noti che $a \in K$ corrisponde a $a + I \in L$. L'Esercizio (14.G) mostra che $[L : K] = \deg(f)$.

Sia $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in K[X]$. Siccome $K \hookrightarrow L$ è dato da $a \mapsto a + I$, dobbiamo mostrare che

$$f(\alpha) = (a_n + I)(X + I)^n + (a_{n-1} + I)(X + I)^{n-1} + \ldots + (a_0 + I)$$

è zero nel campo L. Usando la definizione del prodotto in un anello quoziente, $(x+I)(y+I) = xy+I$, otteniamo $(X+I)^2 = X^2+I$, ..., $(X+I)^n = X^n+I$ e poi $(a_i+I)(X^i+I) = a_i X^i + I$, quindi rimane da mostrare che

$$(a_n X^n + I) + (a_{n-1} X^{n-1} + I) + \ldots + (a_0 + I)$$

è zero in L. La definizione di addizione in un anello quoziente è $(x + I) + (y + I) = x + y + I$, quindi

$$f(\alpha) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 + I = f + I.$$

Visto che $f \in I = (f)$, abbiamo $f + I = 0 + I$ in $K[X]/I$, quindi $f(\alpha) = 0$ in L come desiderato. Questo conclude la dimostrazione del Teorema 14.18. □

14.19 Esempio. Sia $f = X^2 + 1 \in \mathbb{R}[X]$. Come abbiamo visto nella Proposizione 10.6, $\mathbb{R}[X]/(f) \cong \mathbb{C}$. Questo isomorfismo è ottenuto dall'omomorfismo $\Phi : \mathbb{R}[X] \to \mathbb{C}$, $g \mapsto g(i)$. Quindi $\alpha = X + (f) \in \mathbb{R}[X]/(f)$ corrisponde a $i \in \mathbb{C}$ e i è uno zero di f.

14.20 Definizione. Sia K un campo e sia $f \in K[X]$ un polinomio non nullo. Un'estensione L di K si dice *un campo di spezzamento* di f rispetto a K se

(*i*) esistono $\alpha_1, \alpha_2, \ldots, \alpha_d$ e $c \in L$ tali che

$$f = c(X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_d) \qquad \text{in } L[X],$$

(*ii*) $L = K(\alpha_1, \alpha_2, \ldots, \alpha_d)$.

14.21 Teorema. Sia K un campo. Per ogni $f \in K[X]$, $f \neq 0$, esiste un campo di spezzamento. Questo campo è unico a meno di K-isomorfismi, cioè, se L e L' sono due campi di spezzamento di f, allora esiste un isomorfismo di campi

$$\sigma : L \longrightarrow L'$$

che, ristretto a K, è l'applicazione identica.

Dimostrazione. Prima proviamo *l'esistenza* di un campo di spezzamento per induzione rispetto al grado di f. Se $\deg(f) = 1$, allora $f = X - \alpha$ con $\alpha \in K$. In questo caso il campo di spezzamento è K. Se $\deg(f) = d > 1$, consideriamo due possibilità:

(1) Il polinomio f non è irriducibile. Allora $f = g \cdot h$ in $K[X]$ con $\deg(g), \deg(h) < d$. Per l'ipotesi di induzione, esiste un campo di spezzamento F di g rispetto a K. Poi consideriamo $h \in K[X] \subset F[X]$ e, per induzione, il campo di spezzamento L di h rispetto a F. Affermiamo che L è anche il campo di spezzamento di f rispetto a K: se

$$g = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_e)$$

dove $\alpha_1, \ldots, \alpha_e \in F$ e

$$h = (X - \alpha_{e+1}) \cdot \ldots \cdot (X - \alpha_d)$$

dove $\alpha_{e+1}, \ldots, \alpha_d \in L$, allora

$$f = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_e)(X - \alpha_{e+1}) \cdot \ldots \cdot (X - \alpha_d)$$

e $L = F(\alpha_{e+1}, \ldots, \alpha_d) = K(\alpha_1, \ldots, \alpha_e, \alpha_{e+1}, \ldots, \alpha_d)$ come richiesto.

(2) Il polinomio f è irriducibile. Allora l'anello

$$F = K[X]/(f)$$

è un campo. Per costruzione, l'elemento $\alpha = \overline{X} = X + (f) \in F$ soddisfa $f(\alpha) = 0$ e quindi, f è il polinomio minimo di α. Per la Prop.14.15 abbiamo $K(\alpha) \subset F$.

Dividiamo f per $X - \alpha$:

$$f(X) = (X - \alpha) f_1(X)$$

in $F[X]$. Il grado di f_1 è $d - 1$. Esiste dunque, per induzione, un campo di spezzamento L di f_1 rispetto al campo F: siano $\alpha_1, \ldots, \alpha_{d-1} \in L$ gli zeri di f_1 in L. Allora

$$L = F(\alpha_1, \ldots, \alpha_{d-1}) = K(\alpha, \alpha_1, \ldots, \alpha_{d-1}).$$

Questo prova che L è un campo di spezzamento per f.

Per mostrare *l'unicità* del campo di spezzamento, a meno di isomorfismi, dimostriamo il seguente fatto più generale:

Affermazione. *Siano K_1 e K_2 due campi e sia $\sigma : K_1 \longrightarrow K_2$ un isomorfismo di campi. Sia $f_1 = a_d X^d + \ldots + a_1 X + a_0 \in K_1[X]$ e sia L_1 un campo di spezzamento di f_1 rispetto a K_1. Sia L_2 un campo di spezzamento del polinomio $f_2 = \sigma(a_d) X^d + \ldots + \sigma(a_1) X + \sigma(a_0) \in K_2[X]$ rispetto a K_2. Allora esiste un isomorfismo $\tau : L_1 \longrightarrow L_2$ tale che τ ristretto a K_1 è σ.*

Un'applicazione dell'affermazione al caso $K = K_1 = K_2$ e $\sigma = \mathrm{id}_K$ dimostra il teorema. Basta quindi dimostrare l'affermazione:

Dimostrazione. *(dell'affermazione.)* Diamo la dimostrazione per induzione rispetto al grado di f_1. Per un polinomio $h = b_m X^m + \ldots + b_1 X + b_0 \in K_1[X]$, intendiamo con $\sigma(h) \in K_2[X]$ il polinomio $\sigma(b_m) X^m + \ldots + \sigma(b_1) X + \sigma(b_0)$.

