# Algebra

René Schoof

Dipartimento di Matematica
Università degli Studi di Trento
I-38050 Povo (Trento) ITALY
Email: schoof@itnvax.cineca.it

**Abstract.** Note provvisorie per il corso di *Algebra,* Trento 1991–1992.

## 0. Numeri interi.

L'insieme dei numeri interi è

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

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 (0.8): ogni intero positivo può essere scritto in modo unico come prodotto di numeri primi.

**Teorema (0.1).** *(Divisone con resto) Siano $a, b \in \mathbf{Z}$ con $b > 0$. Allora esistono unici due interi, il quoziente $q$ ed il resto $r$, tali che*

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

**Dimostrazione.** Sia

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

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 $x \in \mathbf{Z}$. 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

$$a = qb + r,$$
$$a = q'b + r'$$

con $0 \leq r, r' < b$. Supponiamo che $q \neq q'$. Scambiando $q'$ e $q$, se necessario, possiamo supporre che $q > q'$. Adesso sottraiamo membro a membro le due uguaglienze 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.

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

$$b = ac.$$

Per esempio, 3 divide 15, perche $15 = 3 \cdot 5$. Ogni intero divide 0. Se $a$ divide $b$, si dice anche che $a$ e 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.

**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 $\mathrm{mcd}(0, 0) = 0$.

**Proposizione (0.2).** *Siano $a, b \in \mathbf{Z}$.*
*(i)* $\mathrm{mcd}(b, a) = \mathrm{mcd}(a, b)$,
*(ii)* $\mathrm{mcd}(-a, b) = \mathrm{mcd}(a, b)$,
*(iii) Per ogni $q \in \mathbf{Z}$ 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 $q \in \mathbf{Z}$. 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 (*iii*).

**Teorema (0.3).** *Siano $a, b \in \mathbf{Z}$, non entrambi nulli. Allora il massimo comun divisore di $a$ e $b$ è uguale al più piccolo elemento positivo nell'insieme*

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

**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 0.1, 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.

**Corollario (0.4).** *Siano $a, b \in \mathbf{Z}$. Allora esistono $x, y \in \mathbf{Z}$ tali che*

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

**Dimostrazione.** L'affermazione è banale quando $a = b = 0$ e nell' altro caso segue dal Teorema 0.3.

**Corollario (0.5).** *Siano $a, b \in \mathbf{Z}$. 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 0.4.

**Corollario (0.6).** *Siano $a, b, c \in \mathbf{Z}$. Se* $\mathrm{mcd}(a, b) = 1$ *e $a|bc$ allora $a|c$.*

**Dimostrazione.** Per il Corollario 0.4 esistono $x, y \in \mathbf{Z}$ tale che $ax + by = 1$. Moltiplicando per $c$ otteniamo:

$$cax + bcy = c.$$

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

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

Esempi di numeri primi sono $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots, 94291, 94307, 94309, \ldots,$ 772865886177933052632667046915246737827100790144773744195236265619879496879953539649, .... I numeri primi sono infiniti (si veda Eserc.0.K).

**Proposizione (0.7).** *Siano $b, c \in \mathbf{Z}$ 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.0.6 abbiamo che $p$ divide $c$.

**Teorema (0.8).** *(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

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

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.0.7, $p_1$ 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.

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

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

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

**Proposizione (0.9).** *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 0.8, 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.

Infine diamo un *algoritmo* per calcolare il mcd di due interi. Questo metodo si chiama *algoritmo di Euclide:* siano $a, b \in \mathbf{Z}$ e supponiamo che $a, b > 0$. Per la Proposizione 0.2*(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 0.1, 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 $r_{k+1}$:

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

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.

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

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

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

**Proposizione (0.10).** *L'algoritmo di Euclide è un algoritmo corretto: termina e da 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 Prop.0.2*(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 $x, y \in \mathbf{Z}$ del Cor.0.4 tali che

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

**Algoritmo.** Scriviamo

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

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.

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

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

**Esercizi.**

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

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

(0.C) Calcolare $\mathrm{mcd}(10000000000, 2^5 \cdot 91)$. (Utilizzare la Prop.0.9*(iii)*.)

(0.D) Siano $a, b \in \mathbf{Z}$. 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 $\mathrm{mcd}(ac, bc) = c \cdot \mathrm{mcd}(a, b)$.

(0.E) (Il mcd di più numeri.)

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

(ii) Per $a_1, a_2, \ldots, a_m$ 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 $x_1, x_2 \ldots, x_m \in \mathbf{Z}$ tali che $x_1 a_1 + x_2 a_2 + \ldots + x_m a_m = \mathrm{mcd}(a_1, a_2, \ldots, a_m)$.

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

(0.G) Siano $a, b \in \mathbf{Z}$. 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 $\mathrm{mcm}(a, b) \cdot \mathrm{mcd}(a, b) = |ab|$.

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

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

(0.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?

(0.K) Dimostrare che esiste una infinità di numeri primi.

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

(0.M) Sia $n$ un intero positivo e sia $p$ un primo. Determinare $\mathrm{ord}_p(n!)$. Con quanti zeri finisce 1000! ?

(0.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 $n < p < 2n$.

(0.O) Siano $a, b \in \mathbf{Z}$.

(i) Siano $r, s \in \mathbf{Z}$ 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 $x \in \mathbf{Q}$, allora $x \in \mathbf{Z}$.

(0.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.

(0.Q) Siano $a, b \in \mathbf{Z}$ 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.*

(0.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.

(0.S) Siano $a, b \in \mathbf{Z}$ 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.*

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

(0.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.

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

(0.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* $n^2 2^{n+1}$.)

## 1. Gruppi.

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

**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.*

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 $\circ$.

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. 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 $x$.

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

**Esempio (1.1).** *I gruppi additivi* $\mathbf{Z}$, $\mathbf{Q}$ *ed* $\mathbf{R}$.
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 $\mathbf{Z}$ 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: $\mathbf{Z}$ è un gruppo commutativo. Si verifica in modo simile che anche i numeri razionali $\mathbf{Q}$ e i numeri reali $\mathbf{R}$ formano un gruppo per l'addizione. In questi tre esempi l'elemento neutro è 0. I gruppi $\mathbf{Q}$ ed $\mathbf{R}$ sono commutativi.

**Esempio (1.2).** *I gruppi moltiplicativi* $\mathbf{Q}^*$ *e* $\mathbf{R}^*$.
Due numeri interi si possono moltiplicare tra di loro. L'elemento neutro è 1. Ma $\mathbf{Z}$ non è un gruppo per la moltiplicazione perché mancano gli inversi moltiplicativi. Per esempio, se $x \in \mathbf{Z}$ fosse l'inverso di 2, allora sarebbe $2x = 1$ e questa equazione non ha soluzioni in $\mathbf{Z}$. In $\mathbf{Q}$ e $\mathbf{R}$ invece, ogni elemento $a \neq 0$ ha un inverso. Definiamo

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

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

**Esempio (1.3).** *I numeri complessi* $\mathbf{C}$.
L'insieme dei numeri complessi $\mathbf{C}$ è definito come

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

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 $\mathbf{C}$ diventa un gruppo per l'addizione. L'elemento neutro è $0 = 0 + 0i$. L'insieme $\mathbf{C}$ 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

$1 \in \mathbf{C}$ ha la proprietà $1 \cdot (a+bi) = (a+bi) \cdot 1 = a+bi$. Siccome 0 soddisfa $0 \cdot (a+bi) = 0$ per ogni $a+bi \in \mathbf{C}$, non può avere un inverso moltiplicativo. Per questa ragione poniamo

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

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

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

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

Similmente si verifica che $\mathbf{C}^*$ è chiuso rispetto alla moltiplicazione: siano $a+bi, c+di \in \mathbf{C}^*$. 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.

**Esempio (1.4).** *I Quaternioni* $\mathbf{H}$ *di Hamilton.*
L'insieme $\mathbf{H}$ dei quaternioni di Hamilton è definito come

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

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

$$\begin{gathered}
i^2 = j^2 = k^2 = -1 \\
ij = k \qquad jk = i \qquad ki = j, \\
ji = -k \qquad kj = -i \qquad ik = -j.
\end{gathered}$$

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

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

ed il prodotto

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

Si pussono memorizzare le regole per la moltiplicazione con questo disegno:

moltiplicando due elementi in senso orario si ottiene il terzo con il segno "+" e moltiplicando in senso antiorario con il segno "-".

I quaternioni $\mathbf{H}$ formano un gruppo additivo. Lasciamo la verifica al lettore. L'insieme $\mathbf{H}^* = \mathbf{H} - \{0\}$ dei quaternioni non zero è un gruppo per la moltiplicazione. Siccome $ij \neq ji$, il gruppo $\mathbf{H}^*$ non è commutativo. Si può verificare l'associatività in modo diretto. Per un metodo più efficiente veda l'Eserc.1.H. Gli altri assiomi si verificano come nel caso di $\mathbf{C}^*$, 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.

**Esempio (1.5).** *Il gruppo $Q$ dei quaternioni.*
Il gruppo $Q$ è un sottoinsieme di 8 elementi di $\mathbf{H}^*$:

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

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

**Esempio (1.6).** *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.

**Esempio (1.7).** *Il gruppo* $\mathbf{Z}/n\mathbf{Z}$ *delle classi resto modulo* $n$.
Sia $n \in \mathbf{Z}$ un intero positivo. Per $k \in \mathbf{Z}$, con $0 \leq k < n$, definiamo

$$R_k = \{a \in \mathbf{Z} : \ k \text{ è il resto della divisione di } a \text{ per } n\} \qquad \text{per } 0 \leq k < n.$$

Per il Teorema 0.1 si ha $\mathbf{Z} = R_0 \cup R_1 \cup \ldots R_{n-1}$ 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 $a, b \in \mathbf{Z}$ si ha che $\overline{a} = \overline{b}$ se e soltanto $a$ e $b$ hanno lo stesso resto della divisione per $n$ e questo è equivalente a dire che $n$ divide $a - b$ (vedi Eserc.1.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 $a \equiv b \pmod{n}$.

Definiamo

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

o, equivalentemente,

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

Dunque, gli elementi di $\mathbf{Z}/n\mathbf{Z}$ sono *sottoinsiemi di* $\mathbf{Z}$. Mettiamo una struttura di gruppo additivo su $\mathbf{Z}/n\mathbf{Z}$. 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 $\mathbf{Z}$ 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 $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$:

$$\begin{matrix} \overline{0} + \overline{a} = \overline{0 + a} = \overline{a}, \\ \overline{a} + \overline{0} = \overline{a + 0} = \overline{a} \end{matrix}.$$

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

$$\begin{aligned} \overline{-a} + \overline{a} &= \overline{(-a) + a} = \overline{0}, \\ \overline{a} + \overline{-a} &= \overline{a + (-a)} = \overline{0}. \end{aligned}$$

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

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

il gruppo delle classi resto modulo $n$ è commutatitivo.

**Esempio (1.8).** *Il gruppo moltiplicativo* $(\mathbf{Z}/n\mathbf{Z})^*$ *delle classi resto modulo* $n$.
Sia $n$ un intero positivo. Definiamo

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

Se $\overline{a'} = \overline{a}$ si ha che $n$ divide $a' - a$ esiste dunque $k \in \mathbf{Z}$ tale che $a' - a = kn$. Per la Prop.0.2*(iii)* si ha $\mathrm{mcd}(a', n) = \mathrm{mcd}(a + kn, n) = \mathrm{mcd}(a, n)$. Questo dimostra che l'insieme $(\mathbf{Z}/n\mathbf{Z})^*$ 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 $(\mathbf{Z}/n\mathbf{Z})^*$. 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 $k, l \in \mathbf{Z}$. 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 $\mathbf{Z}/n\mathbf{Z}$, dall'associatività in $\mathbf{Z}$. Si verifica che l'elemento neutro è la classe $\overline{1}$. Dimostriamo che ogni classe $\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^*$ ha un inverso: siccome $\mathrm{mcd}(a, n) = 1$, esistono, per il Cor.0.4, 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 $(\mathbf{Z}/n\mathbf{Z})^*$ è un gruppo moltiplicativo. Definiamo

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

La funzione $\varphi$ si dice la *funzione di Eulero*. Si vede che $\varphi(n) = \#\{a \in \{1, 2, \ldots, n\} : \mathrm{mcd}(a, n) = 1\}$. Per $n = 12$ si trova la seguente tavola:

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

Si vede che è la "stessa" tavola del gruppo di Klein (1.5). Siccome la moltiplicazione di $(\mathbf{Z}/12\mathbf{Z})^*$ è associativa, abbiamo gratis una dimostrazione dal fatto che la composizione del gruppo $V_4$ di Klein è associativa.

**Esempio (1.9).** *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 $\mathbf{R}^n$ 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 $\mathbf{R}^n$ 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 $\mathbf{C}^n$. Per $\mathbf{v} = (v_1, \ldots, v_n)$ e $\mathbf{w} = (w_1, \ldots, w_n)$ in $\mathbf{C}^n$ si definisce la somma come nel caso di $\mathbf{R}$. Per la teoria degli spazi vettoriali su $\mathbf{R}$ e $\mathbf{C}$ si veda il corso di geometria I.

**Esempio (1.10).** *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 $\mathrm{id}_X$, 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 3 per i gruppi $S_n$.

**Esempio (1.11).** *Il gruppo ortogonale $O_2(\mathbf{R})$.*
Una *isometria* $A$ del piano $\mathbf{R}^2$ è una mappa $A : \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ che rispetta l'usuale distanza $d(P, Q)$ fra punti $P, Q \in \mathbf{R}^2$, cioè $d(A(P), A(Q)) = d(P, Q)$ per ogni $P, Q \in \mathbf{R}^2$.

In questo esempio studiamo le isometrie che fissano l'origine $\mathbf{0} = (0, 0)$ di $\mathbf{R}^2$. Definiamo

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

L'applicazione identica è in $O_2(\mathbf{R})$. La composizione di due elementi di $O_2(\mathbf{R})$ è in $O_2(\mathbf{R})$. Esempi di elementi di $O_2(\mathbf{R})$ sono *rotazioni* $R_\alpha$ con centro $\mathbf{0}$ e angolo $\alpha$. Altri esempi sono le *riflessioni* $S_\ell$ lungo una retta $\ell$ passante per $\mathbf{0}$.

Siano $\mathbf{e}_1 = (1, 0)$ ed $\mathbf{e}_1 = (0, 1)$ gli usuali vettori in $\mathbf{R}^2$.

**Lemma.** *Sia $A \in O_2(\mathbf{R})$*
*(i) Se $A(\mathbf{e_1}) = \mathbf{e}_1$ e $A(\mathbf{e}_2) = \mathbf{e}_2$ allora $A$ è l'applicazione identica.*
*(ii) Se $A(\mathbf{e}_1) = \mathbf{e}_1$ allora*

$$A(\mathbf{e}_2) = \pm \mathbf{e}_2.$$

**Dimostrazione.** *(i)* Sia $P = (x, y) \in \mathbf{R}^2$ un punto arbitrario e sia $(x', y') = A(P)$. Siccome $A$ è una isometria, abbiamo

$$\begin{aligned} d(A(P), \mathbf{0}) &= d(P, \mathbf{0}), \\ d(A(P), \mathbf{e}_1) &= d(P, \mathbf{e}_1), \\ d(A(P), \mathbf{e}_2) &= d(P, \mathbf{e}_2), \end{aligned}$$

cioè

$$\begin{aligned} x'^2 + y'^2 &= x^2 + y^2, \\ (x' - 1)^2 + y'^2 &= (x - 1)^2 + y^2, \\ x'^2 + (y' - 1)^2 &= x^2 + (y - 1)^2. \end{aligned}$$

Sottraendo la prima equazione dalle altre due otteniamo $x' = x$ e $y' = y$, come richiesto.
*(ii)* Abbiamo $A(\mathbf{0}) = \mathbf{0}$ e $A(\mathbf{e}_1) = \mathbf{e}_1$. Dunque per il vettore $A(\mathbf{e}_2)$ abbiamo

$$\begin{aligned} d(A(\mathbf{e}_2), \mathbf{0}) &= d(\mathbf{e}_2, \mathbf{0}) = 1, \\ d(A(\mathbf{e}_2), \mathbf{e}_1) &= d(A(\mathbf{e}_2), A(\mathbf{e}_1)) = d(\mathbf{e}_2, \mathbf{e}_1) = \sqrt{2}. \end{aligned}$$

Dunque, $A(\mathbf{e}_2)$ è nell'intersezione di due cerchi: uno con centro $\mathbf{0}$ e raggio 1 e uno con centro $\mathbf{e}_1$ e raggio $\sqrt{2}$.

Ci sono allora due possibilità per $A(\mathbf{e}_2)$: può essere $A(\mathbf{e}_2) = \mathbf{e}_2$ oppure $A(\mathbf{e}_2) = -\mathbf{e}_2$. Questo completa la dimostrazione del lemma.

**Corollario.** *Ogni isometria in $O_2(\mathbf{R})$ è una rotazione $R_\alpha$ o una riflessione $S_\ell$ lungo una retta $\ell$ per $\mathbf{0}$.*

**Dimostrazione.** Sia $A \in O_2(\mathbf{R})$. Abbiamo

$$d(A(\mathbf{e}_1), \mathbf{0}) = d(A(\mathbf{e}_1), A(\mathbf{0})) = d(\mathbf{e}_1, \mathbf{0}) = 1.$$

Dunque l'immagine $A(\mathbf{e}_1)$ di $\mathbf{e}_1$ è sulla circonferenza di raggio 1 in $\mathbf{R}^2$. Sia $\alpha$ l'angolo fra $\mathbf{e}_1$ e $A(\mathbf{e}_1)$. Poniamo

$$B = R_{-\alpha}A$$
$$B' = S_\ell A$$

dove $S_\ell$ è la riflessione lunga la retta $\ell$ che forma l'angolo $\alpha/2$ con il semiasse positivo delle ascisse. Si vede facilmente che

$$B(\mathbf{e}_1) = B'(\mathbf{e}_1) = \mathbf{e}_1.$$

Studiamo adesso l'isometria $B$. Per il lemma precedente abbiamo $B(\mathbf{e}_2) = \pm\mathbf{e}_2$. Se è $B(\mathbf{e}_2) = \mathbf{e}_2$, allora ancora per il lemma, $B$ è l'applicazione identica e dunque $A = R_\alpha$.

Se invece $B(\mathbf{e}_2) = -\mathbf{e}_2$, allora l'isometria $S_{y=0}B$ fissa i vettori $\mathbf{e}_1$ e $\mathbf{e}_2$. Per il lemma abbiamo che il prodotto $S_{y=0}B$ di $B$ per la rifflessione $S_{y=0}$ é l'identità, cioè $A = R_\alpha S_{y=0}$. In particolare, $A$ è una biiezione. Per mostrare che $A$ è una riflessione, utilizziamo la mappa $B'$.

Per il lemma abbiamo $B'(\mathbf{e}_2) = \pm\mathbf{e}_2$. Se è $B'(\mathbf{e}_2) = -\mathbf{e}_2$, allora la biiezione $B'B^{-1}$ fissa i vettori $\mathbf{e}_1$ ed $\mathbf{e}_2$. Per il lemma abbiamo $B'B^{-1} = \mathrm{id}_{\mathbf{R}^2}$ e dunque $B' = B$. Allora $R_\alpha A = S_\ell A$

e quindi, siccome $A$ è una biiezione, $R_\alpha = S_\ell$. Ma questo è assurdo: una rotazione non è una riflessione perché gli insiemi dei punti fissi delle due isometrie sono diversi.

Concludiamo che $B'(\mathbf{e}_2) = \mathbf{e}_2$ e dunque $B' = S_\ell A$ è l'applicazione identica. Questo implica che $A$ è uguale alla riflessione $S_\ell$, come richiesto.

Abbiamo visto, in particolare, che gli elementi di $O_2(\mathbf{R})$ sono biiezioni. L'inverso di una isometria che fissa $\mathbf{0}$ è una isometria che fissa $\mathbf{0}$. Concludiamo che $O_2(\mathbf{R})$ è un gruppo con la composizione.

**Esempio (1.12).** *Il gruppo diedrale $D_n$.*
Sia $n$ un intero positivo. Sia $\Delta_n$ l'$n$-gono regolare in $\mathbf{R}^2$ con centro $\mathbf{0}$ e un vertice in $\mathbf{e}_1$. Per esempio, per $n = 5$ si trova il pentagono regolare:

Definiamo il gruppo *diedrale* $D_n$

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

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 $R_\alpha$ per $\alpha = 0, 2\pi/n, 4\pi/n, \ldots, 2(n-1)\pi/n$. Inoltre, $D_n$ contiene certe riflessioni per rette passanti per $\mathbf{0}$. Vediamo prima le riflessioni per le 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. Poi, per $n$ pari, ci sono anche le $n/2$ riflessioni per le rette passanti per $\mathbf{0}$ e per il punto medio di un lato.

In questo modo troviamo $2n$ elementi diversi in $D_n$. Si prova, con una dimostrazione analoga a quella data nell'Esempio 1.11 che non ci sono altri elementi di $O_2(\mathbf{R})$ che trasformano l'$n$-gono in se stesso. Cioè $\#D_n = 2n$. Si veda l'Eserc.1.R per una presentazione efficiente di $D_n$.

**Esercizi.**

(1.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) $G = \mathbf{R}$, $a \circ b = a + b + 3$,
- (iii) $G = \mathbf{R}_{>1}$, $a \circ b = a^{\log(b)}$.
- (iv) $G = \{-1, 0, 1\}$, $a \circ b = a + b$.
- (v) $G = \{1, 2, 3, 4, \ldots\}$, $a \circ b = \max(a, b)$.
- (vi) $G = \mathbf{R}^2$, $\binom{a}{b} \circ \binom{c}{d} = \binom{c+ad}{bd}$.
- (vii) $G = \{0, 1, 2, 3, 4, 5\}$ e la composizione $a \circ b$ e data dalla seguenta tavola. La composizione $a \circ b$ e 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 |

(1.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 $e' = e$.

(1.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.

(1.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

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

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

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

Dimostrare che $G$ è un gruppo con elemento neutro $e$.

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

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

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

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

(1.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.

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

(i) Far vedere che

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

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

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

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

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

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

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

(i) Far vedere che

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

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

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

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

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

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

(i) Sia $\alpha \in \mathbf{C}$ e sia $\overline{\alpha}$ il coniugato di $\alpha$. (Veda Es.1.F). Far vedere

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

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

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

(1.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 $V_4$.

(1.L) Sia $n$ un intero positivo e siano $a, b \in \mathbf{Z}$. 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) $a \equiv b \pmod{n}$.

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

(1.N)* Sia $G$ l'insieme $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. 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.
(ii) Dimostrare che $x^3 = e$ per ogni $x \in G$.

(1.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 $n \in \mathbf{Z}$. 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 $a^{-2}b^{-2} = (ab)^{-2}$.

(1.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 $a = b = e$.

(1.Q) *Il gruppo* $O_2(\mathbf{R})$.

(i) Siano $\ell$ e $\ell'$ due rette passanti per $\mathbf{0}$. Sia $S_\ell$ la riflessione lungo la retta $\ell$ e $S_{\ell'}$ la riflessione lungo la retta $\ell'$. Dimostrare che

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

dove $\alpha$ è l'angolo tra $\ell$ ed il semiasse positivo delle $x$ e $\beta$ quello tra $\ell'$ ed il semiasse positivo delle $x$. Come nell'esempio 1.13, $R_\varepsilon$ indica una rotazione con centro $\mathbf{0}$ di angolo $\varepsilon$.

(ii) Sia $S_\ell$ la riflessione lungo la retta $\ell$ e sia $\alpha$ l'angolo tra $\ell$ ed il semiasse positivo delle $x$. Dimostrare che

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

(1.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.

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

$$x \mapsto ax + b$$

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

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

(ii) È un gruppo commutativo?

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

(i) Dimostrare che queste trasformazioni formano un gruppo.

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

(1.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.

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

$$\alpha + \beta\ell$$

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

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

(Il coniugato $\overline{x}$ di un quaternione $x$ è stato definito nell'Eserc.1.H). Definiamo inoltre

$$\begin{aligned} \overline{\alpha+\beta\ell} &= \overline{\alpha}-\beta\ell \qquad & \alpha,\beta\in\mathbf{H},\\ \mathrm{N}(x) &= x\overline{x} & x\in\mathbf{O}. \end{aligned}$$

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

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

Le sfere $n$-dimensionali $S^n=\{(x_0,x_1,\ldots,x_n)\in\mathbf{R}^{n+1} : x_0^2+x_1^2+\ldots+x_n^2=1\}$ hanno certe notevoli proprietà geometriche solo per le dimensioni $n=1,3$ e 7. Si possono spiegare queste proprietà con le proprietà algebriche di **C**, **H** e **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.

(1.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 $B$ e 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.

## 2. Sottogruppi, omomorfismi, prodotti.

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

**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.

Per esempio, **Z** è un sottogruppo del gruppo additivo **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.

**Teorema (2.1).** *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 *(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.

**Esempi.**

(i) Sia $H \subset \mathbf{Z}$ l'insieme dei numeri pari. Ovviamente $H \neq \emptyset$ e $a - b \in H$ per ogni $a, b \in H$. Per il Teorema 2.1, l'insieme $H$ è un sottogruppo di $\mathbf{Z}$. L'insieme dei numeri dispari, invece, non è un sottogruppo di $\mathbf{Z}$, perché non contiene lo zero.

(ii) Se $x, y$ sono numeri reali positivi, il quoziente $x/y$ è positivo. Dunque, per il Teorema 2.1*(iii)*, l'insieme $\mathbf{R}_{>0}$ dei numeri reali positivi è un sottogruppo di $\mathbf{R}^*$.

(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 2.1*(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 sottoinsieme del gruppo $Q$ dei quaternioni.

(v) Sia $n$ un intero positivo. Sia $k \in \{1, 2, \ldots, n\}$ e sia $H$ il sottoinsieme di $S_n$ dato da

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

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

Un esempio di sottogruppo importante è il *centro* di un gruppo:

**Definizione.** 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 $G$. Con la seguente proposizione troviamo tutti i sottogruppi di $\mathbf{Z}$ e dei gruppi additivi $\mathbf{Z}/n\mathbf{Z}$.

**Teorema (2.3).**

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

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

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

*(ii) Sia* $n$ *un intero positivo. I sottogruppi di* $\mathbf{Z}/n\mathbf{Z}$ *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 $\mathbf{Z}$. 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 $d\mathbf{Z} \subset H$.

Affermiamo che è anche $H \subset d\mathbf{Z}$, 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 0.1:

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

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 $d\mathbf{Z}$ sono diversi fra loro perché sono caratterizzati da $d$: l'intero $d$ è l'elemento positivo minimo in $d\mathbf{Z}$.
*(ii)* Sia $H$ un sottogruppo di $\mathbf{Z}/n\mathbf{Z}$. Definiamo

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

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 $\mathbf{Z}$. Siccome $\overline{0} = \overline{n} \in H$ abbiamo $n \in H'$. Dunque $H' \neq \{0\}$ e per la prima parte abbiamo che $H' = d\mathbf{Z}$ 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)*.

**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 $G$.

**Esempi (2.4).**
(i) Sia $G = G' = \mathbf{R}^*$ e sia $f : \mathbf{R}^* \longrightarrow \mathbf{R}^*$ la funzione data da $f(x) = x^2$. Quest'omomorfismo è un endomorfismo. Non è un automorfismo perché non è suriettivo.
(ii) Sia $f : \mathbf{R}_{>0} \longrightarrow \mathbf{R}$ 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 $\mathbf{R}_{>0}$, con la moltiplicazione, e $\mathbf{R}$, 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 $f : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$ data da $a \mapsto \overline{a}$ è un omomorfismo.
(v) Sia $V_4$ il gruppo di Klein. L'applicazione $f : (\mathbf{Z}/12\mathbf{Z})^* \longrightarrow V_4$ 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 veda l'Esempio 1.8)
(vi) Sia $G$ un gruppo e sia $g \in G$. L'applicazione

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

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

**Teorema (2.5).** *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 $f(a^{-1}) = f(a)^{-1}$. Questo dimostra il Teorema 2.5.

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

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

L'*immagine* $f(G)$ è il sottoinsieme di $G'$ definito da

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

**Teorema (2.6).** *Siano $G$ e $G'$ gruppi con elementi neutri respettivamente $e$ 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 2.5, 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 2.1*(iii)*.
*(ii)* Per il Teorema (2.5), 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 2.1*(iii)*.
*(iii)* Supponiamo che $f$ sia iniettiva. Per il Teorema 2.5 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 $xy^{-1} \in \ker(f)$. Concludiamo che $xy^{-1} = e$ e dunque $x = y$. Questo finisce la dimostrazione del Teorema 2.6.

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

**Teorema (2.7).**
*(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.

Per ogni gruppo $G$ l'applicazione identica è un automorfismo di $G$, cioè un isomorfismo $G \longrightarrow G$. Allora ogni gruppo $G$ è isomorfo a se stesso. Questo fatto, combinato con il Teorema 2.7, implica che la relazione di isomorfismo è una relazione di equivalenza. Le classi di equivalenza si dicono *classi di isomorfismo*. Gruppi nella stessa classe, cioè gruppi che sono isomorfi, sono, dal punto di vista della teoria di gruppi, oggetti uguali.

**Definizione.** (*Prodotto*) 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* $G_2$.

**Esempio.**

(i) Prendiamo $G = G' = \mathbf{R}$. Allora $G \times G' = \mathbf{R} \times \mathbf{R}$ è isomorfo allo spazio vettoriale $\mathbf{R}^2$ dello Esempio 1.9.

(ii) Prendiamo $G = G' = \mathbf{Z}/2\mathbf{Z}$. La tavola di composizione del gruppo prodotto $G \times G'$, cioè di $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ è dato 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 (Es.1.6). Più precisamente l'applicazione data da

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

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

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

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

data da

$$a \pmod{n} \mapsto a \pmod{d}.$$

Utilizziamo la notazione $a \pmod{n}$ piuttosto di $\overline{a}$ per indicare la dipendenza da $n$. La definizione dell'applicazione canonica dipende, a priori della scelta dal rappresentante $a$ della classe $a \pmod{n}$. In realtà, essa è ben definita perché $d$ divide $n$. Infatti, se le classi di $a$ e $a'$ in $\mathbf{Z}/n\mathbf{Z}$ sono uguali, la differenza di $a$ e $a'$ è dividibile per $n$ (Eserc.1.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.

**Teorema (2.8).** *(Teorema cinese del resto) Siano $n, m$ due interi positivi con* $\mathrm{mcd}(n,m) = 1$. *Allora l'applicazione*

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

*data da*

$$f(a \pmod{nm}) = (a \pmod{n}, a \pmod{m})$$

*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 $a \pmod{nm} \in \ker(f)$. Abbiamo $a \equiv 0 \pmod{n}$ e $a \equiv 0 \pmod{m}$, cioè $n$ ed $m$ dividono $a$. Esistono quindi $u, v \in \mathbf{Z}$ tali che $a = un$ e $a = vm$.

Siccome $\mathrm{mcd}(n,m) = 1$, esistono per il Cor.0.4 due interi $x, y \in \mathbf{Z}$ 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 $a \equiv 0 \pmod{nm}$. Per il Teorema 2.6, l'omomorfismo $f$ è iniettivo. Siccome le cardinalità di $\mathbf{Z}/nm\mathbf{Z}$ e di $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ sono entrambe uguali a $nm$, si conclude che $f$ è una biiezione come richiesto.

**Corollario (2.9).** *(Teorema cinese del resto) Siano $n, m$ due interi positivi con* $\mathrm{mcd}(n,m) = 1$ *e siano $\alpha, \beta \in \mathbf{Z}$. Allora esiste $z \in \mathbf{Z}$ tale che*

$$z \equiv \alpha \pmod{n},$$
$$z \equiv \beta \pmod{m}.$$

*L'intero $z$ è unico modulo $nm$.*

**Dimostrazione.** La prima affermazione è equivalente alla suriettività della mappa $f$ del Teorema 2.8 e la seconda alla iniettività.

Anche se abbiamo dimostrato la suriettività della mappa $f$ nel Teorema 2.8 in modo indiretto, è facile trovare l'intero $z$ del Cor.2.9 esplicitamente: siano $x, y \in \mathbf{Z}$ tali che $nx + my = 1$. Poniamo

$$z = \beta nx + \alpha my.$$

Si verifica

$$\begin{aligned} z &\equiv \alpha my \equiv \alpha(1 - nx) \equiv \alpha \pmod{n}, \\ &\equiv \beta nx \equiv \beta(1 - my) \equiv \beta \pmod{n}. \end{aligned}$$

**Esercizi.**

(2.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 $G$.

(2.B) Determinare quali sottoinsiemi sono sottogruppi:
- (i) $\mathbf{Q}_{>0} \subset \mathbf{Q}^*$,
- (ii) $\{1, i, j, k\} \subset Q$,
- (iii) $\{\pm 1, \pm i\} \subset \mathbf{C}^*$
- (iv) $\{z \in \mathbf{C} : z\overline{z} = 1\} \subset \mathbf{C}^*$,
- (v) $D_d \subset D_n$ per $d$ un divisore positivo di $n \in \mathbf{Z}_{>0}$,
- (vi) $\{x \in \mathbf{Q}^* :$ esistono $a, b \in \mathbf{Q}$ tali che $x = a^2 + b^2\}$,

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

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

(2.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 $G = H_1 \cup H_2 \cup H_3$.

(2.E) Siana $G, G'$ 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 $G$.

(2.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 $G$.

(2.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 $D_n$.

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

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

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

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

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

(v) $\mathbf{Z}/10\mathbf{Z} \longrightarrow \mathbf{Z}/5\mathbf{Z}$ $\quad x \pmod{10} \mapsto x \pmod 5$,

(vi) $(\mathbf{Z}/10\mathbf{Z})^* \longrightarrow (\mathbf{Z}/5\mathbf{Z})^*$ $\quad x \pmod{10} \mapsto x \pmod 5$,

(vii) $\mathbf{R} \longrightarrow \mathbf{C}^*$ $\quad x \mapsto \cos(x) + \text{sen}(x)i$,

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

Quali sono iniettive e quali suriettive?

(2.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.

(2.J) Determinare i nuclei e le immagini degli omomorfismi nell'Eserc.2.H.

(2.K) Sia $G = \{f_{a,b} : a \in \mathbf{R}^*, b \in \mathbf{R}\}$ dove $f_{a,b}(x) = ax + b$ è detta trasformazione affine di $\mathbf{R}$ (si veda Eserc.1.S). Dimostrare che l'applicazione $F : G \longrightarrow \mathbf{R}$ data da $F(f) = f(0)$ è un omomorfismo. Determinare l'immagine ed il nucleo.

(2.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?

(2.M) Provare che

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

dove $P(X)$ è l'insieme dei sottoinsiemi dell'insieme $X$ di due elementi. (Si veda l'Eserc.1.K.)

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

(2.O) Sia $\Delta_3$ il triangolo equilatero con baricentro $\mathbf{0}$ dell'Esempio 1.12. Sia $X$ l'insieme dei tre vertici 1,2,3 di $\Delta_3$. Ogni elemento $A \in D_3$ induce una permutazione dei vertici di $\Delta_3$. Questo definisce un'applicazione

$$D_3 \longrightarrow S_3.$$

Dimostrare che si tratta di un isomorfismo.

(2.P) Sia $G$ un gruppo e siano $H$ e $H'$ due sottogruppi con le seguenti proprietà:

- $hh' = h'h$ per ogni $h \in H$, $h' \in H'$,
- $H \cap H' = \{e\}$,
- 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.

(2.Q) (i) Dimostrare che

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

(Sugg. Utilizzare l'Eserc.2.P)

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

(iii) Dimostrare che

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

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

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

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

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

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

(Sugg. Utilizzare l'Eserc.2.P)

(2.S) (i) Trovare $n \in \mathbf{Z}$ con $0 \leq n \leq 1000$ tale che

$$n \equiv 3 \pmod 7,$$
$$n \equiv 4 \pmod{11},$$
$$n \equiv 8 \pmod{13}.$$

Dimostrare che l'intero $n$ è unico.

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

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

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

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

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

(2.V)*(*Simmetrie del cubo.*) Sia $G$ il gruppo delle isometrie di $\mathbf{R}^3$ che trasformano un cubo con centro di gravità in $\mathbf{0}$ in se stesso. Sia $H \subset G$ l'insieme $\{\mathrm{id}_{\mathbf{R}^3}, \sigma\}$, dove $\sigma$ è la trasformazione $\mathbf{x} \mapsto -\mathbf{x}$ e sia $H'$ il sottoinsieme delle trasformazioni che rispettano l'*orientazione* di $\mathbf{R}^3$ (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

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

**3. Permutazioni.**

In questo paragrafo discuteremo i gruppi *simmetrici* $S_n$ introdotti nell'Esempio 1.10. Gli elementi di $S_n$ sono le biiezioni da $\{1, 2, \ldots, n\}$ a $\{1, 2, \ldots, n\}$. Esse vengono dette *permutazioni dell'insieme* $\{1, 2, \ldots, n\}$.

**Proposizione (3.1).** *La cardinalità di* $S_n$ *è* $n!$

**Dimostrazione.** Dobbiamo determinare quante sono le biiezioni $\sigma$ dall'insieme $\{1, 2, \ldots, n\}$ a $\{1, 2, \ldots, n\}$. 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.

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

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

$$\begin{aligned}
\sigma(a_1) &= a_2,\\
\sigma(a_2) &= a_3,\\
&\vdots\\
\sigma(a_{k-1}) &= a_k,\\
\sigma(a_k) &= a_1,\\
\sigma(x) &= x \qquad \text{se } x \notin \{a_1, a_2, \ldots, a_k\}.
\end{aligned}$$

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

**Esempio.** Prendiamo $n = 4$. La biiezione $\sigma$ data da

$$\begin{aligned}
1 &\mapsto 2 \qquad 2 \mapsto 3\\
3 &\mapsto 1 \qquad 4 \mapsto 4
\end{aligned}$$

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 $\sigma$ è 3. Non ogni permutazione è un ciclo. Per esempio la biiezione $\tau$ data da

$$\begin{aligned}
1 &\mapsto 2 \qquad 2 \mapsto 1\\
3 &\mapsto 4 \qquad 4 \mapsto 3
\end{aligned}$$

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

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

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 $\sigma$ e $\tau$ cicli disgiunti invece vale $\sigma\tau = \tau\sigma$ (si veda Eserc.3.F).

**Teorema (3.2).** *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 $x \in \{1, 2, \ldots, n\}$ e consideriamo il sottoinsieme

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

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 $\sigma^{-l}$ 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 $\sigma$ 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 $\sigma$, *ristretta a* $Z$, è un prodotto $\pi_1\pi_2 \ldots \pi_t$ di cicli disgiunti $\pi_i$. Su $Y$ la permutazione $\sigma$ è data dal ciclo $(x\, \sigma(x) \ldots \sigma^{k-1}(x))$ e questo ciclo è disgiunto dai cicli $\pi_i$. Quindi $\sigma$ 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 $\sigma$ è una biiezione. Questo dimostra 3.2.