Se f_1 ha grado 1, anche f_2 ha grado 1 e dunque $L_1 = K_1$ e $L_2 = K_2$. Prendiamo dunque $\tau = \sigma$. Sia $\deg(f_1) > 1$ e sia $g_1 \in K_1[X]$ un fattore irriducibile di f_1. Sia $\alpha_1 \in L_1$ uno zero di g_1. Applicando l'isomorfismo σ, troviamo $g_2 = \sigma(g_1) \in K_2[X]$ un fattore irriducibile di $f_2 = \sigma(f_1)$ e uno zero $\alpha_2 = \sigma(\alpha_1) \in L_2$.

Si verifica facilmente che la mappa

$$K_1[X]/(f_1) \longrightarrow K_2[X]/(f_2)$$

data da $h \mapsto \sigma(h)$ è un isomorfismo, che, ristretto a K_1 è semplicemente σ. Abbiamo dunque un isomorfismo

$$\sigma' : K_1(\alpha_1) = K_1[\alpha_1] \xrightarrow{\cong} K_1[X]/(f_1) \xrightarrow{\cong} K_2[X]/(f_2) \xrightarrow{\cong} K_2[\alpha_2] = K_2(\alpha_2).$$

Ristretto a K_1, questo isomorfismo è uguale a σ.

$$\begin{array}{ccc} L_1 & & L_2 \\ \cup & & \cup \\ K_1(\alpha_1) & \xrightarrow{\sigma'} & K_2(\alpha_2) \\ \cup & & \cup \\ K_1 & \xrightarrow{\sigma} & K_2 \end{array}$$

Adesso si applica l'ipotesi di induzione con $K_1(\alpha_1)$ per il campo K_1 e $f_1/(X-\alpha_1)$ per il polinomio f_1; e con $K_2(\alpha_2)$ per il campo K_2 e $f_2/(X-\alpha_2)$ per il polinomio f_2. Questo è giustificato perché i campi L_1 e L_2 sono anche i campi di spezzamento di $f_1/(X-\alpha_1)$ e $f_2/(X-\alpha_2)$.

Questo conclude la dimostrazione del teorema. □

Esercizi.

(14.A) Sia K un campo e sia $\sigma : K \longrightarrow K$ un omomorfismo di campi.

(i) Far vedere che

$$K^\sigma = \{x \in K : \sigma(x) = x\}$$

è un sottocampo di K.

(ii) Determinare K^σ se $K = \mathbb{C}$ e σ è la coniugazione complessa.

(iii) Dimostrare che $\sigma(x) = x$ per ogni x nel campo primo K_0 di K.

(14.B) Sia $\sigma : K \longrightarrow L$ un omomorfismo di campi. Far vedere che σ induce un isomorfismo fra i campi primi di K e L. Far vedere che $\mathrm{car}(K) = \mathrm{car}(L)$.

(14.C) Provare che la caratteristica di un campo finito non è 0. Far vedere che i campi finiti sono perfetti.

(14.D) Sia K un campo di caratteristica p.

(i) Far vedere che per ogni intero positivo n

$$\{x^{p^n} : x \in K\}$$

è un sottocampo di K.

(ii) Mostrare che

$$\{x \in K : x^{p^n} = x\}$$

è un sottocampo di K. Far vedere che esso ha al più p^n elementi.

(14.E) Consideriamo $\sqrt{2} \in \mathbb{R}$ e sia $K = \mathbb{Q}(\sqrt{2})$.

(i) Far vedere che $[K : \mathbb{Q}] = 2$.

(ii) Dimostrare che ogni elemento $\alpha \in K$ è algebrico su $\mathbb{Q}$.

(14.F) Far vedere che

$$f_{\min}^{\sqrt[n]{2}} = X^n - 2$$

per ogni intero $n > 0$.

(14.G) Sia K un campo e sia f un polinomio non nullo.

(i) Far vedere che l'anello $K[X]/(f)$ è uno spazio vettoriale su K di dimensione finita.

(ii) Dimostrare

$$\dim_K K[X]/(f) = \deg(f).$$

(14.H) Calcolare il poliomio minimo degli elementi

$$2 - \sqrt{3}, \quad \sqrt[3]{2} + \sqrt[3]{4}, \quad \sqrt{3 + 2\sqrt{2}}, \quad \beta^{-1}, \quad \beta + 1$$

dove β soddisfa $\beta^3 + 3\beta - 3$.

(14.I) Consideriamo $\sqrt{2}, \sqrt{7} \in \mathbb{R}$.

(i) Far vedere che $\mathbb{Q}(\sqrt{2}, \sqrt{7}) = \mathbb{Q}(\sqrt{2} + \sqrt{7})$.

(ii) Calcolare $f_{\min}^{\sqrt{2}+\sqrt{7}}$.

(iii) Dimostrare che $[\mathbb{Q}(\sqrt{2}, \sqrt{7}) : \mathbb{Q}] = 4$.

(14.J) Sia $\alpha \in \mathbb{R}$ con $\alpha^3 - \alpha - 1 = 0$. Scrivere i seguenti elementi nella forma $a + b\alpha + c\alpha^2$ dove $a, b, c \in \mathbb{Q}$:

$$\alpha^{10}, \quad (\alpha^2 + \alpha + 1)^2, \quad (\alpha^2 + 1)^{-1}.$$

(14.K) Sia K un campo e supponiamo che α e β siano elementi in certe estensioni di K con $f_{\min}^{\alpha} = f_{\min}^{\beta}$. Dimostrare che esiste un isomorfismo di campi

$$K(\alpha) \longrightarrow K(\beta)$$

che manda α a β.

(14.L) Sia K un campo e siano α, β elementi algebrici su K. Dimostrare

$$[K(\alpha,\beta):K] \leq [K(\alpha):K][K(\beta):K].$$

(14.M) (i) Far vedere che non esistono $a, b \in \mathbb{Q}$ tali che $(a+b\sqrt{2})^2 = 3$.

(ii) Dimostrare che il polinomio $X^2 - 3$ è irriducibile nell'anello $\mathbb{Q}(\sqrt{2})[X]$.

(iii) Provare

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4.$$

(14.N) Sia L un'estensione finita del campo K e sia $\alpha \in L$. Dimostrare che $\deg(f^{\alpha}_{\min})$ è un divisore di $[L:K]$.

(14.O) Sia K un campo e sia $f \in K[X]$ un polinomio irriducibile. Sia α uno zero di f contenuto in un'estensione di K. Dimostrare che se $g \in K[X]$ soddisfa $g(\alpha) = 0$, allora f divide g.

(14.P) Sia K un campo e sia α un elemento algebrico su K. Supponiamo che $[K(\alpha):K]$ sia *dispari*. Far vedere che $K(\alpha^2) = K(\alpha)$.

(14.Q) Sia L un'estensione del campo K e siano $\alpha, \beta \in L$ elementi algebrici su K. Supponiamo che i gradi $[K(\alpha):K]$ e $[K(\beta):K]$ non abbiano divisori comuni. Far vedere che

$$[K(\alpha,\beta):K] = [K(\alpha):K][K(\beta):K].$$

(14.R) Sia K un campo e sia α un elemento trascendente su K. Sia $\beta \in K(\alpha)$, $\beta \notin K$.

(i) Mostrare che α è algebrico su $K(\beta)$. (Sugg. Sia $\beta = f(\alpha)/g(\alpha)$ per certi $f, g \in K[X]$. Considerare il polinomio $f(X) - \beta g(X) \in K(\beta)[X]$).

(ii) Dimostrare che β è trascendente su K.

(14.S) Sia K un campo e sia $f \in K[X]$. Sia L un campo di spezzamento di f. Abbiamo dunque in $L[X]$

$$f = (X-\alpha_1)\cdot\ldots(X-\alpha_{n-1})(X-\alpha_n)$$

con $\alpha_1, \ldots, \alpha_{n-1}, \alpha_n \in L$. Dimostare che $L = K(\alpha_1, \ldots, \alpha_{n-1})$.

(14.T) Sia K un campo e sia $f \in K[X]$ un polinomio di grado n. Far vedere che il grado di un campo di spezzamento di f divide $n!$.

(14.U) Sia ζ una radice primitiva di ordine 3, cioè abbiamo che $\zeta^2 + \zeta + 1 = 0$. Dimostrare che il campo $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ è il campo di spezzamento di $X^3 - 2$ su $\mathbb{Q}$. Determinare il grado $[K:\mathbb{Q}]$.

(14.V) Sia i una radice primitiva di ordine 4, cioè abbiamo che $i^2 + 1 = 0$. Far vedere che il campo $K = \mathbb{Q}(\sqrt[4]{2}, i)$ è il campo di spezzamento di $X^4 - 2$ su $\mathbb{Q}$. Determinare il grado $[K:\mathbb{Q}]$.

(14.W) Sia ζ uno zero del polinomio $f = X^4 + X^3 + X^2 + X + 1$.

(i) Far vedere che $\zeta^5 = 1$.

(ii) Far vedere che ζ^2, ζ^3 e ζ^4 sono gli altri zeri di f.

(iii) Dimostrare che $\mathbb{Q}(\zeta)$ è un campo di spezzamento di f.

15 Il campo dei numeri complessi

15.1 Definizione. Un campo K si dice *algebricamente chiuso* se per ogni polinomio non nullo $f \in K[X]$ esiste $c \in K^*$ ed esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ tali che

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n).$$

15.2 In questo paragrafo dimostriamo che il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso. Diamo la dimostrazione che diede Gauss nel 1799, quando aveva 22 anni. Per capire la dimostrazione è necessario sapere qualcosa sui polinomi *simmetrici*.

15.3 Definizione. Sia R un anello commutativo e sia $n > 0$ un intero. Un polinomio $f(X_1, X_2, \ldots, X_n)$ in $R[X_1, X_2, \ldots, X_n]$ di dice *simmetrico* se

$$f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = f(X_1, X_2, \ldots, X_n)$$

per ogni permutazione $\sigma \in S_n$.

15.4 Esempi. Per esempio, i polinomi

$$\begin{aligned} &X_1 + X_2 + \ldots + X_n, \\ &X_1 \cdot X_2 \cdot \ldots \cdot X_n, \\ &X_1^k + X_2^k + \ldots + X_n^k, \qquad \text{per } k \in \mathbb{Z}_{\geq 0} \\ &X_1 + X_2 + \ldots + X_n + X_1^2 + X_2^2 + \ldots + X_n^2 \end{aligned}$$

sono simmetrici.

15.5 Definizione. Sia R un anello commutativo e sia n un intero positivo. Consideriamo il seguente polinomio in Z con coefficienti in $R[X_1, X_2, \ldots, X_n]$:

$$g(Z) = (Z - X_1) \cdot (Z - X_2) \cdot \ldots \cdot (Z - X_n) \in R[X_1, X_2, \ldots, X_n][Z].$$

Moltiplicando tutti i fattori si trova

$$g(Z) = Z^n - \sigma_1 Z^{n-1} + \sigma_2 Z^{n-2} - \ldots + (-1)^{n-1}\sigma_{n-1} Z + (-1)^n \sigma_n$$

dove i polinomi $\sigma_i \in R[X_1, X_2, \ldots, X_n]$ sono i cosiddetti *polinomi simmetrici elementari*:

$$\begin{aligned}
\sigma_1 &= X_1 + X_2 + \ldots + X_n, \\
\sigma_2 &= X_1X_2 + X_1X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_{n-1}X_n, \\
&= \textstyle\sum_{1\le i<j\le n} X_iX_j, \\
\sigma_3 &= \textstyle\sum_{1\le i<j<k\le n} X_iX_jX_k, \\
&\vdots \\
\sigma_n &= X_1X_2 \cdot \ldots \cdot X_n.
\end{aligned}$$

15.6 Si vede facilmente che somme e prodotti di polinomi simmetrici elementari sono ancora simmetrici. Più generalmente, ogni polinomio in $\sigma_1, \sigma_2, \ldots, \sigma_n$ è un polinomio simmetrico in $X_1, X_2, \ldots, X_n$.