**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 $\rho$ manda 1 in 6 e poi $\sigma$ 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:

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

Allo scopo di definire il *segno* di una permutazione in $S_n$ consideriamo l'insieme $\Omega$ delle funzioni da $\mathbf{Z}^n$ a $\mathbf{Z}$. Gli elementi di $\Omega$ 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 $\Omega$ 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

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

**Definizione.** Sia $\sigma \in S_n$. Il *segno* di $\sigma$ 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 $\sigma$ con $\varepsilon(\sigma) = 1$ si dicono *pari,* e quelle con $\varepsilon(\sigma) = -1$ *dispari.*

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

$$\begin{aligned}(\sigma(D))(X_1, X_2, X_3) &= D(X_2, X_1, X_3)\\ &= (X_2 - X_1)(X_3 - X_1)(X_3 - X_2)\\ &= -D(X_1, X_2, X_3)\end{aligned}$$

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

**Teorema (3.3).** *Siano $\sigma, \tau$ 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.

**Teorema (3.4).** *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 $\tau$ si ha $\varepsilon(\tau) = -1$. In generale, per ogni $k$-ciclo $\tau$ si ha $\varepsilon(\tau) = (-1)^{k-1}$.*
*(iii) Ogni permutazione è un prodotto di trasposizioni. Se $\sigma$ è il prodotto di $k$ trasposizioni allora $\varepsilon(\sigma) = (-1)^k$.*

**Dimostrazione.** Consideriamo la permutazione

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

Ovviamente, se $x \notin \{a_1, a_2, \ldots, a_k\}$, si ha $\sigma(x) = x$. Si verifica facilmente che $\sigma(a_i) = a_{i+1}$ per $1 \leq i < k$ e che $\sigma(a_k) = a_1$. Concludiamo che $\sigma$ ha lo stesso effetto del ciclo $(a_1\, a_2\, \ldots\, a_k)$. In altre parole si ha $\sigma = (a_1\, a_2\, \ldots\, a_k)$ come richiesto.
*(ii)* Sia $a \in \{1, 2, \ldots, n\}$ 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

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

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

Sia ora $k > 0$ un intero qualsiasi e sia $\sigma = (a_1\,a_2\,\ldots\,a_k)$ un $k$-ciclo. Per il Teorema 3.3, 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 3.2 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 $\varepsilon$ è un omomorfismo. Questo conclude la dimostrazione del teorema.

**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 2.6 l'insieme $A_n = \ker(\varepsilon)$ è un sottogruppo di $S_n$, che, per il Teorema 3.4, non contiene trasposizioni. Vale il seguente teorema:

**Teorema (3.5).** *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 3.4 ,$\sigma$ 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.

**Teorema (3.6).** *(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 1.10. 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

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

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 $gh = h$ 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 3.6.

Come esempio applichiamo il Teorema 3.6 al gruppo $V_4$ di Klein (Esempio.1.6). 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.**

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

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

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

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

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

(3.E) Siano $k, n \in \mathbf{Z}$, 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 $S_k \times S_{n-k}$.

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

(3.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.

(3.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 $\tau\sigma$.

(3.I) Sia $n$ un intero positivo e siano $\sigma\tau \in S_n$. Provare che:

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

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

(3.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 $(1\,a)$.

(3.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 $\sigma$ è un $p$-ciclo.

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

(3.M) Dimostrare che il centro di $S_n$ è banale.

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

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

(3.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.1.5). Sia $\tau$ 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 $n \geq 8$.

(3.Q) (i) Ecco il famoso puzzle di *Sam Lloyd* (statunitense noto per i suoi rompicapo, 1841–1911). Ci sono 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 | |

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

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

## 4. Generatori, ordine e indice.

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.

**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 $X$.

**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 $G$.

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

**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.

**Proposizione (4.1).** *Sia $G$ un gruppo e sia $x \in G$ di ordine finito $m$. Sia $n \in \mathbf{Z}$. 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 $\mathbf{Z}$ o a $\mathbf{Z}/m\mathbf{Z}$ per un intero positivo $m$.

**Teorema (4.2).** *Sia $G$ un gruppo e sia $x \in G$.*
*(i)* $< x > \cong \mathbf{Z}$ *se l'ordine di $x$ è infinito.*
*(ii)* $< x > \cong \mathbf{Z}/m\mathbf{Z}$ *se l'ordine di $x$ è $m$.*
*(iii) Se $G$ è ciclico allora $G \cong \mathbf{Z}$ oppure $G \cong \mathbf{Z}/m\mathbf{Z}$.*

**Dimostrazione.** *(i)* Consideriamo l'omomorfismo

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

dato da $f(n) = x^n$. (si veda l'Esempio 2.4.(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 iomomorfismo iniettivo. Segue che la mappa $f : \mathbf{Z} \longrightarrow < x >$ è un isomorfismo. *(ii)* Definiamo un'applicazione

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

con

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

Verifichiamo che $f$ è ben definita, cioè 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 $k \in \mathbf{Z}$. Adesso abbiamo

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

L'applicazione $f$ è ovviamente un omomorfismo suriettivo. Affermiamo che è anche iniettiva: sia $\overline{n}$ in $\ker(f)$. Allora $x^n = e$. Per la Prop.4.1, l'ordine $m$ divide $n$, cioè $\overline{n} = \overline{0}$. Concludiamo che $f$ è iniettiva.
*(iii)* è una consequenza immediata di *(i)* e *(ii)*. Questo completa la dimostrazione del Teorema 4.2.

**Corollario (4.3).** *Sia $G$ un gruppo e sia $x \in G$. Allora*

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

*cioè, l'ordine dell'elemento $x$ è uguale all'ordine dal gruppo generato da $x$.*

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

**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 $H$.

**Esempi.**

(i) Prendiamo $G = \mathbf{R}^*$ e $H$ il sottogruppo $\mathbf{R}^*_{>0}$. Se $x \in \mathbf{R}^*$ è positivo, allora la classe laterale $x\mathbf{R}^*$ è uguale a $\mathbf{R}^*_{>0}$. Se invece $x < 0$, la classe $x\mathbf{R}^*$ è uguale a $\mathbf{R}^*_{<0}$. 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 $\mathbf{R}^*$ è commutativo.

(ii) Prendiamo $G = \mathbf{Z}$ e $H = d\mathbf{Z}$ per un intero positivo $d$ (si veda il Teorema 2.3.). Il gruppo $\mathbf{Z}$ è un gruppo *additivo.* Abbiamo dunque per $a \in \mathbf{Z}$ la classe laterale

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

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

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

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

L'insieme $H$ è una retta per $\mathbf{0}$ in $\mathbf{R}^2$. 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

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

è una retta parallela a $H$. Dunque le classi laterali di $H$ sono esattamente le rette in $\mathbf{R}^2$ 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 veda che la classe laterale sinistra $aH$ non è uguale alla classe laterale destra $Ha$.

**Teorema (4.4).** *Sia $H$ un sottogruppo di un gruppo $G$.*
*(i) Siano $a, b \in G$. Allora $aH = bH$ se e soltanto se $a^{-1}b \in G$.*
*(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 $H$.*

**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 $z = ah = bh_1 \in aH \cap bH$. Dimostriamo che $aH = bH$: sia $x = ah_2$ per un $h_2 \in H$. Allora $x = ah_2 = (bh_1h^{-1})h_2 \in bH$. Viceversa: sia $x = bh_3 \in bH$ per $h_3 \in H$. Allora $x = bh_3 = (ahh_1{}^{-1})h_3 \in aH$.
*(iii)* Sia $x \in G$. Allora $x$ è contenuto nella classe laterale $xH$.
Questo finisce la dimostrazione del Teorema 4.4.

Si potrebbe dire che il Teorema 4.3 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, che è conseguenza dei punti *(ii)* e *(iii)* del teorema, è l'usuale partizione in classi di equivalenza.

Vale un analogo del Teorema 4.4 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 $ab^{-1} \in H$.

**Teorema (4.5).** *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 classaelaterale $aH = \{ah : h \in H\}$. 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!

**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.

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

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

*(ii)* Consideriamo, come nel secondo esempio di questo paragrafo, il sottogruppo $H = d\mathbf{Z}$ in $G = \mathbf{Z}$. Allora l'indice $[G : H]$ è $d$. Un sistema $S$ di rappresantanti 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 $[G : H] = 3$.

**Teorema (4.6).** *(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 rapppresentanti per le classi laterali sinistre di $H$. Per il Teorema 4.3 *(iii)*, le classi laterali sinistre $sH$ con rappresentanti in $S$ sono disgiunte ed il gruppo $G$ è l'unione delle classi laterali sinistre $sH$, $s \in S$. Allora

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

Per il Teorema 4.4 ogni classe laterale ha la stessa cardinalità di $H$. Concludiamo che

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

come richiesto.

**Corollario (4.7).** *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 $G$.

**Dimostrazione.** Le affermazioni seguono direttamente dal teorema precedente.

**Corollario (4.8).**
*(i) (P. de Fermat) Sia $p$ un numero primo e sia $x \in \mathbf{Z}$ tale che $p$ non divide $x$. Allora*

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

*(ii) (L. Eulero) Sia $n$ un intero positivo e si $x \in \mathbf{Z}$ con $\mathrm{mcd}(x, n) = 1$ e sia $\varphi$ la funzione di Eulero (Esempio.1.8). Allora*

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

**Dimostrazione.** *(i)* Sia $G$ il gruppo moltiplicativo $(\mathbf{Z}/p\mathbf{Z})^*$. Siccome $p$ non divide $x$, la classe $\overline{x}$ è in $(\mathbf{Z}/p\mathbf{Z})^*$. Per il Teorema 4.6*(ii)* l'ordine di $\overline{x}$ divide la cardinalità di $(\mathbf{Z}/p\mathbf{Z})^*$ cioè $\mathrm{ord}(x)$ divide $p - 1$. Segue dalla Prop.4.1 che

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

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

**Corollario (4.9).** *Sia $p$ un primo e sia $G$ un gruppo di ordine $p$. Allora*

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

**Dimostrazione.** Sia $x \in G$ un elemento diverso dall'elemento neutro. L'ordine di $x$ è dunque diverso da 1. Siccome $\mathrm{ord}(x)$ divide la cardinalità $p$ di $G$, vediamo che l'ordine di $x$ è $p$. Per il Teorema 4.2*(ii)*, il gruppo $H \subset G$ generato da $x$ è isomorfo a $\mathbf{Z}/p\mathbf{Z}$. Concludiamo che $\mathbf{Z}/p\mathbf{Z} \cong H = G$ come richiesto.

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

**Teorema (4.10).** *Sia $G$ un gruppo di ordine $\leq 5$. Allora*

$$\begin{aligned} G &\cong \mathbf{Z}/n\mathbf{Z} \qquad \text{con } n \leq 5, \text{ oppure} \\ &\cong V_4. \end{aligned}$$

**Dimostrazione.** Se $n = 1$ il gruppo $G$ è $\{e\}$. Per $n = 2, 3, 5$ il Cor.4.8 implica che $G$ è ciclico e dunque isomorfo a $\mathbf{Z}/n\mathbf{Z}$. 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 $G =< g > \cong \mathbf{Z}/4\mathbf{Z}$. 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.1.C), gli elementi nelle posizione con "?" sono determinati e ritroviamo la tavola del gruppo $V_4$ di Klein.

Questo finisce la dimostrazione.

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 $\mathbf{Z}/n\mathbf{Z}$. 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 2.7). Il gruppo simmetrico $S_3$ è isomorfo al gruppo diedrale $D_3$ (Eserc.2.N). Per l'Eserc.2.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 4.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.**

(4.A) Dimostrare
- (i) $D_n =< R, S >$, (Si veda l'Eserc.1.R.)
- (ii) $Q =< i, j >$,
- (iii) $(\mathbf{Z}/23\mathbf{Z})^* =< \overline{5} >$,
- (iv) $S_n =< (1\,2), (1\,2\,\ldots\,n) >$.

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

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

(4.D) Sia $G$ un gruppo e siano $a, b \in G$. Far vedere:
- (i) $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$.
- (ii) $\mathrm{ord}(a) = \mathrm{ord}(bab^{-1})$.
- (iii) $\mathrm{ord}(ab) = \mathrm{ord}(ba)$.

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

(4.F) (*la formula di Gauss*) Per la definizione della funzione $\phi$ si veda l'Esempio 1.8. Sia $n$ un intero positivo.
- (i) Dimostrare: $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ ha ordine $d$ se e soltanto se $\mathrm{mcd}(a, n) = n/d$.
- (ii) Quanti sono i generatori di $\mathbf{Z}/n\mathbf{Z}$?
- (iii) Far vedere che il numero delle classi $\overline{a}$ in $\mathbf{Z}/n\mathbf{Z}$ 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 $\{a \in \mathbf{Z}/n\mathbf{Z} : \mathrm{mcd}(a, n) = n/d\}$ a $(\mathbf{Z}/d\mathbf{Z})^*$.
- (iv) Concludere che

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

(4.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 $\mathrm{ord}(\alpha\beta) = ab$.

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

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

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

(4.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 $\text{mcm}(a, b)$.

(4.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 $\text{ord}(f(g))$ divide $\text{ord}(g)$.

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

(4.K) Dimostrare che

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

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

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

per ogni intero $k \geq 0$.

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

(4.M) Sia $n$ un intero positivo e sia $H$ il sottogruppo di $S_n$ definito nell'Eserc.3.E. Far vedere che l'ordine di $H$ è $k!(n-k)!$. Concludere che $k!(n-k)!$ divide $n!$.

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

(4.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 $1/83$.

(4.P) (*Numeri di Mersenne.*) Sia $p > 2$ un primo e sia $M_p = 2^p - 1$ un numero di Mersenne. (Si veda l'Eserc.0.Q) Dimostrare che ogni divisore di $M_p$ è congruente a 1 (mod $2p$). (Sugg. Sia $l$ un divisore primo di $M_p$. Calcolare l'ordine di $\overline{2}$ in $(\mathbf{Z}/l\mathbf{Z})^*$.)

(4.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.0.S)

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

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

(4.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.

(4.S) Sia $B = (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$. 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 $B \ncong D_6$.

(4.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 $G =< X >$.

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

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

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

(4.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.

**5. Azioni di gruppi.**

In questo paragrafo studiamo l'azione di un gruppo $G$ su un insieme $X$. Un esempio importante è il caso in cui $X = G$ e $G$ agisce su se stesso per coniugio. L'applicazione principale è il Teorema di Cauchy.

**Definizione.** Sia $G$ un gruppo e sia $X$ un insieme. Si dice che $G$ *agisce su* $X$ se ad ogni $g \in G$ e ogni $x \in X$ è associato un elemento $g \circ x \in X$ in modo tale che

$(A_1)$
$$e \circ x = x \qquad \textit{per ogni } x \in X.$$

$(A_2)$
$$(gh) \circ x = g \circ (h \circ x) \qquad \textit{per ogni } g, h \in G \textit{ ed ogni } x \in X.$$

*L'applicazione* $G \times X \longrightarrow X$ *data da* $(g, x) \mapsto g \circ x$ *si dice un'azione di* $G$ *su* $X$.

L'azione sopra definita, si dice un'*azione sinistra.* Un'*azione destra* è una mappa $X \times G \longrightarrow X$ data da $(x, g) \mapsto x \circ g$ tale che

$$x \circ e = x \qquad \text{e} \qquad x \circ (gh) = (x \circ g) \circ h.$$

Si veda l'Eserc.1.D per i rapporti fra azioni destre e sinistre. Nel seguito considereremo sempre azioni sinistre.

**Esempi. (5.1).**

(i) Sia $n$ un intero positivo. Prendiamo $G = S_n$ e $X$ l'insieme $\{1, 2, \ldots, n\}$. Nell'Esempio 1.10 abbiamo definito l'azione di $S_n$ su $X$ in modo seguente:
$$\sigma \circ x = \sigma(x) \qquad \text{per } \sigma \in S_n \text{ e } x \in X.$$

(ii) Il gruppo $G = O_2(\mathbf{R})$ agisce sull'insieme $X = \mathbf{R}^2$. Si veda l'Esempio 1.11.

(iii) Sia $G$ un gruppo e prendiamo $X = G$. Il gruppo $G$ agisce su se stesso per *traslazione*
$$g \circ x = gx \qquad \text{per ogni } g, x \in G.$$
È facile verificare che gli assiomi $(A_1)$ e $(A_2)$ valgono. Similmente, c'è un'azione destra di $G$ su $G$ definita da
$$x \circ g = xg \qquad \text{per ogni } g, x \in G.$$

(iii) (*coniugio.*) Un gruppo $G$ agisce su se stesso per *coniugio:*
$$g \circ x = gxg^{-1} \qquad \text{per ogni } g, x \in G.$$
È facile verificare che gli assiomi $(A_1)$ e $(A_2)$ valgono. Similmente, c'è un'azione destra di $G$ su $G$ definita da
$$x \circ g = g^{-1}xg \qquad \text{per ogni } g, x \in G.$$

(iv) Sia $H$ un sottogruppo di un gruppo $G$. Sia $X = G/H$ l'insieme delle classi laterali sinistre di $H$. Il gruppo $G$ agisce su $G/H$ come segue:
$$g \circ (aH) = (ga)H \qquad \text{per ogni } g, a \in G.$$

La definizione dell'azione di $G$ non dipende dalla scelta di $a$: se $aH = a'H$ allora, per il Teorema (4.3)*(i)*, si ha $a^{-1}a' \in H$. Questo implica che $(ga)^{-1}(ga') \in H$ e quindi $(ga)H = (ga')H$.
Similmente, c'è un'azione destra di $G$ sulle classi laterali destre definita da

$$(Ha) \circ g = H(ag) \qquad \text{per } a, g \in G.$$

**Teorema (5.2).** *Sia $G$ un gruppo che agisce su un insieme $X$. Allora*
*(i) Per ogni $g \in G$ la mappa $T_g : X \longrightarrow X$ data da*

$$T_g(x) = g \circ x$$

*è una biiezione.*
*(ii) L'applicazione $G \longrightarrow S(X)$ data da*

$$g \mapsto T_g$$

*è un'omomorfismo.*

**Dimostrazione.** *(i)* Per l'assioma $(A_1)$ la mappa $T_e$ è l'identità su $X$. Per $g, h \in G$ abbiamo, per $(A_2)$,

$$T_{gh}(x) = (gh) \circ x = g \circ (h \circ x) = T_g(T_h(x)).$$

In particolare

$$T_g T_{g^{-1}} = T_{gg^{-1}} = T_e = \mathrm{id}_X$$

e vediamo che la mappa $T_g$ ha una inversa ed è dunque una biiezione.
*(ii)* Abbiamo già visto che

$$T_{gh} = T_g T_h.$$

Questo finisce la dimostrazione.

Sia $G$ un gruppo che agisce su un insieme $X$. Due elementi $x, y \in X$ si dicono equivalenti sotto l'azione di $G$, notazione $x \sim_G y$, se esiste $g \in G$ tale che $y = g \circ x$.

**Lemma (5.3).** *La relazione $\sim_G$ è una relazione di equivalenza su $G$.*

**Dimostrazione.** Scriviamo $x \sim y$ per $x \sim_G y$. Per l'assioma $(A_1)$ abbiamo $x \sim x$ per ogni $x \in X$. La relazione $\sim$ è dunque *riflessiva.*
Se $x \sim y$ esiste $g \in G$ tale che $y = g \circ x$. Abbiamo

$$x = e \circ x = (g^{-1}g) \circ x = g^{-1} \circ (g \circ x) = g^{-1} \circ y$$

e concludiamo che $y \sim x$. La relazione è dunque *simmetrica.*
Finalmente, se $x \sim y$ e $y \sim z$ esistono $g, h \in G$ tali che $y = g \circ x$ e $z = h \circ y$. Vediamo che

$$z = h \circ y = h \circ (g \circ x) = (hg) \circ x$$

e dunque che $z \sim x$: la relazione è *transitiva.* Questo finisce la dimostrazione.