Per esempio, con $n = 2$:

$$\begin{aligned}
\sigma_1^2 &= X_1^2 + 2X_1X_2 + X_2^2, \\
\sigma_1^2 - 2\sigma_2 &= X_1^2 + X_2^2, \\
\sigma_1^3 - 3\sigma_1\sigma_2 &= X_1^3 + X_2^3.
\end{aligned}$$

Anche il viceversa vale:

15.7 Teorema. (Teorema principale dei polinomi simmetrici.) Sia R un anello commutativo e sia n un intero positivo. Se $f \in R[X_1, X_2, \ldots, X_n]$ è un polinomio simmetrico allora esiste un unico polinomio $F \in R[Y_1, \ldots, Y_n]$ tale che

$$f(X_1, \ldots, X_n) = F(\sigma_1, \ldots, \sigma_n).$$

Dimostrazione. Sia $f \in R[X_1, X_2, \ldots, X_n]$ un polinomio simmetrico. Ordiniamo i termini $rX_1^{a_1}X_2^{a_2} \cdot \ldots \cdot X_n^{a_n}$ di f in modo lessicografico: il termine $rX_1^{a_1}X_2^{a_2} \cdot \ldots \cdot X_n^{a_n}$ appare prima di $r'X_1^{b_1}X_2^{b_2} \cdot \ldots \cdot X_n^{b_n}$ se $a_i > b_i$ per il più piccolo i con $a_i \neq b_i$.

Il "primo termine di f

$$rX_1^{c_1}X_2^{c_2} \cdot \ldots \cdot X_n^{c_n}, \qquad r \in R - \{0\},$$

ha dunque gli esponenti c_i dove c_1 è il più grande esponente di X_1 che occorre in f. Il numero c_2 è il più grande esponente di X_2 che occorre nei termini dove X_1 occorre con esponente c_1. Il numero c_3 è il più grande esponente di X_3 che occorre nei termini dove X_1 occorre con esponente c_1 e X_2 con esponente c_2, ... ecc. Siccome f è un polinomio simmetrico, deve essere $c_1 \ge c_2 \ge \ldots \ge c_n$. Perché se non fosse così, si potrebbero scambiare due variabili e ottenere un termine che dovrebbe occorrere prima in f.

Siccome

$$\begin{aligned}
&\sigma_1 \quad \text{ha primo termine } X_1, \\
&\sigma_2 \quad \text{ha primo termine } X_1X_2, \\
&\quad\vdots \\
&\sigma_n \quad \text{ha primo termine } X_1X_2 \cdot \ldots \cdot X_n,
\end{aligned}$$

si vede che anche il primo termine di

$$r\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\cdot\ldots\cdot\sigma_{n-1}^{c_{n-1}-c_n}\sigma_n^{c_n}$$

è uguale a

$$rX_1^{c_1}X_2^{c_2}\cdot\ldots\cdot X_n^{c_n}.$$

Sia

$$f_1 = f - r\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\cdot\ldots\cdot\sigma_{n-1}^{c_{n-1}-c_n}\sigma_n^{c_n}.$$

Se $f_1 = 0$ abbiamo scritto f come polinomio nei polinomi simmetrici elementari. Se f_1 non è zero, ripetiamo la procedura con il polinomio simmetrico f_1 e scriviamo, se $r'X_1^{c_1'}X_2^{c_2'}\cdot\ldots\cdot X_n^{c_n'}$ è il primo termine di f_1

$$f_2 = f_1 - r\sigma_1^{c_1'-c_2'}\sigma_2^{c_2'-c_3'}\cdot\ldots\cdot\sigma_{n-1}^{c_{n-1}'-c_n'}\sigma_n^{c_n'}.$$

e così via.

Dobbiamo dimostrare che questa procedura finisce ad un certo punto, cioè, dopo un numero finito di passi troviamo un polinomio nullo. Per fare questo osserviamo prima che f_1 contiene, rispetto al nostro ordine lessicografico, soltanto termini che vengono "dopo $rX_1^{c_1}X_2^{c_2}\cdot\ldots\cdot X_n^{c_n}$.

Poi introduciamo il *grado totale* totdeg(f) di f, cioè il massimo valore di $a_1 + a_2 + \ldots a_n$ tale che in f occorre un termine $rX_1^{a_1}X_2^{a_2}\cdot\ldots\cdot X_n^{a_n}$ con $r \neq 0$. Per esempio, totdeg$(\sigma_i) = i$ e

$$\begin{aligned}\text{totdeg}(\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\cdot\ldots\cdot\sigma_{n-1}^{c_{n-1}-c_n}\sigma_n^{c_n}) &= (c_1-c_2)+2(c_2-c_3)+3(c_3-c_4)+\ldots\\ &= c_1+c_2+\ldots+c_n\end{aligned}$$

Siccome totdeg$(f) \geq c_1 + c_2 + \ldots + c_n$, abbiamo

$$\text{totdeg}(f_1) \leq \text{totdeg}(f).$$

Allora, nella procedura sopra abbiamo che

$$\text{totdeg}(f) \geq \text{totdeg}(f_1) \geq \text{totdeg}(f_2) \geq \ldots$$

Quindi il grado totale non cresce. Ci sono, dato un grado totale fisso, soltanto un numero finito di termini $X_1^{a_1}X_2^{a_2}\cdot\ldots\cdot X_n^{a_n}$ possibili. Quindi, nella procedura sopra, incontreremo soltanto un numero finiti di termini $X_1^{a_1}X_2^{a_2}\cdot\ldots\cdot X_n^{a_n}$. Siccome in ogni passo perdiamo il termine lessicograficamente più alto, la procedure deve terminare.

Non avremo bisogno dell'unicità del modo di scrivere un polinomio simmetrico come polinomio nei polinomi simmetrici elementari. Per la dimostrazione dell'unicità si veda l'Eserc.(15.E).

Questo conclude la dimostrazione del Teorema. □

15.8 Esempio. Sia $n = 3$ e sia

$$f = X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3.$$

I termini di f sono già in ordine lessicografico. Il primo termine è dunque $X_1^3X_2$ e abbiamo $c_1 = 3$, $c_2 = 1$ e $c_3 = 0$. Nella procedura della dimostrazione del teorema principale dobbiamo sottrarre

$$\begin{aligned}\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\sigma_3^{c_3} &= \sigma_1^2\sigma_2\\ &= (X_1+X_2+X_3)^2(X_1X_2+X_1X_3+X_2X_3)\end{aligned}$$

di f. Facendo questo, si trova

$$\begin{aligned}f_1 &= f-\sigma_1^2\sigma_2,\\ &= -2X_1^2X_2^2-5X_1^2X_2X_3-2X_1^2X_3^2-5X_1X_2^2X_3-5X_1X_2X_3^2-2X_2^2X_3^2.\end{aligned}$$

Il primo termine di f_1 è $-2X_1^2X_2^2$. Adesso sottraiamo

$$-2\sigma_2^2 = -2X_1^2X_2^2-4X_1^2X_2X_3-2X_1^2X_3^2-4X_1X_2^2X_3-4X_1X_2X_3^2-2X_2^2X_3^2$$

e troviamo che

$$f_2 = f_1-(-\sigma_2^2) = -X_1^2X_2X_3-X_1X_2^2X_3-X_1X_2X_3^2.$$

Il primo coefficiente di f_2 è $-X_1^2X_2X_3$. Seguendo la procedura sottraiamo $-\sigma_1\sigma_3$. Adesso troviamo 0. Concludiamo che

$$f = \sigma_1^2\sigma_2-2\sigma_2^2-\sigma_1\sigma_3.$$

15.9 Corollario. Sia K un campo e sia $h \in K[X]$ un polinomio monico di grado n. Supponiamo che

$$h(X) = (X-\alpha_1)(X-\alpha_2)\cdot\ldots\cdot(X-\alpha_n)$$

in $L[X]$ dove L è un campo di spezzamento di f su K. Allora, per ogni polinomio simmetrico $f \in K[X_1, X_2, \ldots, X_n]$ si ha che

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K.$$

Dimostrazione. Siano $\sigma_1, \sigma_2, \ldots, \sigma_n$ i polinomi simmetrici elementari negli zeri $\alpha_1, \alpha_2, \ldots, \alpha_n$. Allora, siccome i coefficienti di h stanno in K, abbiamo che $\sigma_i \in K$ per $1 \le i \le n$. Per il Teorema 15.7 ogni polinomio simmetrico $f \in K[X_1, X_2, \ldots, X_n]$ è un'espressione polinomiale con coefficienti in K di polinomi simmetrici elementari. Quindi $f(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K$ come richiesto. □

15.10 Polinomi di grado 3. Consideriamo adesso gli zeri α_1, α_2 e α_3 di un polinomio $f \in \mathbb{C}[X]$ di grado 3,

$$f = X^3+aX^2+bX+c.$$

I coefficienti a, b, c di f sono funzioni simmetriche negli zeri α_i di f. L'idea fondamentale per trovare gli zeri di f è di sfruttare il fatto che il gruppo S_3 ha un sottogruppo abeliano A_3 e che S_3/A_3 è abeliano. Definiamo

$$\sigma = (123), \qquad \tau = (23).$$

Sia

$$\omega = (-1 + i\sqrt{3})/2, \qquad \text{allora} \quad \omega^2 = \bar{\omega} = (-1 - i\sqrt{3})/2,$$

e $\omega^3 = 1$. Consideriamo i numeri complessi

$$\begin{aligned} A_1 &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3, \\ A_2 &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3. \end{aligned}$$

Gli elementi di S_3 permutano gli α_i, in questo caso:

$$\sigma(A_1) = \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 = \omega^2(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3) = \omega^2 A_1,$$

e similmente $\sigma(A_2) = \omega A_2$. Perciò A_1A_2, A_1^3 e A_2^3 sono invarianti per il sottogruppo generato da σ, $< \sigma >= A_3$. Adesso consideriamo l'azione di τ:

$$\tau(A_1) = A_2, \quad \tau(A_2) = A_1.$$

Quindi

$$A = A_1A_2, \qquad B = (A_1^3 + A_2^3)/2$$

sono invarianti per i generatori σ e τ di S_3 e quindi per ogni elemento di S_3. Per il Teorema 15.7, A e B sono dunque polinomi nei coefficienti di f. Con un calcolo esplicito si ottiene:

$$A = a^2 - 3b, \qquad B = (-2a^3 + 9ab - 27c)/2.$$

Osserviamo che:

$$(T - A_1^3)(T - A_2^3) = T^2 - 2BT + A^3$$

e perciò troviamo

$$A_1^3,\ A_2^3 = \frac{2B \pm \sqrt{4B^2 - 4A^3}}{2} = B \pm \sqrt{B^2 - A^3},$$

e poi $A_1 = \sqrt[3]{B \pm \sqrt{B^2 - A^3}}$, $A_2 = A/A_1$. Una volta determinato gli A_i, possiamo trovare lo zero α_1 di f tramite

$$\alpha_1 = -a + A_1 + A_2$$

perchè $-a = \alpha_1 + \alpha_2 + \alpha_3$ e $1 + \omega + \omega^2 = 0$.