**Definizione.** Sia $G$ un gruppo che agisce su un insieme $X$. Le classi di equivalenza della relazione $\sim_G$ si dicono *le orbite di $G$ su $X$.* Le orbite sono sottoinsiemi disgiunti di $X$ la cui unione è uguale a $X$.

Per $x \in X$ si scrive $Gx$ l'orbita che contiene $x$:

$$Gx = \{g \circ x : g \in G\}.$$

Si dice che $G$ agisce *transitivamente* su $X$ se esiste una sola orbita. In questo caso c'è per ogni $x, y \in X$ un $g \in G$ tale che $g \circ y = x$.

Sia $G$ un gruppo che agisce su un insieme $X$. Per $x \in X$ lo *stabilizzatore* $G_x$ *di* $x$ è l'insieme

$$G_x = \{g \in G : g \circ x = x\}.$$

**Esempi.** Consideriamo gli esempi 5.1.

(i) Per ogni $a, b \in \{1, 2, \ldots, n\}$ esiste $\sigma \in S_n$ tale che $\sigma(a) = b$. Per esempio $\sigma = (a\, b)$ ha questa proprietà. Perciò che $S_n$ agisce transitivamente sull'insieme $\{1, 2, \ldots, n\}$. Lo stabilizzatore di un elemento $a \in \{1, 2, \ldots, n\}$ è l'insieme

$$(S_n)_a = \{\sigma \in S_n : \sigma(a) = a\}.$$

(ii) Sia $A \in O_2(\mathbf{R})$ e sia $P \in \mathbf{R}^2$. Allora la distanza tra $A(P)$ ed $\mathbf{0}$ è uguale a quella tra $P$ ed $\mathbf{0}$. Dunque le orbite dell'azione di $G = O_2(\mathbf{R})$ su $X = \mathbf{R}^2$ sono circonferenze con centro $\mathbf{0}$. Ovviamente, lo stabilizzatore di $\mathbf{0}$ è l'intero gruppo $O_2(\mathbf{R})$. Si verifica che lo stabilizzatore di un punto $P \neq \mathbf{0}$ contiene soltanto l'applicazione identica e la riflessione lungo la retta per $\mathbf{0}$ e $P$.

(iii) L'azione di $G$ su $X = G$ per traslazione è transitiva. Per ogni $x \in X$ lo stabilizzatore è banale, cioè uguale a $\{e\}$.

(iv) L'azione di $G$ su $X = G$ per coniugio è molto interessante. Le orbite si dicono *classi di coniugio.* In questo caso, l'orbita di $x \in G$ è uguale a

$$\{gxg^{-1} : g \in G\}.$$

Lo stabilizzatore di $x \in G$ si dice il *centralizzante* $C_x$ di $x$. Esso contiene gli elementi $g \in G$ tali che $g \circ x = gxg^{-1} = x$ cioè, tali che $gx = xg$:

$$C_x = \{g \in G : xg = gx\}.$$

**Teorema (5.4).** *Sia $G$ un gruppo che agisce su un insieme $X$. Sia $x \in X$. Allora*

*(i) Lo stabilizzatore $G_x$ è un sottogruppo di $G$.*

*(ii) Per ogni $g \in G$ si ha*

$$G_{g \circ x} = gG_xg^{-1} = \{ghg^{-1} : h \in G_x\}.$$

*(iii)*

$$\#(Gx) = [G : G_x].$$

**Dimostrazione.** *(i)* Per l'assioma $(A_1)$ abbiamo che $e \in G_x$. Dunque $G_x \neq \emptyset$. Poi, se $g, h \in G_x$ abbiamo per l'assioma $(A_2)$

$$(gh^{-1}) \circ x = (gh^{-1}) \circ (h \circ x) = (gh^{-1}h) \circ x = g \circ x = x$$

e quindi $gh^{-1} \in G_x$. Per il Teorema 2.1 concludiamo che $G_x$ è un sottogruppo di $G$.
*(ii)* Sia $h \in G_x$ e, dunque, $ghg^{-1} \in gG_xg^{-1}$. Abbiamo

$$(ghg^{-1}) \circ (g \circ x) = (ghg^{-1}g) \circ x = g \circ (h \circ x) = g \circ x$$

e quindi $ghg^{-1} \in G_{g \circ x}$. Dunque $gG_xg^{-1} \subset G_{g \circ x}$. Si dimostra l'inclusione opposta in modo simile.

*(iii)* Definiamo l'applicazione

$$F : G/G_x \longrightarrow Gx$$

con

$$gG_x \mapsto g \circ x.$$

Abbiamo $gG_x = hG_x$ se e soltanto se $h^{-1}g \in G_x$. Dunque $gG_x = hG_x$ se e soltanto se $(h^{-1}g)\circ x = x$, cioè se e soltanto se $g \circ x = h \circ x$. Concludiamo che l'applicazione $F$ è ben definita e iniettiva. Per la definizione dell'orbita $Gx$, la mappa $F$ è anche suriettiva e dunque biiettiva, come richiesto.

**Corollario (5.5).**

*(i) Sia $G$ un gruppo che agisce su un insieme $X$. Sia $Y \subset X$ un insieme che contiene esattamente un elemento in ogni orbita di $G$. Allora*

$$\#X = \sum_{x \in Y} [G : G_x].$$

*(ii) (Equazione delle classi) Sia $G$ un gruppo. Allora*

$$\#G = \sum_{g \in Y} [G : C_g]$$

*dove $Y$ è un sottoinsieme di $G$ che contiene esattamente un elemento in ogni classe di coniugio di $G$.*

**Dimostrazione.** *(i)* Siccome $X$ è unione disgiunta delle orbite di $G$ abbiamo

$$\#X = \sum_{x \in Y} \#(Gx).$$

Il risultato segue ora dal Teorema 5.4.
*(ii)* Questa parte è un caso particolare die *(i)* dove ora $G$ agisce su $X = G$ via coniugio.

**Corollario (5.6).** *Siano $p$ un numero primo e $G$ un gruppo di ordine una potenza di $p$. Sia $X$ un insieme sul quale $G$ agisce. Allora*

$$\#X \equiv \#X^G \pmod{p}$$

*dove $X^G$ indica l'insieme dei punti fissi di $G$:*

$$X^G = \{x \in X : g \circ x = x \text{ per ogni } g \in G\}.$$

**Dimostrazione.** Per il Teorema 5.4, un'orbita $Gx$ di $G$ ha cardinalità $[G : G_x]$. Dunque, per il Teorema 4.5 di Lagrange, la cardinalità di $Gx$ divide $\#G$ e quindi ogni orbita ha cardinalità una potenza di $p$. Un'orbita $Gx$ ha cardinalità $p^0 = 1$ se e soltanto se

$$\{g \circ x : g \in G\} = \{x\}$$

cioè se e soltanto se $x$ è un punto fisso. Le altre orbite $Gx$ soddisfano $\#(Gx) \equiv 0 \pmod{p}$. Il risultato segue adesso dal fatto che $X$ è riunione delle orbite di $G$.

**Teorema (5.7).** *(A. Cauchy) Sia $p$ un numero primo e sia $G$ un gruppo finito tale che*

$$p \quad \textit{divide} \quad \#G.$$

*Allora $G$ contiene un elemento di ordine $p$.*

**Dimostrazione.** Sia $X$ l'insieme dato da

$$X = \underbrace{G \times G \times \ldots \times G}_{p}.$$

Consideriamo il sottoinsieme

$$X^0 = \{(g_1, g_2, \ldots, g_p) \in X : g_1 \cdot g_2 \cdot \ldots \cdot g_p = e\}$$

Il gruppo $\mathbf{Z}/p\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ agisce su $X^0$ via "permutazioni cicliche":

$$\overline{a} \circ (g_1, g_2, \ldots, g_p) = (g_{1+a}, g_{2+a}, \ldots, g_{(p-1)+a})$$

prendendo gli indici (mod $p$). Si verifica che il prodotto $g_{1+a}, g_{2+a} \cdot \ldots \cdot g_{(p-1)+a}$ è uguale a $e$. È facile verificare che gli assiomi $(A_1)$ e $(A_2)$ valgono.

Per il Cor.5.5 il numero dei punti fissi di $G$ è congruente a $\#X^0$ modulo $p$. Siccome $\#X^0 = \#G^{p-1} \equiv 0 \pmod{p}$ vediamo che $\#(X^0)^G \equiv 0 \pmod{p}$. Ma l'azione ha sicuramente un punto fisso, cioè $(e, e, \ldots, e)$ e allora ne ha almeno un altro! Sia $x = (g_1, g_2, \ldots, g_p)$ un altro punto fisso. Siccome $x$ è fisso sotto l'azione di $\mathbf{Z}/p\mathbf{Z}$ abbiamo $g_1 = g_2 = \ldots = g_p$ e dunque, dalla relazione $g_1 \cdot g_2 \cdot \ldots \cdot g_p = e$ si ottiene

$$g_1^p = e.$$

Siccome $x \neq (e, e, \ldots, e)$, abbiamo $g_1 \neq e$ e la dimostrazione è completa.

Come applicazione del Teorema 5.7 dimostriamo che, a meno di isomorfismo, esistono soltanto due gruppi di ordine 6. La proposizione seguente insieme al Cor.4.9 ed al Teorema 4.10 ci permette così determinare tutte le classi di isomorfismo di gruppi di ordine al più 7.

**Proposizione (5.8).** *Sia $G$ un gruppo di ordine 6. Allora*

$$G \cong \mathbf{Z}/6\mathbf{Z} \qquad \textit{oppure} \qquad G \cong S_3.$$

**Dimostrazione.** Per il teorema di Cauchy, esiste un elemento $x \in G$ di ordine 2 ed un elemento $y \in G$ di ordine 3. Si vede facilmente che gli elementi

$$y^j x^i \qquad 0 \leq j \leq 2, \quad 0 \leq j \leq 1$$

sono tutti distinti. Dunque

$$G = \{e, y, y^2, x, yx, y^2x\}.$$

Consideriamo l'elemento $x^{-1}yx \in G$. Se fosse $x^{-1}yx = y^j x$, allora $x = y^{1-j}$ che è impossibile. Dunque $x^{-1}yx = y^j$ per $j = 0, 1$ oppure 2. Siccome $j$ non può essere 0, ci sono due possibilità:
*Caso $j = 1$.* In questo caso abbiamo $xy = yx$. Si verifica senza problemi che l'elemento $xy$ ha ordine 6. Per il Teorema 4.2, il sottogruppo generato da $xy$ è isomorfo a $\mathbf{Z}/6\mathbf{Z}$. Concludiamo che $G =< xy > \cong \mathbf{Z}/6\mathbf{Z}$.

*Caso* $j = 2$. Abbiamo $yx = xy^2 = xy^{-1}$. Sia $X$ l'insieme delle classi laterali sinistre del sottogruppo $H$ generato da $x$. Dunque $X$ contiene 3 elementi:

$$X = \{H = \{e, x\}, yH = \{y, yx\}, y^2H = \{y^2, y^2x\}\}.$$

Adesso facciamo agire $G$ su $X$ per moltiplicazione a sinistra. Per il Teorema 5.2 questo ci dà un omomorfismo

$$f : G \longrightarrow S(X) \cong S_3.$$

Verifichiamo che $f$ è un'isomorfismo: Sia $g \in G$ nel nucleo di $f$. Allora, in particolare $gH = H$ e dunque $g = e$ oppure $g = x$. Per eliminare la possibilità $g = x$ consideriamo la classe $yH$. Siccome $gyH = yH$, abbiamo $xy = y$ oppure $xy = yx$. L'uguaglianza $xy = y$ è evidentemente impossibile e la relazione $xy = yx$ dà, con $yx = xy^2$, la relazione $xy = xy^2$ che è assurda. Concludiamo che $g \neq x$ e quindi $g = e$.

L'applicazione $G \longrightarrow S_3$ è dunque iniettiva. Siccome i gruppi $G$ e $S_3$ hanno entrambi ordine 6, vediamo che $f$ è una biiezione e concludiamo che $G \cong S_3$ come richiesto.

**Esercizi.**

(5.A) Sia $(x, g) \mapsto x \circ g$ un'azione destra $X \times G \longrightarrow X$ di $G$ su $X$. Dimostrare che $G \times X \longrightarrow X$ data da $(g, x) \mapsto x \circ g^{-1}$ è un'azione sinistra di $G$ su $X$.

(5.B) Sia $G$ un gruppo che agisce su un insieme $X$. Sia

$$F : G \longrightarrow S(X)$$

l'applicazione del Teorema 5.2. Dimostrare

$$\ker(F) = \cap_{x \in X} G_x.$$

(5.C) Sia $H$ un sottogruppo di un gruppo $G$. Sia $g \in G$. Far vedere:

$$[G : H] = [G : gHg^{-1}].$$

(5.D) Sia $G$ un gruppo. Dimostrare che $x, y \in G$ sono elementi coniugati se e soltanto se esistono $a, b \in G$ tali che $x = ab$ e $y = ba$.

(5.E) Siano $\sigma, \tau \in S_n$. Far vedere che $\sigma$ e $\tau$ sono coniugate se e soltanto se nella loro decomposizione in prodotto di cicli disgiunti (Teorema 3.2), c'è lo stesso numero di $k$-cicli hanno, per ogni $k$.

(5.F) Determinare le classi di coniugio in $S_n$ per $n \leq 5$. Far vedere che in $A_4$ esistono 3-cicli che non sono coniugati.

(5.G) Sia $n$ un intero positivo. Far vedere: per $n$ dispari tutte le riflessioni in $D_n$ sono coniugate, ma per $n$ pari, ci sono due distinti classi di coniugio.

(5.H) Sia $G$ un gruppo che agisce transitivamente su un insieme $X$ di almeno due elementi. Dimostrare che esiste un elemento $g \in G$ tale che per ogni $x \in X$ si ha $g \circ x \neq x$.

(5.I) Sia $p$ un primo e $G$ un gruppo con $\#G \equiv 0 \pmod{p}$. Sia $k$ il numero degli elementi di $G$ di ordine $p$ e sia $l$ il numero dei sottogruppi di $G$ di ordine $p$. Far vedere

$$\begin{aligned} k &\equiv -1 \pmod{p}, \\ k &= (p-1)l, \\ l &\equiv 1 \pmod{p}. \end{aligned}$$

(5.J) Sia $p$ un primo. provare che se $S_n$ contiene un elemento di ordine $p^2$, allora $p^2$ divide $n$.

(5.K) Sia $G$ un gruppo finito con due sole classi di coniugio. Dimostrare che $\#G = 2$.

(5.L)*(*Formula di Burnside*) Sia $G$ un gruppo finito che agisce su $X$. Definiamo per $g \in G$

$$n(g) = \#\{x \in X : g \circ x = x\}.$$

Dimostrare che il *numero* delle orbite di $G$ è dato da

$$\frac{1}{\#G} \sum_{g \in G} n(g).$$

(5.M) Sia $G$ un $p$-gruppo finito, cioè un gruppo la cui cardinalità è una potenza di un numero primo $p$. Dimostrare che il centro $Z(G)$ di $G$ non è banale. (Sugg. Considerare l'azione di $G$ su $X = G$ per coniugio. Utilizzare il Cor.5.6.)

(5.N) Sia $p$ un primo e sia $G$ un gruppo di ordine $p^2$. Dimostrare che $G$ è abeliano. (Sugg. Utilizzare l'Eserc.5.M per trovare $e \neq x \in Z(G)$. Poi far vedere che $G =< x, y >$ per un elemento $y \in G$.)

(5.O) Sia $G$ un gruppo e sia $g \in G$ Si consideri l'applicazione

$$T_g : G \longrightarrow G$$

in $S(G)$ data da $T_g(x) = gx$ (Si veda Teorema 5.2).

(i) Dimostrare che $T_g$ è il prodotto di $[G :< g >]$ cicli di lunghezza $\mathrm{ord}(g)$.

(ii) Dimostrare che $T_g$ è una permutazione dispari se e soltanto se $\#G$ è pari e l'indice $[G :< g >]$ è dispari.

(iii) Supponiamo che $\#G = 2m$ dove $m$ è dispari. Dimostrare che $T_g$ è una permutazione pari se e soltanto se $\mathrm{ord}(g)$ è dispari. Concludere che gli elementi di $G$ di ordine dispari formano un sottogruppo di $G$ di indice 2.

(5.P) Sia $G$ un gruppo finito di ordine $2^k \cdot m$ con $m$ dispari. Supponiamo che $G$ contenga un elemento di ordine $2^k$. Provare che gli elementi di $G$ di ordine dispari formano un sottogruppo di $G$ di ordine $m$. (Sugg. Utilizzare l'Eserc.5.O)

## 6. Sottogruppi normali. Gruppi quozienti.

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 $\mathbf{Z}/n\mathbf{Z}$ delle classi resto modulo $n$: se si prende $G = \mathbf{Z}$ e $N = n\mathbf{Z}$ si ritrova il gruppo $G/N = \mathbf{Z}/n\mathbf{Z}$ di 1.7.

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

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

**Esempi (6.1).**

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

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

(iii) Il centro $Z(G)$ (Si veda Esempio 2.2(v)) 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 $\tau\sigma\tau^{-1} \in A_n$.

(v) Sia $G$ un gruppo e sia $[G, G]$ il sottogruppo di $G$ generato dai *commutatori* $[g, h] = ghg^{-1}h^{-1}$ dove $g, h \in G$. Per mostrare che $[G, G]$ è un sottogruppo normale, prendiamo $h \in [G, G]$ 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.

**Teorema (6.2).** *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

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

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.

Nell'esempio (iv) dopo il Cor.4.3 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 6.2 concludiamo che $H$ non è un sottogruppo normale di $S_3$.

**Teorema (6.3).** *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:

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

Quindi la conclusione segue dal Teorema 6.2.

**Teorema (6.4).** *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 2.6, 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.

**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 6.3.
(ii) Sia $n$ un intero positivo *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 $R_\pi$ con centro $\mathbf{O}$ e angolo $\pi$. Per il Teorema 6.4, il gruppo $\{\mathrm{id}, R_\pi\}$ è un sottogruppo normale di $D_n$.

**Costruzione del gruppo quoziente.** Sia $G$ un gruppo e sia $N$ un sottogruppo normale. Siccome $N$ è normale, non c'è differenza fra le classi laterali sinistre e destre. Come nel paragrafo 4, indichiamo con $G/N = \{gN : g \in G\}$ l'insieme delle classi laterali di $N$. Scriviamo $\overline{g}$ per $gN$. Definiamo la composizione

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

Questa definizione dipende, a priori, dalla scelta dei rappresentanti $a$ e $b$ delle classi $\overline{a}$ e $\overline{b}$. Verifichiamo che in realtà non c'è dipendenza da queste scelte: supponiamo che $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Per il Teorema 4.4 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 $[G : N]$. L'applicazione $\pi : G \longrightarrow G/N$ data da $\pi(g) = \overline{g}$ è un omomorfismo ed è detta applicazione *canonica.*

**Esempi.**

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

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

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.2.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 $G = \mathbf{Z}$, sia $n \in \mathbf{Z}$ e sia $N = n\mathbf{Z}$. Siccome $\mathbf{Z}$ è un gruppo commutativo, $N$ è un sottogruppo normale. Le classi laterali di $N = n\mathbf{Z}$ sono

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

Si verifica che il gruppo quoziente $G/N = \mathbf{Z}/n\mathbf{Z}$ coincide con il gruppo delle classi resto modulo $n$ dello Esempio 1.7.