15.11 Polinomi di grado 4. Il caso di un polinomio di grado 4 si tratta in modo simile, sfruttando il sottogruppo normale abeliano $V_4 \subset S_4$ con gruppo quoziente S_3, vedi Capitolo 7. Questo permette di 'ridurre' l'equazione di grado 4 a un'equazione di grado 3.

Siano $\alpha_1, \ldots, \alpha_4 \in \mathbb{C}$ gli zeri di

$$f = X^4 + aX^3 + bX^2 + cX + d.$$

Definiamo

$$\begin{aligned} \beta_1 &= \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4, \\ \beta_2 &= \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4, \\ \beta_3 &= \alpha_1 - \alpha_2 - \alpha_3 + \alpha_4. \end{aligned}$$

Visto che $a = -(\alpha_1 + \ldots + \alpha_4)$ si ha:

$$4\alpha_1 = -a + \beta_1 + \beta_2 + \beta_3,$$

quindi basta determinare i tre β_i. Il sottogruppo V_4 di S_4 è:

$$K = \{\, e,\ k_1 = (12)(34),\ k_2 = (13)(24),\ k_3 = (14)(23)\ \}.$$

Non è difficile verificare che per ogni i e j si ha $k_i(\beta_j) = \pm\beta_j$, quindi gli β_j^2 sono invarianti per V_4.

Ogni $\sigma \in S_4$ permuta i β_i, a meno di un segno, cioè per ogni i, $\sigma(\beta_i) = \pm\beta_j$ per un certo j (i β_i hanno sempre due '$-$'). Quindi $S_3 = S_4/V_4$ permuta i tre β_i^2 e dunque i coefficienti A, B, e C del polinomio, nella variabile T,

$$P = (T - \beta_1^2)(T - \beta_2^2)(T - \beta_3^2) = T^3 - AT^2 + BT - C$$

sono invariante per S_4. Perciò questi coefficienti sono polinomi nei coefficienti di f. Con un calcolo esplicito si ottiene:

$$\begin{aligned} A = \beta_1^2 + \beta_2^2 + \beta_3^2 &= 3a^2 - 8b \\ B = \beta_1^2\beta_2^2 + \beta_1^2\beta_3^2 + \beta_2^2\beta_3^2 &= 3a^4 - 16a^2b + 16b^2 + 16ac - 64d \\ C = \beta_1^2\beta_2^2\beta_3^2 &= (a^3 - 4ab + 8c)^2. \end{aligned}$$

Abbiamo già visto come trovare gli zeri di un polinomio di grado 3 e quindi siamo in grado di trovare anche gli zeri di un polinomio di grado 4.

15.12 Non è possibile procedere in questo modo per polinomi di grado almeno 5. Il problema è che i gruppi S_n, per $n \geq 5$, non ammettono omomorfismi suriettivi a gruppi con meno di $n!$ elementi, diversi dal gruppo $\{\pm 1\}$ e dal gruppo banale $\{e\}$.

Adesso dimostriamo un caso speciale del risultato principale di questo paragrafo:

15.13 Lemma. Ogni polinomio $f \in \mathbb{C}[X]$ di grado due ha gli zeri in $\mathbb{C}$.

Dimostrazione. Dimostriamo prima che per ogni $z \in \mathbb{C}$ anche $\sqrt{z} \in \mathbb{C}$, cioè esiste $w \in \mathbb{C}$ tale che $w^2 = z$. Sia $z = x + yi$ dove $x, y \in \mathbb{R}$. Consideriamo

$$w = \sqrt{\frac{\sqrt{x^2+y^2} + x}{2}} \pm \sqrt{\frac{\sqrt{x^2+y^2} - x}{2}}\, i$$

dove il segno $\pm$ è il segno di y. Si verifica che

$$w^2 = x \pm \sqrt{y^2}\, i = x + yi = z.$$

Il caso generale, $f = aX^2 + bX + c$ dove $a \neq 0$, segue adesso dalla solita formula per gli zeri α di f:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

□

15.14 Nel passato il prossimo teorema si chiamava *Il Teorema Fondamentale dell'Algebra*. Oggigiorno, non si ritiene questo teorema così fondamentale. C'è una dimostrazione molto semplice ed elegante che utilizza l'analisi complessa, vale a dire il Teorema di Liouville. Noi diamo la dimostrazione algebrica di Gauss.

15.15 Teorema. (Teorema Fondamentale dell'Algebra) Sia $g \in \mathbb{C}[X]$ un polinomio non nullo. Allora

$$g(X) = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$$

dove $c \in \mathbb{C}^*$ e $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$.

Dimostrazione. Sia $g \in \mathbb{C}[X]$ un polinomio, $g \notin \mathbb{C}$. Se $\alpha \in \mathbb{C}$ è uno zero di g, allora, per la Prop.10.5, si ha $g = (X - \alpha) \cdot g_1$ dove $g_1 \in \mathbb{C}[X]$. Dunque, per induzione rispetto al grado di g, basta dimostrare che ogni polinomio non costante in $\mathbb{C}[X]$ ha uno zero in $\mathbb{C}$.

Affermiamo che basta dimostrare che ogni polinomio non costante con coefficienti in $\mathbb{R}$ ha uno zero in $\mathbb{C}$: sia

$$g = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \ \in \mathbb{C}[X]$$

un polinomio non nullo e sia

$$\overline{g} = \overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} + \dots + \overline{a_1} X + \overline{a_0} \ \in \mathbb{C}[X]$$

il polinomio coniugato. Per l'Eserc.(15.F) il prodotto $G = g\overline{g}$ è un polinomio con coefficienti in $\mathbb{R}$. Se $G(\alpha) = 0$ per un certo $\alpha \in \mathbb{C}$, allora $g(\alpha)\overline{g}(\alpha) = 0$. Quindi $g(\alpha) = 0$ oppure $\overline{g}(\alpha) = 0$. Nell'ultimo caso abbiamo che $g(\overline{\alpha}) = \overline{\overline{g}(\alpha)} = 0$. Dunque, in ogni caso g ha uno zero in $\mathbb{C}$.

Sia dunque $G \in \mathbb{R}[X]$ un polinomio non nullo. Senza perdere la generalità assumiamo che G sia monico. Sia $n = \deg(G)$ e sia $k \in \mathbb{Z}_{\geq 0}$ tale che 2^k è la più grande potenza di 2 che divide n. Dimostreremo per induzione rispetto a k che G ha uno zero in $\mathbb{C}$.

Se $k = 0$, il grado di G è dispari. In questo caso abbiamo che

$$\lim_{x\to\infty} G(x) = +\infty \qquad \text{e} \qquad \lim_{x\to-\infty} G(x) = -\infty$$

La funzione $\mathbb{R} \longrightarrow \mathbb{R}$ data da $x \mapsto G(x)$ è continua per la topologia usuale di $\mathbb{R}$. Quindi, per il Teorema "del valor medio in analisi, G ha uno zero in $\mathbb{R}$ e quindi anche in $\mathbb{C}$.

Per $k > 0$, scriviamo

$$G(X) = (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n) \quad \text{in } F[X].$$

dove F è un campo di spezzamento di G su $\mathbb{C}$. Definiamo, per ogni $t \in \mathbb{R}$ il polinomio

$$H_t(X) = \prod_{1\leq i<j\leq n} (X - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$$

Il grado di H_t è $\binom{n}{2} = n(n-1)/2$. I coefficienti di H_t sono espressioni simmetriche negli zeri α_i con coefficienti in $\mathbb{R}$. Per il Cor.15.9, i coefficienti di H_t sono in $\mathbb{R}$.

Siccome 2^{k-1} è la più grande potenza di 2 che divide il grado $n(n-1)/2$, i polinomi H_t possiedono, per l'ipotesi di induzione, uno zero in $\mathbb{C}$. Quindi, per ogni $t \in \mathbb{R}$ ci sono $i, j \in \{1, 2, \ldots, n\}$, tali che

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}.$$

Siccome i numeri reali sono infiniti, ma ci sono soltanto un numero finito di sottoinsiemi $\{i, j\}$ di $\{1, 2, \ldots, n\}$, devono esistere $t, t' \in \mathbb{R}$ con $t \neq t'$ e con

$$\begin{aligned} \alpha_i + \alpha_j + t\alpha_i\alpha_j &\in \mathbb{C} \\ \alpha_i + \alpha_j + t'\alpha_i\alpha_j &\in \mathbb{C}. \end{aligned}$$

Questo implica facilmente che sia $\alpha_i + \alpha_j$ che $\alpha_i\alpha_j$ sono in $\mathbb{C}$. Quindi, il polinomio

$$X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j = (X - \alpha_i)(X - \alpha_j)$$

è in $\mathbb{C}[X]$. Per il Lemma 15.13, questo polinomio ha gli zeri in $\mathbb{C}$. Concludiamo che α_i e α_j sono contenuti in $\mathbb{C}$. Il polinomio G ha, dunque, uno zero in $\mathbb{C}$, come richiesto. □

15.16 Definizione. Sia K un campo. Un campo L si dice *una chiusura algebrica di* K se

(1) L è una estensione algebrica di K.

(2) L è algebricamente chiuso.

15.17 Esempio. Sia

$$F = \{\alpha \in \mathbb{C} : \alpha \text{ è algebrico su } \mathbb{Q}\}$$

il campo dei numeri algebrici. Affermiamo che F è una chiusura algebrica di $\mathbb{Q}$: per definizione F è una estensione algebrica di $\mathbb{Q}$. Adesso vediamo che F è algebricamente chiuso. Sia $f = a_nX^n + \ldots + a_1X + a_0 \in F[X]$ un polinomio e sia $\alpha \in \mathbb{C}$ uno zero di f. Siccome ogni coefficiente a_i è algebrico su $\mathbb{Q}$, abbiamo per 14.8 e 14.11 che

$$[\mathbb{Q}(a_n, \ldots, a_1, a_0) : \mathbb{Q}] < \infty.$$

Siccome α è algebrico sul campo $\mathbb{Q}(a_n, \ldots, a_1, a_0)$ abbiamo che

$$[\mathbb{Q}(\alpha, a_n, \ldots, a_1, a_0) : \mathbb{Q}(a_n, \ldots, a_1, a_0)] < \infty$$

e quindi, per 14.8, che $\mathbb{Q}(\alpha, a_n, \ldots, a_1, a_0)$ è una estensione finita di $\mathbb{Q}$. Questo implica che α è algebrico su $\mathbb{Q}$, cioè $\alpha \in F$.

Siccome $\mathbb{C}$ è algebricamente chiuso,

$$f = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$$

dove $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Siccome ogni zero di f in $\mathbb{C}$ sta in F, concludiamo che F è algebricamente chiuso, come richiesto.

15.18 Teorema. Ogni campo K possiede una chiusura algebrica $\overline{K}$. Il campo $\overline{K}$ è unico a meno di K-isomorfismi.

Dimostrazione. Si ha bisogno dell'assioma della scelta. Si veda il libro di S. Lang: *Algebra*, Second edition, Addison-Wesley, Menlo Park 1984. □

Esercizi.

(15.A) Esprimere il polinomio simmetrico

$$X_1^3 + X_2^3 + X_3^3$$

in termini dei polinomi simmetrici elementari σ_1, σ_2 e σ_3.

(15.B) Siano $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ tali che

$$X^3 - X - 1 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

sia

$$p_k = \alpha_1^k + \alpha_2^k + \alpha_3^k \qquad \text{per } k \in \mathbb{Z}.$$

Dimostrare che

$$\begin{aligned} p_{-1} &= -1, \quad p_0 = 3, \quad p_1 = 0, \\ p_k &= p_{k-2} + p_{k-3} \qquad \text{per ogni } k \in \mathbb{Z}, \\ p_k &\in \mathbb{Z} \qquad\qquad \text{per ogni } k \in \mathbb{Z}. \end{aligned}$$

(15.C) Sia

$$X^3 - X^2 + X - 2 = (X - \alpha)(X - \beta)(X - \gamma).$$

(i) Trovare il polinomio che ha α^2, β^2 e γ^2 come zeri.