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

**Teorema (6.5).** *Sia $G$ un gruppo e sia $N$ un sottogruppo normale di $G$. Allora*
*(i) Il nucleo dell'applicazione canonica $G \longrightarrow G/N$ è uguale a $N$.*
*(ii) I sottogruppi di $G/N$ sono esattamente i gruppi $H/N$, cioè $\{hN : h \in H\}$, dove $H$ è un sottogruppo di $G$.*

**Dimostrazione.** *(i)* Sia $\pi : G \longrightarrow G/N$ l'applicazione canonica. Abbiamo $g \in \ker(\pi)$ se e soltanto se $gN = \pi(g) = N$, cioè se e soltanto se $g \in N$.
*(ii)* È banale verificare che ogni insieme $\{hN : h \in H\}$ dove $H$ è un sottogruppo di $G$ è un sottogruppo di $G/N$. Viceversa, sia $H'$ un sottogruppo di $G/N$. Definiamo

$$H = \{h \in G : hN \in H'\}.$$

Lasciamo al lettore la verifica che $H$ è un sottogruppo di $G$. Per definizione si ha $H' = \{hN : h \in H\}$, come richiesto.

**Teorema (6.6).** *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 $ghg^{-1}h^{-1}$ generanno $[G, G]$, 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 alla fine dello paragrafo 3. 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.F) 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.G) Sia $G$ un gruppo e sia $N \subset G$ un sottogruppo normale di ordine 2. Far vedere che $N \subset Z(G)$.
(6.H) Dimostrare che ogni sottogruppo del gruppo $Q$ dei quaternioni è normale in $Q$.
(6.I) Determinare i sottogruppi normali del gruppo diedrale $D_4$.
(6.J) Dare un esempio di un gruppo $G$ e di sottogruppi $H, N \subset G$ tali che

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

(6.K) 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.L) Sia $n$ un intero positivo. Dimostrare che $[S_n, S_n] = A_n$. (Sugg. Utilizzare il Teorema 3.5).
(6.M) Determinare la struttura di $D_4/N$ per ogni sottogruppo normale $N$ del gruppo diedrale $D_4$.
(6.N) Sia $G$ un gruppo. Provare che se $G/Z(G)$ è ciclico, allora $G$ è abeliano.
(6.O) 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.P) 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.Q) Sia $\mathrm{N} : \mathbf{H}^* \longrightarrow \mathbf{R}^*$ l'applicazione "norma" dell'Eserc.1.H. Dimostrare
(i) $[\mathbf{H}^*, \mathbf{H}^*] \subset \ker(N)$,
(ii) per ogni $x \in \mathbf{H}$ esiste $y \in \mathbf{H}^*$ tale che $yx = \overline{x}y$.
(iii) per $x \in \ker(N)$, $x \neq -1$ esiste $y \in \mathbf{H}^*$ tale che $x = [1 + \overline{x}, y]$,
(iv) $[\mathbf{H}^*, \mathbf{H}^*] = \ker(N) = \{x \in \mathbf{H}^* : x\overline{x} = 1\}$.
(6.R) Sia $n \geq 2$ un intero. Dimostrare che

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

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

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

e sia $Q \subset \mathbf{H}^*$ 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 $\alpha, \beta$, 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 $\mathbf{R}$ con $\mathbf{Z}/3\mathbf{Z}$.)

(6.T) Esiste un sottogruppo $H$ di $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ tale che

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

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

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

(6.V) Dimostare che $S_n$ e $A_n \times \mathbf{Z}/2\mathbf{Z}$ 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 quozienti.

**Teorema (7.1).** *(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 $h(gN) = f(g)$. Si dice anche che il diagramma*

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

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

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

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

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

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

Siccome

$$h(\overline{g}\,\overline{g'}) = h(\overline{gg'}) = f(gg') = f(g)f(g') = h(\overline{g})h(\overline{g'}),$$

l'applicazione $h$ è un omomorfismo. Per definizione $h$ soddisfa $h(\overline{g}) = f(g)$. Un omomorfismo $h' : G/N \longrightarrow G'$ con le stesse proprietà, è evidentemente uguale ad $h$. Questo finisce la dimostrazione del teorema.

**Teorema (7.2).** *(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

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

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

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

Dunque, l'applicazione

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

è una biiezione, come richiesto.

**Corollario (7.3).** *Sia $f : G \longrightarrow G'$ un omorfismo suriettivo di gruppi. Allora*

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

**Dimostrazione.** Immediata dal Teorema 7.2.

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

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

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

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

è un omomorfismo (Si veda l'Eserc.2.H(vii)). È ben noto che per ogni $a, b \in \mathbf{R}$ con $a^2 + b^2 = 1$ esiste $\phi \in \mathbf{R}$ 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 $\ker(F) = \{\phi \in \mathbf{R} : \cos(2\pi\phi) = 1 \text{ e } \mathrm{sen}(2\pi\phi) = 0\}$. Si vede dunque facilmente che $\ker(F) = \mathbf{Z}$. Adesso applichiamo il Corollario 7.3:

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

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

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.

**Teorema 7.4.** *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*

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ & \searrow \quad \nearrow_{h} & \\ & G/[G,G] & \end{array}$$

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

**Teorema 7.5.** *(Secondo teorema di isomorfismo.)*
*Sia $G$ un gruppo, sia $H \subset G$ un sottogruppo e sia $N \subset G$ un sottogruppo normale* di $G$. Allora
(i) $H \cap N$ è un sottogruppo normale di $H$.
(ii) L'insieme $HN = \{hn : h \in H,\, n \in N\}$ è un sottogruppo di $G$. Il gruppo $N$ è un sottogruppo normale di $HN$.
(iii) Abbiamo

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

**Dimostrazione.** *(i)* Sia $n \in H \cap N$ e sia $g \in H$. Ovviamente $gng^{-1} \in H$. Siccome $N$ è un sottogruppo normale di $G$ abbiamo anche $gng^{-1} \in N$. Quindi $gng^{-1} \in H \cap N$ e concludiamo che $H \cap N$ è un sottogruppo normale di $H$.
*(ii)* Siccome $e \in H, N$ abbiamo che $e = e \cdot e \in HN$ e dunque $HN \neq \emptyset$. Sia $a = h_1 n_1 \in HN$ e $b = h_2 n_2 \in HN$. Siccome $N$ è un sottogruppo normale abbiamo

$$h_2(n_1 n_2^{-1})h_2^{-1} = n_3 \in N.$$

Dunque, $ab^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 h_2^{-1} n_3 \in HN$. Per il Teorema 2.1, 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 7.3.

Diamo una applicazione del Teorema 7.5. 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 1:

$$H = \{\sigma \in S_4 : \sigma(1) = 1\}.$$

l'insieme $H$ è un sottogruppo di $G$. Applichiamo il Teorema 7.5. Troviamo

$$S_3/(S_3 \cap V_4) \cong S_3V_4/V_4.$$

Si vede che solo l'elemento neutro di $V_4$ ha punti fissi. Dunque $S_3 \cap V_4 = \{(1)\}$ e $S_3/(S_3 \cap V_4) \cong S_3$. Abbiamo

$$V_4 \subset S_3V_4 \subset S_4.$$

L'indice $[S_3V_4 : V_4] = \#S_3 = 6$. D'altra parte, per il Teorema di Lagrange (4.6) l'indice $[S_4 : V_4]$ è uguale a 24/4=6. Concludiamo che $S_3V_4 = S_4$. Sostituiamo tutto questo e troviamo

$$S_3 \cong S_4/V_4.$$

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

**Teorema 7.6.** *(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 il Teorema 6.5*(ii)* per una dimostrazione dal 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 da 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 7.3 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.

Come esempio di applicazione del Teorema 7.6, sia $H$ il sottogruppo $\{\overline{0}, \overline{3}\}$ di $\mathbf{Z}/6\mathbf{Z}$. (Si veda il Teorema 2.3). Si potrebbe calcolare la struttura di $(\mathbf{Z}/6\mathbf{Z})/H$ così: sia $G = \mathbf{Z}$, sia $N' = 3\mathbf{Z}$ e sia $N = 6\mathbf{Z}$. Il gruppo $N'/N$ è uguale a

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

Il Teorema 7.6 ci dà

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

**Esercizi.**

(7.A) Sia $G$ un gruppo e sia $g \in G$. Dimostrare che l'applicazione $F : \mathbf{Z} \longrightarrow G$ data da $n \mapsto g^n$ è un omomorfismo suriettivo da $\mathbf{Z}$ a $< g >$. Far vedere che $F$ è iniettiva se e soltanto se $g$ ha ordine infinito. Se $F$ non è iniettiva, utilizzare il Teorema 7.2 per dimostrare che $\mathbf{Z}/n\mathbf{Z} \cong < g >$ dove $n$ è l'ordine di $g$.

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

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

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

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

con $a \in \mathbf{R}^*$ e $b \in \mathbf{R}$. Sia $G$ il gruppo delle trasformazioni affine di $\mathbf{R}$. (Si veda l'Eserc.1.H) Dimostrare che $f : G \longrightarrow \mathbf{R}^*$ data da $f(A) = A(0)$ è un omomorfismo suriettivo. Sia $T = \{A \in G : A(x) = x + b, \text{ per un certo } b \in \mathbf{R}\}$ il sottogruppo delle traslazioni di $\mathbf{R}$. Far vedere che

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

(7.F) 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.G) Dimostrare:

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

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

(7.H) 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, si ha

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

(7.I)* Sia $G$ il gruppo delle trasformazioni isometriche di $\mathbf{R}^3$ che rispettano un tetraedro regolare con baricentro $\mathbf{0}$. Sia

$$G \longrightarrow S_4$$

l'applicazione che associa a una isometria la permutazione indotta sui vertici.

(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 diagonali. 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.J)* Sia $G$ il gruppo delle 48 trasformazioni isometriche di $\mathbf{R}^3$ che rispettano un cubo con baricentro $\mathbf{0}$ (Si veda l'Eserc.1.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 $\mathbf{R}^3$ (quelle che hanno il determinante uguale a $+1$). Dimostrare che l'applicazione $F$ ristretta ad $H$ è un isomorfismo far $H$ e $S_4$.

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

**8. Automorfismi.**

In questo paragrafo diamo qualche applicazione dei teoremi che abbiamo dimostrato. Studiamo certe condizioni affinchè un sottogruppo sia normale in un gruppo. Consideriamo inoltre il gruppo degli *automorfismi* di un gruppo.

**Teorema (8.1).** *Sia $G$ un gruppo e sia $H$ un sottogruppo di $G$ con $[G : H] = n$. Allora esiste un sottogruppo $N \subset H$ normale in $G$ tale che $[G : N]$ divide $n!$.*

**Dimostrazione.** Consideriamo l'insieme $X = G/H$ delle classi laterali sinistre di $H$. Facciamo agire $G$ su $X$ per moltiplicazione a sinistra:

$$g \cdot (aH) = (ga)H \qquad \text{per } g \in G \text{ e } x = aH \in G/H.$$

Per il Teorema 5.2, otteniamo così un'omomorfismo

$$F : G \longrightarrow S(X).$$

Sia $N = \ker(F)$. Per vedere che $N \subset H$ prendiamo $n \in N$. Siccome $nH = H$ abbiamo $n \in H$.

Per il primo Teorema di isomorfismo abbiamo che $G/N$ è isomorfo a un sottogruppo di $S(X) \cong S_n$. Dunque $[G : N] = \#G/N$ divide $\#S_n = n!$ come richiesto.

**Corollario (8.2).** *Sia $G$ un gruppo finito e sia $H \subset G$ un sottogruppo tale che*

$$\text{mcd}(\#H, ([G : H] - 1)!) = 1.$$

*Allora $H$ è un sottogruppo normale di $G$.*

**Dimostrazione.** Sia $n = [G : H]$. Per il Teorema 8.1, esiste un sottogruppo normale $N \subset H$ di $G$ tale che $[G : N]$ divide $n!$. Dunque

$$[H : N] = \frac{[G : N]}{[G : H]} \quad \text{divide} \quad \frac{n!}{n} = (n-1)!$$

D'altra parte

$$[H : N] \quad \text{divide} \quad \#H.$$

Siccome $\text{mcd}(\#H, ([G : H] - 1)!) = 1$ abbiamo $[H : N] = 1$, cioè $N = H$. Concludiamo che $H$ è un sottogruppo normale.

Adesso dimostriamo una generalizzazione del Teorema 6.3.

**Corollario (8.3).** *Sia $G$ un gruppo finito e sia $H$ un sottogruppo di $G$ con $[G : H] = p$ dove $p$ è il numero primo più piccolo che divide l'ordine di $G$. Allora $H$ è un sottogruppo normale di $G$.*

**Dimostrazione.** Il numero $([G : H] - 1)! = (p-1)!$ ha soltanto divisori primi più piccoli di $p$. Siccome $p$ è il numero primo più piccolo che divide $\#G$, abbiamo che $\text{mcd}(\#G, ([G : H] - 1)!) = 1$ e dunque anche $\text{mcd}(\#H, ([G : H] - 1)!) = 1$. Adesso il risultato segue dal corollario 8.2.

Come esempio consideriamo un gruppo $G$ di ordine 15. Per il Teorema di Cauchy, il gruppo $G$ contiene un elemento $x$ di ordine 5. Sia $H$ il sottogruppo generato da $x$. Per il corollario 8.3, il sottogruppo $H$ è normale in $G$.

**Definizione.** Sia $G$ un gruppo. Con $\text{Aut}(G)$ indichiamo l'insieme degli automorfismi $f : G \longrightarrow G$. Con la composizione

$$(f \circ g)(x) = f(g(x))$$

l'insieme $\text{Aut}(G)$ diventa un gruppo con elemento neutro l'applicazione identica. Per ogni $g \in G$, l'applicazione $\phi_g$ definita da

$$\phi_g(x) = gxg^{-1} \qquad \text{per ogni } x \in G$$

è un automorfismo di $G$. Un tale automorfismo si dice *interno.* L'insieme degli automorfismi interni si indica con $\text{Inn}(G)$.

**Proposizione (8.4).** *Sia $G$ un gruppo. Allora*
*(i)* $\mathrm{Inn}(G)$ *è un sottogruppo normale di* $\mathrm{Aut}(G)$.
*(ii)*

$$\mathrm{Inn}(G) \cong G/Z(G).$$

**Dimostrazione.** *(i)* L'insieme $\mathrm{Inn}(G)$ contiene $\phi_e = \mathrm{id}$ ed è dunque non vuoto. Siccome $\phi_g\phi_{h^{-1}} = \phi_{gh^{-1}}$ l'insieme $\mathrm{Inn}(G)$ è un sottogruppo di $\mathrm{Aut}(G)$.

Per dimostrare che $\mathrm{Inn}(G)$ è un sottogruppo normale, sia $\phi_g \in \mathrm{Inn}(G)$ e sia $\sigma \in \mathrm{Aut}(G)$. Per ogni $x \in G$ abbiamo

$$\sigma\phi_g\sigma^{-1}(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)x\sigma(g)^{-1} = \phi_{\sigma(g)}(x)$$

e dunque $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$. Questo finisce la dimostrazione della prima parte.
*(ii)* Consideriamo l'applicazione

$$F : G \longrightarrow \mathrm{Aut}(G)$$

data da $F(g) = \phi_g$. È facile verificare che $F$ è un omomorfismo. L'immagine è, per definizione, uguale a $\mathrm{Inn}(G)$. Il nucleo contiene gli elementi $g \in G$ tali che $\phi_g = \mathrm{id}$, cioè gli elementi $g$ tali che $gxg^{-1} = x$ per ogni $x \in G$. Dunque $\ker(F) = Z(G)$. La parte *(ii)* segue adesso dal primo teorema di isomorfismo 7.2.

Come esempio determiamo i gruppi di automorfismo di $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$ e di $S_3$:

**Teorema (8.5).**
*(i) Tutti gli automorfismi di $S_3$ sono interni. Ce ne sono sei.*
*(ii)*

$$\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \cong (\mathbf{Z}/n\mathbf{Z})^*.$$

*(iii)*

$$\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}^* \cong \mathbf{Z}/2\mathbf{Z}.$$

**Dimostrazione.** *(i)* Gli unici elementi di $S_3$ di ordine 2 sono $(1\,2)$, $(1\,3)$ e $(2\,3)$. Ogni automorfismo di $S_3$ deve dunque permutare questi tre elementi. D'altra parte, siccome le trasposizioni generanno $S_3$, ogni automorfismo è determinato dalle immagini di questi tre trasposizioni. Ci sono dunque al più $3! = 6$ automorfismi di $S_3$.

Per l'Eserc. 3.M il centro di $S_3$ è banale. Per il Teorema 8.4 ci sono dunque 6 automorfismi interni di $S_3$. Concludiamo che tutti gli automorfismi di $S_3$ sono interni.
*(ii)* Sia $\sigma$ un automorfismo di $\mathbf{Z}/n\mathbf{Z}$. Sia $a$ un intero positivo e sia $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$. Allora

$$\begin{aligned}\sigma(\overline{a}) &= \sigma(\underbrace{\overline{1} + \ldots + \overline{1}}_{a \text{ volte}}) \\ &= \sigma(\overline{1}) + \ldots + \sigma(\overline{1}) \\ &= a \cdot \sigma(\overline{1}).\end{aligned}$$

L'applicazione $\sigma$ è dunque completamente determinata da $\sigma(\overline{1})$. Siccome $\sigma$ è una biiezione, esiste $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ tale che

$$\sigma(\overline{a}) = a \cdot \sigma(\overline{1}) = \overline{1}.$$

Questo implica che $\sigma(\overline{1})$ è in $(\mathbf{Z}/n\mathbf{Z})^*$.

È facile vedere che l'applicazione

$$F : \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

data da $F(\sigma) = \sigma(\overline{1})$, è un'omomorfismo. Siccome l'applicazione

$$G : (\mathbf{Z}/n\mathbf{Z})^* \longrightarrow \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$$

data da $G(\overline{x}) = \sigma_{\overline{x}}$ dove $\sigma_{\overline{x}}(\overline{a}) = \overline{ax}$, è l'applicazione inversa di $F$, abbiamo che $F$ è un isomorfismo, come richiesto.
*(iii)* Similmente si dimostra che

$$\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}^*.$$

Siccome $\mathbf{Z}^* = \{\pm 1\}$, la dimostrazione è completa.

**Proposizione (8.6).** *Sia $N$ un sottogruppo normale di un gruppo $G$. Allora l'applicazione*

$$f : G \longrightarrow \mathrm{Aut}(N)$$

*data da $f(g)(n) = gng^{-1}$, è un omomorfismo.*

**Dimostrazione.** Lasciamo la dimostrazione al lettore.

Come esempio studiamo la struttura di un gruppo $G$ di ordine 15. Abbiamo già visto sopra che un tale gruppo ha sempre un sottogruppo normale $N$ di ordine 5. In questo caso la proposizione precedente ci dà un'omomorfismo

$$F : G \longrightarrow (\mathbf{Z}/5\mathbf{Z})^*.$$

Siccome $\overline{2} \in (\mathbf{Z}/5\mathbf{Z})^*$ ha ordine 4, il gruppo $(\mathbf{Z}/5\mathbf{Z})^*$ ha 4 elementi. Dunque

$$\#\mathrm{im}(F) \quad \text{divide} \quad 4.$$

Per il primo teorema di isomorfismo abbiamo che

$$\#\mathrm{im}(F) \quad \text{divide} \quad \#G = 15.$$

Siccome $\mathrm{mcd}(4, 15) = 1$, troviamo che $\mathrm{im}(F)$ è banale, cioè $F(\overline{a}) = \mathrm{id}$ per ogni $\overline{a} \in G$. In altre parole, abbiamo $\overline{a}\,\overline{x}\,\overline{a}^{-1} = \overline{x}$ per ogni $a \in G$ ed ogni $x \in N$. Dunque $N \subset Z(G)$.

Il gruppo $G/N$ ha ordine 3 ed è dunque ciclico. Per l'Eserc.6.N concludiamo che $G$ è abeliano. Siano ora $x, y \in G$ due elementi di ordine 5 e 3 rispettivamente. Si verifica facilmente che il prodotto $xy$ ha ordine 15 (Si veda l'Eserc.4.G). Dunque ogni gruppo di ordine 15 è ciclico

**Esercizi.**

(8.A) Sia $H$ un sottogruppo di un gruppo $G$ e sia

$$N_H = \{g \in G : gHg^{-1} = H\}$$

il *normalizzante* di $H$ in $G$. Dimostrare
(i) $N_H$ è un sottogruppo di $G$ che contiene $H$.
(ii) Il numero dei gruppi coniugati a $H$ (cioè i gruppi $gHg^{-1}$) è al più $[G : H]$.
(iii) Se $G$ è finito e $H \neq G$, allora

$$\cap_{g \in G} gHg^{-1} \neq G.$$

(8.B) Sia $G$ un gruppo di ordine 20. Dimostrare che $G$ contiene un sottogruppo normale di ordine 5.
(8.C) Sia $p$ un primo e $G$ un gruppo di ordine $p^2$. Far vedere che $G$ contiene un sottogruppo normale $N$ di ordine $p$. Dimostrare che $N \subset Z(G)$ e concludere che $G$ è abeliano.

(8.D) Sia $G$ un gruppo. Un sottogruppo $H$ di $G$ si dice *caratteristico* se $\sigma(H) = H$ per ogni $\sigma \in \mathrm{Aut}(G)$. Dimostrare:
  (i) un sottogruppo caratteristico di $G$ è normale in $G$.
  (ii) Se $H \subset N \subset G$ sono tali che $H$ è caratteristico in $N$ e $N$ è normale in $G$, allora $H$ è normale in $G$.

(8.E) Far vedere che ogni sottogruppo di un gruppo ciclico $G$ è caratteristico in $G$.

(8.F) Sia $G$ un gruppo, dimostrare che il sottogruppo di $G$ generato dagli elementi $g^2$, con $g \in G$ è caratteristico.

(8.G) Determinare i sottogruppi caratteristici di $V_4$ e di $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(8.H) Dimostrare che per ogni $a \in \mathbf{Q}^*$ l'applicazione $\mathbf{Q} \longrightarrow \mathbf{Q}$ data da

$$x \mapsto ax$$

è un automorfismo del gruppo additivo $\mathbf{Q}$. Far vedere che ogni automorfismo di $\mathbf{Q}$ ha questa forma. Concludere che

$$\mathrm{Aut}(\mathbf{Q}) \cong \mathbf{Q}^*.$$

(8.I) Sia $G$ un gruppo non abeliano. Far vedere che $\#\mathrm{Inn}(G) \geq 4$.

(8.J) Sia $G$ un gruppo con $Z(G) = \{e\}$. Far veder che $Z(\mathrm{Aut}(G)) = \{e\}$. (Sugg. Utilizzare l'uguaglianza $\sigma\phi_g\sigma^{-1} = \phi_{\sigma(g)}$ per $\sigma \in \mathrm{Aut}(G)$ e $g \in G$.)

(8.K) È ciclico $\mathrm{Aut}(\mathbf{Z}/9\mathbf{Z})$? E $\mathrm{Aut}(\mathbf{Z}/16\mathbf{Z})$?

(8.L) Sia $G$ un gruppo di ordine dispari. Sia $N$ un sottogruppo normale di ordine 17. Far vedere che $N \subset Z(G)$.

(8.M) Sia $G$ un gruppo. Un *anti-automorfismo di* $G$ è una biiezione $\varphi : G \longrightarrow G$ tale che

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

Sia $A$ l'insieme degli anti-automorfismi di $G$ e sia $B = A \cup \mathrm{Aut}(G)$. Dimostrare
  (i) L'applicazione $x \mapsto x^{-1}$ è un anti-automorfismo.
  (ii) $A = \mathrm{Aut}(G)$ se e soltanto se $G$ è abeliano.
  (iii) Se $G$ non è abeliano, allora $B$ è un gruppo isomorfo con

$$\mathrm{Aut}(G) \times (\mathbf{Z}/2\mathbf{Z}).$$

(8.N) Sia $G$ un gruppo con $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$. Far vedere che $\#G \leq 2$.

(8.O) Sia $G$ un gruppo e sia $N$ un sottogruppo normale di $G$. Dimostrare che l'applicazione

$$G/N \longrightarrow \mathrm{Aut}(N)/\mathrm{Inn}(N)$$

è ben definita ed è un'omomorfismo.

(8.P) Sia $G$ un gruppo. Far vedere
  (i) Se $G$ è ciclico, allora $\mathrm{Aut}(G)$ è abeliano.
  (ii) Se $\mathrm{Aut}(G)$ è ciclico, allora $G$ è abeliano.

(8.Q) Sia $G$ un gruppo. Siano $G' = [G, G]$ e $G'' = [G', G']$. Supponiamo che $G''$ sia ciclico.
  (i) Far vedere $G'' \subset Z(G')$.
  (ii) Supponiamo che $G'/G''$ sia ciclico. Dimostrare che $G'' = \{e\}$.

**11. Anelli.**

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

**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 valgono 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 $x, y, z \in R$

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

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 11.2), 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 $a \cdot b$.

**Esempio (11.1).** Con l'addizione e la moltiplicazione introdotte nel primo paragrafo gli insiemi $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ e $\mathbf{H}$ sono anelli. Lasciamo al lettore la facile verifica. Gli anelli $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ e $\mathbf{C}$ sono commutativi. Gli anelli $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ e $\mathbf{H}$ sono anelli con divisone (si vedano gli Esempi (1.3) e (1.4)). Siccome la moltiplicazione in $\mathbf{H}$ non è commutativa, solo gli anelli $\mathbf{Q}$, $\mathbf{R}$ e $\mathbf{C}$ sono campi.

**Esempio (11.2).** (*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.11.C. Dunque, se $0 = 1$, l'anello $R$ è uguale a $\{0\}$. Questo anello si chiama *l'anello banale.*

**Esempio (11.3).** Con l'addizione dell'Esempio 1.7 e la moltiplicazione data da

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

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

**Esempio (11.4).** (*L'anello degli interi di Gauss*) Sia $\mathbf{Z}[i]$ il sottoinsieme di $\mathbf{C}$ dato da

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

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

**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.11.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 $R^*$.

È da notare che le notazioni $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ e $\mathbf{H}^*$ coincidono con quelle del paragrafo 1. Anche la notazione $(\mathbf{Z}/n\mathbf{Z})^*$ coincide: nell'Esempio 1.8 abbiamo già dimostrato che il sottoinsieme $\{\overline{a} : \mathrm{mcd}(a, n) = 1\}$ di $\mathbf{Z}/n\mathbf{Z}$ è un gruppo moltiplicativo. Ogni elemento di questo gruppo ha dunque un inverso moltiplicativo. Viceversa, se $\overline{a} \in \mathbf{Z}/n\mathbf{Z}$ ha un inverso moltiplicativo $\overline{b}$, allora $\overline{a}\,\overline{b} = \overline{1}$, cioè

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

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

**Proposizione (11.5).** *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.

Per esempio, il gruppo $\mathbf{Z}^*$ è uguale a $\{+1, -1\}$. Si veda l'Eserc.11.L per una dimostrazione che $\mathbf{Z}[i]^* = \{\pm 1, \pm i\}$.

**Proposizione (11.6).** *Sia $n$ un intero positivo. L'anello $\mathbf{Z}/n\mathbf{Z}$ è un campo se e soltanto se $n$ è un numero primo.*

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

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

Equivalentemente, ogni $a \in \mathbf{Z}$ 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.

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

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

**Proposizione (11.7).** *Un divisore di zero di un anello $R$ non può essere un unità.*

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

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

Abbiamo

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

contraddicendo la definizione di $b$. Se $a$ è un divisore di zero destro la dimostrazione è simile.

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 11.8) di un anello con divisione non contiene divisori di zero. L'anello $\mathbf{Z}$ e l'anello degli interi di Gauss $\mathbf{Z}[i]$ ne sono esempi.

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

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

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

**Esempio (11.8).** (*Sottoanelli; prodotti*) 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 esempio, $\mathbf{Z}$ è un sottoanello di $\mathbf{Q}$. Il campo $\mathbf{Q}$ è un sottoanello di $\mathbf{R}$. Abbiamo le seguenti inclusioni di anelli:

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

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

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

**Esempio (11.9).** (*Anelli di 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

$$\sum_{i=0}^{\infty} a_iX^i$$

dove gli elementi $a_i$ appartengono ad $R$ e sono quasi tutti zero, cioè, esiste $n \in \mathbf{Z}_{\geq 0}$ tale che $a_i = 0$ per ogni $i > n$. Si veda l'Eserc.12.W per una definizione più formale dei polinomi. Per definizione, due polinomi $\sum_{i=0}^{\infty} a_iX^i$ e $\sum_{i=0}^{\infty} b_iX^i$ 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 $f = \sum_{i=0}^{\infty} a_iX^i$ 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 $f = \sum_{i=0}^{\infty} a_iX^i$ di grado $n$ si dice *monico* se $a_n = 1$.

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

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

con l'addizione data da

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

e la moltiplicazione implicata dalle regole della distributività e da

$$(a_iX^i)\cdot(b_jX^j) = a_ib_jX^{i+j},$$

cioè

$$\left(\sum_{i=0}^{\infty} a_iX^i\right)\cdot\left(\sum_{i=0}^{\infty} b_iX^i\right) = \left(\sum_{k=0}^{\infty}(\sum_{\substack{i,j\\ i+j=k}} a_ib_j)X^k\right).$$

Questa è la moltiplicazione di polinomi usuale; per esempio:

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

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.11.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

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

**Esempio (11.10).** (*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 $\Omega$ 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 utilliziamo 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 $\Omega$. 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

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

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 $R = \mathbf{Z}$ si trova un campo isomorfo al campo $\mathbf{Q}$ 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

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

**Esempio (11.11).** (*Endomorfismi).* Sia $A$ un gruppo *additivo* e sia $\mathrm{End}(A)$ l'insieme degli endomorfismi di $A$ (si veda il paragrafo 2). Per $f, g \in \mathrm{End}(A)$ definiamo la somma $f + g$ ed il prodotto $fg$:

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

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 $\mathrm{Id}_A$.

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

**Esempio (11.12).** (*Funzioni).* Sia $X$ un insieme e sia $R$ un anello. L'insieme $R^X$ delle funzioni $X \longrightarrow R$ è un anello can le seguenti addizione e moltiplicazione: per $f, g : X \longrightarrow R$ definiamo

$$\begin{aligned}(f + g)(x) &= f(x) + g(x), \\ (f \cdot g)(x) &= f(x) \cdot g(x),\end{aligned}$$

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 $[0, 1] = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$ e sia

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

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

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

e l'anello delle funzioni $C^\infty$:

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

**Esercizi.**

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

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

(11.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

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

(11.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.

(11.E) Sia $R$ un anello. Definiamo una nuova moltplicazione "$\star$" 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.*

(11.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 $R$.

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

$$A + B = A \Delta B, \qquad \text{(si veda l'Eserc.1.K)}$$
$$A \cdot B = A \cap B.$$

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

(11.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.

(11.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 en non è un divisore di zero.
- (iv) Dare un esempio di un anello infinito con divisori di zero.

(11.J) Dimostrare che nessun anello $R$ ha un gruppo addittivo isomorfo a $\mathbf{Q}/\mathbf{Z}$.

(11.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.

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

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

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

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

(11.N) Sia $m \in \mathbf{Z}$. Supponiamo che $m \equiv 3 \pmod 4$ e che $m$ non sia un quadrato.

(i) Dimostrare: l'insieme

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

è un sottoanello di $\mathbf{C}$.

(ii) Sia $m = 7$. Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbf{Z}[\sqrt{7}]$. (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 $\pm 1$)

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

(11.O) Sia $m \in \mathbf{Z}$. Supponiamo che $m \equiv 1 \pmod 4$ e che $m$ non sia un quadrato. Sia

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

(i) Dimostrare: l'insieme

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

è un sottoanello di $\mathbf{C}$.

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

(iii) Sia $\alpha = \frac{1+\sqrt{13}}{2}$. Trovare un'unità $\varepsilon \neq \pm 1$ nell'anello $\mathbf{Z}[\alpha]$. (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 $\pm 1$)

(iv) Sia

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

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

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

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

(ii) 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

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

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

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

(11.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.

(11.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 $f$.)

(11.T) Sia $A$ un gruppo abeliano. Far vedere che $\mathrm{End}(A)^* = \mathrm{Aut}(A)$.

(11.U) (i) Far vedere che l'anello $C([0,1]) = \{f : [0,1] \longrightarrow \mathbf{R} : \ f \text{ è continua}\}$ ha divisori di zero.

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

(11.V) Sia $A$ il gruppo additivo di $\mathbf{R}[X]$. 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.

(11.W) (*Polinomi di Laurent*) Sia $R$ un anello. Un *polinomio di Laurent* è un'espressione

$$\sum_{i \in \mathbf{Z}} a_i X^i \qquad \text{con } a_i \in R \text{ per ogni } i \in \mathbf{Z}.$$

con $a_i = 0$ per quasi tutti gli indici $i$.

(i) Con l'addizione e moltiplicazione ovvia gli insieme dei polinomi di Laurent di 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

$$R[X, \frac{1}{X}] = \{uX^i : \ u \in R^* \text{ e } i \in \mathbf{Z}\}.$$

(11.X)*(*Funzioni aritmetiche.*) Una *funzione aritmetica* è una funzione $f : \mathbf{Z}_{>0} \longrightarrow \mathbf{C}$. La somma di due funzioni aritmetiche $f$ e $g$ è definita da

$$(f + g)(n) = f(n) + g(n) \qquad \text{per ogni } n \in \mathbf{Z}_{>0}$$

ed il cosidetto *prodotto di convoluzione* $f \star g$ è di $f$ e $g$ è definito da

$$(f \star g)(n) = \sum_{\substack{d \text{ divide } n \\ d>0}} f(d)g(\frac{n}{d}) \qquad \text{per ogni } n \in \mathbf{Z}_{>0}.$$

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

(iii) 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 $n \in \mathbf{Z}_{>0}$. Calcolare $E \star E$.

(v) Sia "id" la funzione $\mathrm{id}(n) = n$ per ogni $n \in \mathbf{Z}_{>0}$ e sia $\varphi$ la funzione di Eulero dell'Esempio 1.8. Dimostrare che

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

**12. Omomorfismi ed ideali.**

In questo paragafo 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.

**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

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

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* $f$.

**Esempio (12.1).** (i) Sia $n$ un intero positivo. L'applicazione canonica

$$\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$$

è un omomorfismo dall'anello $\mathbf{Z}$ all'anello $\mathbf{Z}/n\mathbf{Z}$.
(ii) Sia $\alpha \in \mathbf{R}$. L'applicazione

$$\mathbf{R}[X] \longrightarrow \mathbf{R}$$

data da $f \mapsto f(\alpha)$ è un omomorfismo di anelli. Lasciamo la verifica al lettore. È facile vedere che è un omomorfismo suriettivo. In generale, per ogni anello *commutativo* $R$ ed ogni $\alpha \in R$, l'applicazione $R[X] \longrightarrow R$ data da $f \mapsto f(\alpha)$ è un omomorfismo. Questo non è più vero per anelli non commutativi. Si veda l'Eserc.12.J.
(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 $\mathbf{Z} \longrightarrow R$ data da $m \mapsto m$, cioè

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

è un omomorfismo.

**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 $R$.

**Esempi (12.2).** (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 2.6, 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 2.6.
(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 di $R$ solo si dicono *ideali principali.*
(iv) Sia $I$ un ideale di $\mathbf{Z}$. Questo significa, in particolare, che $I$ è un sottogruppo additivo di $\mathbf{Z}$. Per il Teorema 2.3, ogni sottogruppo di $\mathbf{Z}$ ha la forma $n\mathbf{Z}$. Ogni sottogruppo di $\mathbf{Z}$ è quindi anche un ideale di $\mathbf{Z}$. Ogni ideale di $\mathbf{Z}$ è dunque principale.

Sia $R$ un anello e sia $f : \mathbf{Z} \longrightarrow R$ l'omomorfismo dell'Esempio 12.1(v). Il nucleo di $f$ si dice la *caratteristica di* $R$. Spesso si dice che la caratteristica $\mathrm{car}(R)$ di $R$ è l'intero non negativo $n$ che genera $\ker(f)$. Per esempio, la caratteristica di $\mathbf{Z}$ è 0 e $\mathrm{car}(\mathbf{Z}/n\mathbf{Z})$ è uguale a $n$.
(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 $a_1, a_2, \ldots, a_n$.

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

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

per certi polinomi $h, g \in \mathbf{Z}[X]$. Siccome $\mathbf{Z}$ 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 $\alpha \in \mathbf{Z}$, 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.

**Proposizione (12.3).** *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.

**Corollario (12.4).** *Sia $R$ un anello con divisione.*
*(i) I soli ideali di $R$ sono quelli banali.*
*(ii) 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.12.3 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.

*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. La nostra notazione coincide con quella dell'Esempio 12.5(v). 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

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

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.12.T. L'ideale $IJ$ è contenuto in sia $I$ che $J$ e quindi $IJ \subset I \cap J$. Abbiamo il seguente diagramma di ideali di $R$:

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

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

L'intersezione $n\mathbf{Z} \cap m\mathbf{Z}$ consiste degli interi $a$ che sono divisibile sia per $n$ che per $m$. Dunque il *minimo comune multiplo* $\mathrm{mcm}(n, m)$ di $n$ ed $m$ è contenuto nella intersezione $n\mathbf{Z} \cap m\mathbf{Z}$. D'altra parte, per l'Eserc.0.G, ogni multiplo comune di $n$ ed $m$ è divisibile per $\mathrm{mcm}(n, m)$. Concludiamo che

$$n\mathbf{Z} \cap m\mathbf{Z} = \mathrm{mcm}(n, m)\mathbf{Z}.$$

La somma $n\mathbf{Z} + m\mathbf{Z}$ è, per definizione, uguale all'insieme $\{an + bm : a, b \in \mathbf{Z}\}$. Per il Teorema 0.3 esso contiene $\mathrm{mcd}(n, m)$. È banale che ogni numero della forma $an + bm$ è divisibile per $\mathrm{mcd}(n, m)$. Concludiamo che

$$n\mathbf{Z} + m\mathbf{Z} = \mathrm{mcd}(n, m)\mathbf{Z}.$$

In particolare, $\mathrm{mcd}(n, m) = 1$ se e soltanto se $n\mathbf{Z} + m\mathbf{Z} = \mathbf{Z}$. 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.12.S il prodotto di $n\mathbf{Z}$ e $m\mathbf{Z}$ è dato da

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

**Definizione.** (*Anelli quozienti*). 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 $\overline{a}$ per la classe laterale $a + I$ dell'elemento $a \in R$. Per due elementi $\overline{a}, \overline{b} \in R/I$ definiamo

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

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

$$a' = a + x \qquad \text{per un certo } x \in I$$
$$b' = b + y \qquad \text{per un certo } y \in I$$

e, per la distributività di $R$,

$$a'b' = ab + xb + ay + xy.$$

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

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

e che 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

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

per ogni $\overline{a}, \overline{b}, \overline{c} \in R/I$.