(ii) Trovare il polinomio che ha $\alpha\beta$, $\beta\gamma$ e $\gamma\alpha$ come zeri.

(15.D) *(Discriminanti.)* Sia K un anello commutativo e sia

$$\begin{aligned} f &= X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \\ &= (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n) \end{aligned}$$

Definiamo il *discriminante* $\Delta(f)$ *di* f per

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

(i) Far vedere che $\Delta(f)$ è un polinomio simmetrico negli zeri α_i.

(ii) Far vedere che $\Delta(f) = 0$ se e soltanto se f ha zeri doppi.

(iii) Dimostrare che

$$\begin{aligned} \Delta(X^2 + aX + b) &= a^2 - 4b, \\ \Delta(x^3 + aX^2 + bX + c) &= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc. \end{aligned}$$

(iv) Dimostrare che per ogni grado n esiste un polinomio D nei coefficienti $a_{n-1}, \ldots, a_1, a_0$ tale che $\Delta(f) = D(a_{n-1}, \ldots, a_1, a_0)$.

(15.E) * Lo scopo di questo esercizio è di dimostrare l'unicità del modo di scrivere un polinomio simmetrico in termini dei polinomi simmetrici elementari. Si veda la dimostrazione del Teorema 15.7.

Sia R un anello commutativo e sia $g \in R[Y_1, Y_2, \ldots, Y_n]$, $g \neq 0$.

(i) Far vedere che ogni termine di g si può scrivere come

$$rY_1^{a_1-a_2} \cdot Y_2^{a_2-a_3} \cdot \ldots \cdot Y_n^{a_n}$$

dove $r \in R$, $r \neq 0$ e $a_i \in \mathbb{Z}_{\geq 0}$.

(ii) Ordiniamo i termini di g in modo che il termine $rY_1^{a_1-a_2} \cdot Y_2^{a_2-a_3} \cdot \ldots \cdot Y_n^{a_n}$ venga prima del termine $r'Y_1^{b_1-b_2}Y_2^{b_2-b_3} \cdot \ldots \cdot Y_n^{b_n}$ se $a_i > b_i$ per il più piccolo i tale che $a_i \neq b_i$.

(iii) Sia $rY_1^{a_1-a_2} \cdot Y_2^{a_2-a_3} \cdot \ldots \cdot Y_n^{a_n}$ il primo termine di g in questo senso. Far vedere che il primo termine nel senso della dimostrazione del Teorema 15.7 del polinomio

$$G(X_1, X_2, \ldots, X_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n) \in R[X_1, X_2, \ldots, X_n]$$

è uguale a $rX_1^{a_1}X_2^{a_2} \cdot \ldots \cdot X_n^{a_n}$. Concludere che $G \neq 0$.

(iii) Dimostrare che si può scrivere un polinomio simmetrico $G \in R[X_1, X_2, \ldots, X_n]$ in termini di polinomi simmetrici elementari *in modo unico*.

(15.F) Sia

$$f = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{C}[X]$$

e sia $\overline{f} = \overline{a_n}X^n + \ldots + \overline{a_1}X + \overline{a_0}$. Provare che il polinomio $f \cdot \overline{f}$ ha coefficienti in $\mathbb{R}$.

(15.G) Sia R un anello commutativo. Sia n un intero positivo e siano $\sigma_1, \sigma_2, \ldots, \sigma_n$ i polinomi simmetrici elementari in $X_1, X_2, \ldots, X_n$. Sia $R[\sigma_1, \sigma_2, \ldots, \sigma_n]$ il più piccolo sottoanello di $R[X_1, X_2, \ldots, X_n]$ che contiene i polinomi σ_i. Dimostrare che c'è un'isomorfismo di anelli

$$R[\sigma_1, \sigma_2, \ldots, \sigma_n] \cong R[X_1, X_2, \ldots, X_n].$$

(15.H) Dimostrare che un campo algebricamente chiuso è infinito.

(15.I) Sia $K \subset \mathbb{C}$ una estensione finita di $\mathbb{Q}$. Far vedere che la chiusura algebrica $\overline{\mathbb{Q}}$ di $\mathbb{Q}$ è anche una chiusura algebrica di K.

(15.J) Sia $\overline{\mathbb{Q}} \subset \mathbb{C}$ la chiusura algebrica di $\mathbb{Q}$ in $\mathbb{C}$. Dimostrare che

$$[\overline{\mathbb{Q}} : \overline{\mathbb{Q}} \cap \mathbb{R}] = 2.$$

(15.K) Sia p un primo. Sia $\overline{\mathbf{F}_p}$ una chiusura algebrica di $\mathbf{F}_p$.

(i) Dimostrare che per ogni intero positivo n, esiste un'unica estensione $K_n \subset \overline{\mathbf{F}_p}$ di grado $n!$ su $\mathbf{F}_p$.

(ii) Far vedere che $K_n \subset K_{n+1}$ per ogni $n \in \mathbb{Z}_{\geq 1}$.

(iii) Far vedere che

$$\overline{\mathbf{F}_p} = \bigcup_{n \geq 1} K_n.$$

(15.L) Sia $f \in \mathbb{R}[X]$ un polinomio non nullo. Dimostrare che

$$f = c \cdot (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_k) \cdot f_1 \cdot \ldots \cdot f_m$$

dove $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$, $c \in \mathbb{R}^*$ e

$$f_j = X^2 + \beta_j X + \gamma_j, \qquad \text{per } 1 \leq j \leq m$$

con $\beta_j, \gamma_j \in \mathbb{R}$ e $\beta_j^2 - 4\gamma_j < 0$. Inoltre, questo modo di scrivere è unico a meno dell'ordine dei fattori.