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

**Proposizione (12.5).** *Sia $I$ un ideale di un anello $R$. L'omomorfismo canonico*

$$\pi : R \longrightarrow R/I,$$

*dato da $x \mapsto \overline{x}$, è un omomorfismo suriettivo. Il nucleo di $\pi$ è $I$.*

**Dimostrazione.** Siccome $\pi(x) = \overline{x}$, la mappa $\pi$ 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.

**Teorema (12.6).** *(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.*

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

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

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

**Teorema (12.7).** *(Primo Teorema di Isomorfismo.) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli. Allora*

$$R/\ker(f) \cong f(R).$$

**Dimostrazione.** Consideriamo l'omomomorfismo

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

Applicando il Teorema 12.6 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 un isomorfismo. Sia $y = f(x)$ un elemento arbitrario di $f(R)$. Allora $h(\overline{x}) = f(x) = y$ e vediamo che $h$ è una suriezione, come richiesto.

Gli Teoremi 12.6 e 12.7 sono molto simili ai corrispondenti Teoremi 7.1 e 7.3 per i gruppi. Per il corrispondente secondo Teorema di isomorfismo si veda l'Eserc.12.N. Il prossimo Teorema è l'analogo del Teorema 7.6.

**Teorema 12.8.** *(Terzo Teorema di isomorfismo.) Sia $R$ un anello e sia $I$ un ideale di $R$.*
*(i) Ogni ideale dell'anello $R/I$ 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 7.6 e la lasciamo al lettore.

**Esempi (12.9).** (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 $\Phi$ è un omomorfismo suriettivo. Il nucleo di $\Phi$ 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 12.7 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 $\Psi$ è un omomorfismo suriettivo.

Sia $f(X) = a_0 + a_1X + \ldots + a_nX^n$ nel nucleo di $\Psi$. 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 $J \subset \mathbf{Z}[X]$ l'ideale generato da 2 e $X$. Calcoliamo l'anello quoziente $\mathbf{Z}[X]/(2, X)$ utilizzando il Terzo teorema di isomorfismo. Per un metodo che utilizza invece il primo teorema di isomorfismo si veda l'Eserc.12.P.

Sia $I$ l'ideale generato da 2 in $\mathbf{Z}[X]$. Per il Teorema 12.7 abbiamo

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

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

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

Per il primo esempio, l'anello $(\mathbf{Z}/2\mathbf{Z})[X]/(X)$ è isomorfo a $\mathbf{Z}/2\mathbf{Z}$. Questo conclude l'esempio. Si veda il paragrafo 13 per altri metodi per fare calcoli in anelli di polinomi.

Adesso dimostriamo una generalizzazione del Corollario 2.9.

**Teorema (12.10).** *(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 $\Psi(x) = (x \pmod I, x \pmod J)$. È facile vedere che $\Psi$ è un omomorfismo. Ovviamente il nucleo di $\Psi$ è l'ideale $I \cap J$. Per la parte *(i)* abbiamo anche $\ker(\Psi) = IJ$.

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

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

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

**Corollario (12.11).** *Siano $n, m$ due interi coprimi, cioè tali che* $\mathrm{mcd}(n,m) = 1$.

(i) C'è un isomorfismo di anelli

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

(ii) C'è un isomorfismo di gruppi

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

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

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

dove $\varphi$ è la funzione di Eulero (si veda l'Esempio 1.8).

**Dimostrazione.** *(i)* Questo segue dal Teorema 12.10 e dal fatto che gli ideali $I = n\mathbf{Z}$ e $J = n\mathbf{Z}$ sono coprimi se e soltanto se $\mathrm{mcd}(n,m) = 1$.
*(ii)* Per l'Eserc.11.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 $\varphi(n) = \#(\mathbf{Z}/n\mathbf{Z})^*$.

**Corollario (12.12).** *Sia $n$ un intero positivo. Allora*

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

*dove $p$ varia sui numeri primi che dividono $n$.*

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

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

Siccome $\mathrm{mcd}(x, p^a) > 1$ se e soltanto se $p$ divide $x$, basta determinare i numeri $x$ divisibili per $p$ con $1 \le x \le p^a$. Questi sono esattamente i numeri $yp$ con $1 \le y \le p^{a-1}$. 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 12.11*(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.**

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

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

(12.C) (i) Sia $f : \mathbf{Q} \longrightarrow \mathbf{Q}$ un omomorfismo di anelli. Far vedere che $f$ è l'applicazione identica.
(ii) Sia $f : \mathbf{R} \longrightarrow \mathbf{R}$ un omomorfismo. Far vedere che $f(x) > 0$ se $x > 0$.
(iii) Sia $f : \mathbf{R} \longrightarrow \mathbf{R}$ un omomorfismo. Far vedere che $f$ è l'applicazione identica.

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

(12.E) Sia $R$ un anello senza divisori di zero. Dimostrare che $R$ ha caratteristica $p$ dove $p$ è un numero primo oppure 0.

(12.F) Dimostrare che l'anello di Boole dell'Eserc.11.G ha caratteristica 2.

(12.G) 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?

(12.H) 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.

(12.I) 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 $J \subset I$.

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

(i) Far vedere che $F_\alpha$ è un omomorfismo di anelli se $\alpha$ è contenuto nel centro di $R$. (Si veda l'Eserc.11.F).

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

(12.K) Sia $R$ un anello. Far vedere che

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

è un ideale di $R[X]$.

(12.L) 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 $\mathrm{End}(A)$.

(12.M) 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.

(12.N) 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

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

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

(12.P) (i) Far vedere che la mappa $\Psi : \mathbf{Z}[X] \longrightarrow \mathbf{Z}/2\mathbf{Z}$ data da $f \mapsto f(0) \pmod 2$ è un omomorfismo suriettivo.

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

(iii) Dimostrare che

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

(12.Q) 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 $1 + x \in R^*$.

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

(12.S) 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 $\varepsilon \in R^*$.

(12.T) Sia $R = \mathbf{Z}[X]/(5X, X^2)$.

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

$$f = a + bX \pmod{(5X, X^2)}.$$

(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 $\alpha = \varepsilon\beta$.

(12.U) (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 $R = \mathbf{Z}[X]$ 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 $R$.

(12.V) Sia $R$ un anello. Definiamo

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

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

(12.W) (*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

$$(a + b\varepsilon) + (c + d\varepsilon) = (a + c) + (b + d)\varepsilon,$$
$$(a + b\varepsilon) \cdot (c + d\varepsilon) = (ac) + (ad + bc)\varepsilon.$$

(i) Far vedere che $\varepsilon^2 = 0$. Questa formula e le legge 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

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

(12.X) (*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 $\Omega$ l'insieme delle successioni di elementi in $R$ dato da

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

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

$$x + y = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$
$$x \cdot y = (a_0 b_0, a_1 b_0 + a_0 b_1, a_2 b_0 + a_1 b_1 + a_0 b_2, \ldots).$$

(i) Dimostrare che con quest'addizione e moltiplicazione $\Omega$ è un anello.
(ii) Far vedere che la mappa $F : \Omega \longrightarrow R[X]$ data da

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

è un isomorfismo di anelli.

(12.Y)*(*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 $\mathbf{Z}/6\mathbf{Z}$.
(ii) Dimostrare: se $e$ è un idempotente anche $1 - e$ lo è.
(iii) Dimostrare: se $R$ è il prodotto di due anelli $R_1$ 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 $x \mapsto (x \pmod{eR}, x \pmod{(1-e)R})$ è un isomorfismo di anelli.

(12.Z) Sia $\varphi$ 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 $n \in \mathbf{Z}_{>0}$ con $\varphi(n) = 14$.

(iv) Dimostrare: per ogni $a \in \mathbf{Z}$ esistono soltanto un numero finito di interi $n \in \mathbf{Z}_{>0}$ 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

$$\operatorname*{limsup}_{n\to\infty} \frac{\varphi(n)}{n} = 1 \qquad \text{e} \qquad \operatorname*{liminf}_{n\to\infty} \frac{\varphi(n)}{n} = 0.$$

(Sugg: la somma $\sum_{p \text{ primo}} \frac{1}{p}$ diverge. Si veda l'Eserc.0.?)

(vi)*Dimostrare che l'insieme

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

è denso nell'intervallo $[0, 1]$.

## 13. Zeri di polinomi.

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 $\mathbf{Z}/p\mathbf{Z}$.

**Teorema (13.1).** *(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*

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

**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

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

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 $r = r'$.

**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 preciza diamo un esempio esplicito con polinomi in $\mathbf{Z}/12\mathbf{Z}[X]$. In questo esempio, tutti gli coefficienti vanno considerato nel anello $\mathbf{Z}/12\mathbf{Z}$. Siano

$$f = 6X^3 + 7X^2 + 2X + 3,$$
$$g = 5X^2 + 2X + 3.$$

Osserviamo che il primo coefficiente di $g$ è l'unità $5 \in (\mathbf{Z}/12\mathbf{Z})^*$. L'inverso moltiplicativo di 5 è uguale a 5.

$$\begin{array}{rcrcrcr} 6X^3 & + & 7X^2 & + & 2X & + & 3 \\ 6X^3 & + & 0 & + & 6X & & \\ 0 & & 7X^2 & + & 8X & + & 3 \\ & - & 5X^2 & - & 2X & - & 3 \\ & & 0 & - & 2X & + & 6 \end{array} \qquad \begin{array}{rcrcr} 5X^2 & + & 2X & + & 3 \\ 6X & - & 1 & & \end{array}$$

Prima sottraiamo $6 \cdot 5^{-1} X \cdot (5X^2 + 2X + 3) = 6X^3 + 6X$ di $f$. In questo modo si cancella il termine di grado 3 e si trova la differenza $7X^2 + 8X + 3$. Poi sottraiamo $7 \cdot 5^{-1} \cdot (5X^2 + 2X + 3) = -5X^2 - 2X - 3$. Adesso si cancella il termine di grado 2 e si trova come differenza $-2X + 6$. Concludiamo che abbiamo $f = qg + r$ con

$$q = 6X - 1,$$
$$r = -2X + 6.$$

Dimostriamo qualche corollario del Teorema 13.1.

**Teorema (13.2).** *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 13.1 possiamo dividere $f$ per $g$ con quoziente $q$ e resto $r$:

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

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.

**Proposizione (13.3).** *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*

$$\Psi : R[X] \longrightarrow R$$

*data da $f \mapsto f(\alpha)$ è un omomorfismo suriettivo con nucleo $(X - \alpha)$.*

*(iii) C'è un isomorfismo di anelli*

$$R[X]/(X - \alpha) \cong R.$$

**Dimostrazione.** *(i)* Per il Teorema 13.1 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.12.J abbiamo $f(\alpha) = q(\alpha)(\alpha - \alpha) + r$ e quindi $r = f(\alpha)$ come richiesto.
*(ii)* Per l'Eserc.12.J, la mappa $\Psi$ 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 $\Psi$ è $(X - \alpha)$. È ovvio che $\Psi$ è suriettiva.
*(iii)* Questa parte segue dal primo Teorema di Isomorfismo applicato all'omomorfismo $\Psi$ e dalla parte *(ii)*.

**Proposizione (13.4).** *C'è un isomorfismo di anelli*

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

**Dimostrazione.** Consideriamo la mappa

$$\Phi : \mathbf{R}[X] \longrightarrow \mathbf{C}$$

data da $\Phi(f) = f(i)$. È facile vedere che $\Phi$ è un omomorfismo suriettivo. Calcoliamo il nucleo di $\Phi$: 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 13.1, si ha

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

Sostituendo $X = i$, si trova $r(i) = 0$. Se $r$ avesse il grado 1, allora $r = c_1X + c_0$ con $c_1, c_0 \in \mathbf{R}$ e $c_1 \neq 0$. Ma questo implicherebbe che $i = -c_0/c_1 \in \mathbf{R}$, 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 $\Phi$ conclude adesso la dimostrazione.

La Proposizione 13.4 ci dà un modo di costruire il campo dei numeri complessi $\mathbf{C}$ senza introdurre un simbolo $i$. La definizione dei numeri complessi di un algebrista puro è semplicemente

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

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

**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 un *zero* di $f$ se $f(\alpha) = 0$, cioè se

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

**Teorema (13.5).** *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.13.3 abbiamo

$$f = f_1 \cdot (X - \alpha_{n+1}).$$

Per ogni $1 \leq i \leq n$ abbiamo inoltre $0 = f(\alpha_i) = f_1(\alpha_i)(\alpha_i - \alpha_{n+1})$ e 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 $f = f_1 \cdot (X - \alpha_{n+1})$.

**Corollario (13.6).** *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 13.5 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.

Può succedere che un polinomio $f$ con coefficienti in un dominio $R$ di grado $n$ abbia esattamente $n$ zeri distinti. Per esempio il polinomio $X^3 - 9X \in \mathbf{Z}[X]$ ha gli zeri $0, 3$ e $-3$. Però, in generale non è così. Per esempio $2X - 3 \in \mathbf{Z}[X]$ ha grado 1 ma non ha zeri in $\mathbf{Z}$. Un altro esempio è il polinomio $X^2 - 2 \in \mathbf{Q}[X]$, il quale non ha zeri in $\mathbf{Q}$ perché $\sqrt{2} \notin \mathbf{Q}$. Il polinomio $(X-1)^2 \in \mathbf{Z}[X]$ ha grado 2, ma soltanto uno zero in $\mathbf{Z}$. In questo caso si dice che lo zero ha molteplicità 2.

La Proposizione 13.5 e il suo Corollario 13.6 sono, in generale, falsi se $R$ non è un dominio di integrità. Per esempio, il polinomio $X^2 - 1 \in (\mathbf{Z}/12\mathbf{Z})[X]$ ha i quattro zeri $\overline{1}, \overline{5}, \overline{7}$ e $\overline{11}$. Anche la commutatività di $R$ è essenziale: il polinomio $X^2 + 1 \in \mathbf{H}[X]$ ha un numero *infinito* di zeri in $\mathbf{H}$ (Si veda l'Eserc 13.C). Nella dimostrazione della Prop.13.5, la commutatività di $R$ è stato assunta quando abbiamo utilizzato il fatto che la valutazione dei polinomi su un elemento di $R$ è un omomorfismo da $R[X]$ a $R$.

**Teorema (13.7).** *Sia $p$ un primo. Allora nell'anello $\mathbf{Z}/p\mathbf{Z}[X]$ vale*

$$\prod_{\overline{a} \in \mathbf{Z}/p\mathbf{Z}} (X - \overline{a}) = X^p - X.$$

**Dimostrazione.** Per il Teorema di Fermat (Cor.4.8*(i)*), abbiamo

$$\overline{a}^{p-1} = \overline{1} \qquad \text{per ogni } \overline{a} \in (\mathbf{Z}/p\mathbf{Z})^*.$$

In altre parole, ogni $\overline{a} \in \mathbf{Z}/p\mathbf{Z} - \{0\}$ è uno zero del polinomio $X^{p-1} - \overline{1} \in \mathbf{Z}/p\mathbf{Z}[X]$. Siccome $\mathbf{Z}/p\mathbf{Z}$ è un dominio, possiamo applicare la Prop.13.5. Troviamo

$$X^{p-1} - \overline{1} = q \cdot (X - \overline{1})(X - \overline{2}) \cdot \ldots \cdot (X - \overline{p-1})$$

con $q \in \mathbf{Z}/p\mathbf{Z}[X]$. 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 con $X$, otteniamo la tesi.

**Corollario (13.8).** *(Teorema di Wilson). Un intero $p$ è un primo se e soltanto se*

$$(p-1)! \equiv -1 \pmod{p}.$$

**Dimostrazione.** Sia $p$ un primo. Se $p = 2$ l'affermazione si verifica facilmente. Per $p \neq 2$ utilizziamo il Teorema 13.7:

$$\prod_{i=1}^{p-1}(X - \overline{i}) = X^{p-1} - \overline{1}.$$

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.13.E.

**Teorema (13.9).** *Sia $R$ un dominio di integrità e sia $G$ un sottogruppo finito di $R^*$. Allora $G$ è ciclico.*

**Dimostrazione.** L'anello $R$, essendo un dominio, è commutativo. Quindi, il gruppo $G$ è abeliano. Sia $x \in G$ un elemento con ordine $m$ *massimale.* Per l'Eserc 4.G, ogni elemento $y \in G$ soddisfa $y^m = 1$. In altre parole, ogni $y \in G$ è uno zero del polinomio $X^m - 1 \in R[X]$. Per il Cor.13.6 abbiamo dunque

$$m = \deg(X^m - 1) \geq \#G.$$

D'altra parte $G$ contiene il sottogruppo generato da $x$ di ordine $m$. Concludiamo che $G$ coincide con il sottogruppo ciclico generato da $x$.

**Corollario (13.10).** *Sia $p$ un numero primo. Allora il gruppo $(\mathbf{Z}/p\mathbf{Z})^*$ è ciclico.*

**Dimostrazione.** Basta applicare il Teorema 13.9 al dominio $R = \mathbf{Z}/p\mathbf{Z}$ ed al gruppo $G = (\mathbf{Z}/p\mathbf{Z})^*$.

Sia $p$ un primo. Un intero $g \in \mathbf{Z}$ tale che $\overline{g} \in \mathbf{Z}/p\mathbf{Z}$ è un generatore del gruppo moltiplicativo $(\mathbf{Z}/p\mathbf{Z})^*$ si dice una *radice primitiva modulo $p$*. Equivalentemente, $g \in \mathbf{Z}$ è una radice primitiva modulo $p$ se e soltanto se $\overline{g}$ ha ordine $p-1$ nel gruppo $(\mathbf{Z}/p\mathbf{Z})^*$.

Non è facile trovare radici primitive $g$. Il metodo più efficiente nella pratica sembra essere quello di provare con $g \in \mathbf{Z}$ a caso. Il numero delle radici primitive $\overline{g} \in (\mathbf{Z}/\mathbf{Z})^*$ è uguale a $\varphi(p-1)$ (Si veda l'Eserc.13.G). Non si sa, in generale, se un numero dato $g \in \mathbf{Z}$, come per esempio $g = 2$ o $g = 10$, sia una radice primitiva per un numero *infinito* di primi. La famosa *congettura di Artin,* secondo la quale ciò è vero, non si sa dimostrare.

Ecco una breve lista di radici primitive per i primi $p \leq 227$. Diamo sempre la più piccola radice primitiva $g > 0$.

| $p$ | $g$ | $p$ | $g$ | $p$ | $g$ | $p$ | $g$ | $p$ | $g$ | $p$ | $g$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 23 | 5 | 59 | 2 | 97 | 5 | 137 | 3 | 179 | 2 |
| 3 | 2 | 29 | 2 | 61 | 2 | 101 | 2 | 139 | 2 | 181 | 2 |
| 5 | 2 | 31 | 3 | 67 | 2 | 103 | 5 | 149 | 2 | 191 | 19 |
| 7 | 3 | 37 | 2 | 71 | 7 | 107 | 2 | 151 | 6 | 193 | 5 |
| 11 | 2 | 41 | 6 | 73 | 5 | 109 | 6 | 157 | 5 | 199 | 3 |
| 13 | 2 | 43 | 3 | 79 | 3 | 113 | 3 | 163 | 2 | 211 | 2 |
| 17 | 3 | 47 | 5 | 83 | 2 | 127 | 3 | 167 | 5 | 223 | 3 |
| 19 | 2 | 53 | 2 | 89 | 3 | 131 | 2 | 173 | 2 | 227 | 2 |

Il Corollario 13.10 ha numerose applicazioni. Eccone una: una caratterizzazione dei numeri primi $p$ tali che il polinomio $X^2 + 1$ ha un zero in $\mathbf{Z}/p\mathbf{Z}$.

**Proposizione (13.11).** *Sia $p > 2$ un numero primo. Le seguenti affermazioni sono equivalenti:*
*(i) Esiste $x \in \mathbf{Z}$ tale che $x^2 \equiv -1 \pmod{p}$.*
*(ii) Il polinomio $X^2 + 1$ ha uno zero in $\mathbf{Z}/p\mathbf{Z}$.*
*(iii) $p \equiv 1 \pmod{4}$.*

**Dimostrazione.** Le parti *(i)* e *(ii)* sono soltanto traduzioni una dell'altra.
Supponiamo *(i)*: $x^2 \equiv -1 \pmod{p}$. Allora la classe $\overline{x}$ ha ordine 4 nel gruppo $(\mathbf{Z}/p\mathbf{Z})^*$. Quindi, per il Cor.4.7, l'ordine $p-1$ di $(\mathbf{Z}/p\mathbf{Z})^*$ è divisibile per 4. Questo implica *(iii)*.
*(iii)* $\Rightarrow$ *(i)* Se $p \equiv 1 \pmod{4}$, allora l'ordine di $(\mathbf{Z}/p\mathbf{Z})^*$ è divisibile per 4. Siccome $(\mathbf{Z}/p\mathbf{Z})^*$ è un gruppo *ciclico,* contiene elementi di ordine 4. Per esempio, se $g$ indica una radice primitiva $\pmod{p}$, allora l'elemento $\overline{x} = \overline{g}^{(p-1)/4}$ ha ordine 4. Abbiamo $\overline{x}^4 - \overline{1} \equiv (\overline{x}^2 - \overline{1})(\overline{x}^2 + \overline{1}) \equiv \overline{0} \pmod{p}$. Siccome $\mathbf{Z}/p\mathbf{Z}$ è un dominio e $\overline{x}^2 \not\equiv \overline{1} \pmod{p}$, abbiamo $\overline{x}^2 \equiv -1 \pmod{p}$, come richiesto.

Concludiamo questo paragrafo con una discussione degli zeri *doppi* dei polinomi:

**Definizione.** Sia $R$ un dominio, sia $\alpha \in R$ e sia $f \in R[X]$. Se $\alpha$ è uno zero di $f$, si può, per il Cor.13.3, scrivere $f = f_1 \cdot (X - \alpha)$ dove $f_1 \in R[X]$. Se anche $f_1(\alpha) = 0$ si dice che $\alpha$ è uno zero doppio di $f$. Una seconda applicazione del Cor.13.3 ci da

$$f = f_2 \cdot (X - \alpha)^2$$

dove $f_2 \in R[X]$.

Per studiare gli zeri doppi, introduciamo il polinomio *derivato.*

**Definizione.** Sia $R$ un anello commutativo. Per un polinomio

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

definiamo il polinomio *derivato:*

$$f' = n a_n X^n + (n-1) a_{n-1} X^{n-2} + \ldots + a_1 \in R[X].$$

Si noti che questa definizione del polinomio derivato ha senso su anelli commutativi qualsiasi. Non dipende cioè dall'analisi.

**Proposizione (13.12).** *Sia $R$ un anello commutativo. Siano $f, g \in R[X]$. Allora*

$$\begin{aligned} (f+g)' &= f' + g', \\ (\alpha f)' &= \alpha f' \qquad \text{per } \alpha \in R, \\ (f \cdot g)' &= f'g + fg'. \end{aligned}$$

**Dimostrazione.** Siano $f = a_n X^n + \ldots + a_1 X + a_0$ e $g = b_m X^m + \ldots + b_1 X + b_0$ in $R[X]$. Lasciamo al lettore la facile verifica che $(f+g)' = f' + g'$ e che $(\alpha f)' = \alpha f'$ per $\alpha \in R$. 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 $f = a_n X^n + f_1$ dove $\deg(f_1) < n$. Allora

$$(f \cdot g)' = (X^n \cdot g)' + (f_1 \cdot g)'.$$

Il secondo membro si ottiene dall'ipotesi induttiva. Per il primo membro vale:

$$\begin{aligned}(X^n \cdot g)' &= (b_m X^{n+m} + \ldots + b_1 X^{n+1} + b_0 X^n)' \\ &= (n+m)b_m X^{n+m-1} + \ldots + (n+1)b_1 X^n + n b_0 X^{n-1} \\ &= nX^{n-1}g + X^n g'\end{aligned}$$

Concludiamo dunque

$$\begin{aligned}(f \cdot g)' &= nX^{n-1}g + X^n g' + f_1' g + f_1 g' \\ &= (nX^{n-1} + f_1')g + (X^n + f_1)g' = f'g + fg'\end{aligned}$$

come richiesto.

**Proposizione (13.13).** *Sia $R$ un dominio e sia $f \in R[X]$. Sia $\alpha \in R$ uno zero di $f$. Allora $\alpha$ è uno zero doppio di $f$ se e soltanto se $f'(\alpha) = 0$.*

**Dimostrazione.** Siccome $\alpha$ è uno zero di $f$ abbiamo

$$f = f_1 \cdot (X - \alpha).$$

Per la Proposizione 13.12 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 $\alpha$ come zero doppio, come richiesto.

**Esercizi.**

(13.A) Sia $f = 2X^2 + 1 \in \mathbf{Z}/6\mathbf{Z}[X]$ e sia $g = 2X + 1 \in \mathbf{Z}/6\mathbf{Z}[X]$. Far vedere che non esistono polinomi $q, r \in \mathbf{Z}/6\mathbf{Z}[X]$ tali che $f = qg + r$.

(13.B) (i) Quanti zeri ha il polinomio $X^2 - \overline{1} \in \mathbf{Z}/24\mathbf{Z}[X]$ in $\mathbf{Z}/24\mathbf{Z}$?
(ii)*Quanti zeri ha il polinomio $X^6 - \overline{1} \in \mathbf{Z}/504\mathbf{Z}[X]$ in $\mathbf{Z}/504\mathbf{Z}$?

(13.C) Sia $x = a + bi + cj + dk \in \mathbf{H}$ con $a, b, c, d \in \mathbf{R}$. Far vedere che le seguenti affermazioni sono equivalenti:
(a) $x$ è uno zero di $X^2 + 1$.
(b) $x\overline{x} = 1$ e $\overline{x} = -x$. (Si veda l'Eserc.1.F)
(c) $a = 0$ e $b^2 + c^2 + d^2 = 1$.
Concludere che gli zeri del polinomio $X^2 + 1$ in $\mathbf{H}$ sono infiniti.

(13.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 $0 \leq i \leq n$.

(13.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 $(n-1)! \equiv -1 \pmod{n}$, allora $n$ è primo.
(iii) Far vedere: se $(n-1)!$ non è congruo a 0 o a $-1$ modulo $n$, allora $n = 4$.

(13.F) Dimostrare:

(i) la più piccola radice primitiva di 41 è uguale a 6.

(ii) se $-1$ è una radice primitiva di un primo $p$, allora $p \in \{2, 3\}$.

(iii) 4 non è una radice primitiva modulo nessun numero primo.

(13.G) Sia $p$ un primo. Dimostrare che ci sono esattamente $\varphi(p-1)$ radici primitive modulo $p$. (Si veda l'Esempio 1.8 per la definizione della funzione di Eulero $\varphi$.)

(13.H) In questo esercizio diamo la dimostrazione di Gauss del Teorema 13.9. Gauss dà la sua dimostrazione soltanto nel caso $R = \mathbf{Z}/p\mathbf{Z}$, ma è facile vedere che l'argomento vale per ogni dominio di integrità $R$.
Sia $G$ un sottogruppo del gruppo moltiplicativo $R^*$ di un dominio $R$. Supponiamo che $G$ sia finito di ordine $n$ .

(i) Sia $a \in G$ un elemento di ordine $d$. Far vedere che $\{1, a, a^2, \ldots, a^{d-1}\}$ è l'insieme degli zeri del polinomio $X^d - 1$. Far vedere che $\{a^i : 0 \leq i < d, \text{mcd}(i, d) = 1\}$ sono tutti gli elementi di $G$ di ordine $d$.

(ii) Per ogni divisore $d$ di $n$, sia

$$\psi(d) = \#\{x \in G : \text{ ordine di } x \text{ è } d\}.$$

Far vedere che per ogni divisore $d$ di $n$ si ha $\psi(d) = 0$ oppure $\psi(d) = \varphi(d)$.

(iii) Dimostrare che

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

(iv) Dimostrare che

$$\phi(d) = \psi(d) \qquad \text{per ogni } d|n.$$

(Sugg. Utilizzare l'Eserc.4.F). Concludere che $G$ è un gruppo ciclico.

(C.F. Gauss: *Disquisitiones Arithmeticae,* in commissis apvd Gerh. Fleischer, Jun. Lipsiae 1801.)

I. Si numerus aliquis habetur, $a$, ad exponentem $d$ *pertinens* (*i.e.* cuius potestas $d^{ta}$ unitati congrua, omnes inferiores incongruae), omnes huius potestates, $aa, a^3, a^4 \ldots . a^d$ siue ipsarum residua minima proprietatem priorem etiam possidebunt (vt potestas ipsarum $d^{ta}$ sit congrua) et quum hoc ita etiam exprimi possit, residua minima numerorum $a, aa, a^3 \ldots . a^d$ (quae omnnia sunt diuersa) esse radices congruentiae $x^d \equiv 1$, haec autem plures quam $d$ radices diuersas habere nequeat, manifestum est, praeter numerorum $a, aa, a^3 \ldots a^d$ residua minima alios numeros inter 1 et $p-1$ incl non dari quorum potestates exponentis $d$ congruae sint vnitati. Hinc patet omnes numeros ad exponentem $d$ pertinentes inter residua minima numerorum $a, aa, a^3 \ldots . a^d$ reperiri. Quales vero sint, quantaque eorum multitudo ita definitur. Si $k$ est numerus ad $d$ primus, omnes potestates ipsius $a^k$, quarum exponentes $< d$, vnitati non erunt congrui: esto enim $\frac{i}{k} \pmod d \equiv m$ (vid. art. 31) eritque $a^{km} \equiv a$; quare potestas $e^{ta}$ ipsius $a^k$ vnitati esset congrua atque $e, d$, foret etiam $a^{kme} \equiv 1$ et hinc $a^e \equiv 1$ contra hyp. Hinc manifestum est, residuum minimum ipsius $a^k$ ad exponentem $d$ pertinere. Si vero $k$ diuisorem aliquem, $\delta$, cum $d$ communem habet, ipsius $a^k$ residuum minimum ad exponentem $d$ non pertinet; quoniam tum potestas $\frac{da}{\delta}$ iam vnitati fit congrua (erit enim $\frac{kd}{\delta}$ per $d$ diuisibilis, siue $\equiv 0 \pmod d$ adeoque $a^{\frac{kd}{\delta}} \equiv 1$). Hinc coligitur, totidem numeros ad exponentem $d$ pertinere quot numerorum $1, 2, 3 \ldots . d$ ad $d$ sint primi. At memorem esse oportet, hanc conclusionem innixiam esse suppositioni, vnum numerum $a$ iam haberi ad exponentem $d$ pertinentem. Quamobrem dubium remanet, fierine possit vt ad aliquem exponentem nullus omnino numerus pertineat; conclusioque eo limtatur vt $\psi d$ sit vel $= 0$ vel $= \phi d$.

54. II. Iam sint omnes diuisores numeri $p-1$ hi: $d, d', d''$, etc. eritque, quia omnes numeri $1, 2, 3 \ldots p-1$ inter hos sunt distributi, $\psi d + \psi d' + \psi d'' + \text{etc.} = p - 1$. At in art. 40 demonstrauimus esse $\phi d + \phi d' + \phi d'' + \text{etc.} = p - 1$, atque ex art. praec. sequitur $\psi d$ ipsi $\phi d$ aut aequalem aut ipso minorem esse, maiorem esse non posse, similiterque de $\psi d'$ et $\phi d'$, etc. Si itaque aliquis terminus ex his $\psi d, \psi d', \psi d''$etc.termino respondente ex his $\phi d, \phi d', \phi d''$, esset minor (siue etiam plures) illorum summa summae horum aequalis esse non posset. Vnde tandem concludimus *$\psi d$ ipsi $\phi d$ semper esse aequalem,* adeoque a magnitudine ipsius $p-1$ non perdere.

(13.I) (*L'indice*) Sia $p$ un primo e sia $g \in \mathbf{Z}$ una radice primitiva modulo $p$. Definiamo la funzione $\mathrm{ind} : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathbf{Z}/(p-1)\mathbf{Z}$ mediante

$$\overline{x} = \overline{g}^{\mathrm{ind}(\overline{x})} \qquad \text{per } \overline{x} \in (\mathbf{Z}/p\mathbf{Z})^*.$$

(i) Far vedere che

$$\mathrm{ind}(\overline{x}\overline{y}) = \mathrm{ind}(\overline{x}) + \mathrm{ind}(\overline{y}) \qquad \text{per } \overline{x}, \overline{y} \in (\mathbf{Z}/p\mathbf{Z})^*.$$

(ii) Dimostrare che la mappa ind è un isomorfismo di gruppi e che la mappa inversa $\mathbf{Z}/(p-1)\mathbf{Z} \longrightarrow (\mathbf{Z}/p\mathbf{Z})^*$ è data da $\overline{n} \mapsto \overline{g}^n$.

(13.J) Sia $p \equiv 1 \pmod 4$ un numero primo. Far vedere che $z = \left(\frac{p-1}{2}\right)!$ soddisfa $z^2 \equiv -1 \pmod p$.

(13.K) Per ogni $n \in \mathbf{Z}_{\geq 0}$ calcolare

$$1^n + 2^n + \ldots + (p-1)^n \pmod p.$$

(13.L) Sia $p > 3$ un numero primo.Dimostrare che le seguenti affermazioni sono equivalenti:

(a) Esiste $x \in \mathbf{Z}$ tale che $x^2 \equiv -3 \pmod p$.

(b) Il polinomio $X^2 + 3$ ha uno zero in $\mathbf{Z}/p\mathbf{Z}$.

(c) $p \equiv 1 \pmod 3$.

(Sugg. Fare la sostituzione $X = 2Y + 1$ in $X^2 + 3$. Utilizzare la fattorizzazione $Y^3 - 1 = (Y-1)(Y^2 + Y + 1)$.)

(13.M) 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 $f' \in (g^{k-1})$.

(13.N) Sia $f \in (\mathbf{Z}/2\mathbf{Z})[X]$. Dimostrare che le seguente affermazioni sono equivalenti

(a) $f' = 0$.

(b) $f$ ha la forma $f = \sum_{k=0}^{n} a_k X^{2k}$ con $a_k \in \mathbf{Z}/2\mathbf{Z}$.

(c) Esiste $g \in (\mathbf{Z}/2\mathbf{Z})[X]$ tale che $f = g^2$.

Far vedere che $(f')' = 0$.

(13.O) (*Formula di Leibniz)* Sia $R$ un anello commutativo e sia $f \in R[X]$. Per $k \in \mathbf{Z}_{\geq 0}$ definiamo induttivamente

$$f^{(0)} = f,$$
$$f^{(k)} = (f^{(k-1)})' \qquad \text{per } k \geq 1.$$

Dimostrare che per $f, g \in R[X]$ ed $n \in \mathbf{Z}_{\geq 0}$ 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.

(13.P) Sia $R$ un dominio e siano $f, g \in R[X]$ polinomi con $\deg(f) < \#R$ e $\deg(g) < \#R$. Dimostrare che

$$f = g \quad \Leftrightarrow \quad f(x) = g(x) \text{ per ogni } x \in R.$$

Concludere che per un dominio infinito si ha $f = g \quad \Leftrightarrow \quad f(x) = g(x)$ per ogni $x \in R$.

(13.Q) Sia $p$ un numero primo e siano $f, g \in (\mathbf{Z}/p\mathbf{Z})[X]$. Far vedere che

$$f(x) = g(x) \text{ per ogni } x \in \mathbf{Z}/p\mathbf{Z} \quad \Leftrightarrow \quad f - g \in (X^p - X)$$

(13.R)*Sia $p > 2$ un numero primo. In questo esercizio determiniamo la struttura dei gruppi $(\mathbf{Z}/p^n\mathbf{Z})^*$.

(i) Sia $k \in \mathbf{Z}_{\geq 0}$. Far vedere che

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}.$$

(Sugg. Utilizzare il binomio di Newton dell'Eserc.11.K)

(ii) Far vedere che $1+p \in (\mathbf{Z}/p^n\mathbf{Z})^*$ ha ordine $p^{n-1}$.

(iii) Sia $g \in \mathbf{Z}$ un intero tale che $\overline{g} \in \mathbf{Z}/p\mathbf{Z}$ é una radice primitiva. Far vedere che l'ordine di $\overline{g} \in \mathbf{Z}/p^n\mathbf{Z}$ è divisibile per $p-1$. Concludere che il gruppo $(\mathbf{Z}/p^n\mathbf{Z})^*$ contiene un elemento $\zeta$ di ordine $p-1$.

(iv) Dimostrare che l'elemento $(p-1)\zeta \in (\mathbf{Z}/p^n\mathbf{Z})^*$ ha ordine $(p-1)p^{n-1}$. Concludere che $(\mathbf{Z}/p^n\mathbf{Z})^*$ è un gruppo ciclico:

$$(\mathbf{Z}/p^n\mathbf{Z})^* \cong \mathbf{Z}/(p-1)p^{n-1}\mathbf{Z}.$$

(13.S)*In questo esercizio determiniamo la struttura dei gruppi $(\mathbf{Z}/2^n\mathbf{Z})^*$.

(i) Far vedere che $(\mathbf{Z}/2\mathbf{Z})^*$ è banale, che $(\mathbf{Z}/4\mathbf{Z})^*$ è ciclico di ordine 2 e che $(\mathbf{Z}/8\mathbf{Z})^*$ è isomorfo al gruppo $V_4$ di Klein.

(ii) Far vedere che l'elemento $5 \in (\mathbf{Z}/2^n\mathbf{Z})^*$ ha ordine $2^{n-2}$ se $n \geq 2$. (Sugg. Calcolare l'elemento $5^{2^{n-3}} = (1+4)^{2^{n-3}}$ in $(\mathbf{Z}/2^n\mathbf{Z})^*$ con il binomio di Newton).

(iii) Far vedere che gli elementi $-1$ e 5 generano $(\mathbf{Z}/2^n\mathbf{Z})^*$. Far vedere che $-1 \notin < 5 >$. Concludere che

$$(\mathbf{Z}/2^n\mathbf{Z})^* \cong < -1 > \times < 5 > \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{n-2}\mathbf{Z}.$$

(Sugg. Utilizzare l'Eserc.2.P).

(13.T) Sia $n$ un numero dispari. Dimostrare che il polinomio $X^2 - \overline{1}$ ha $2^t$ zeri in $\mathbf{Z}/n\mathbf{Z}$, dove $t$ è il numero dei primi distinti che dividono $n$ (Sugg. Utilizzare l'Eserc.13.R). Concludere che gli unici elementi di $(\mathbf{Z}/n\mathbf{Z})^*$ di ordine 2 sono $\pm 1$ se e soltanto se $n$ è una potenza di un numero primo.

## 14. Ideali primi e massimali.

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.*

**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:

$$\text{se } xy \in I, \text{ allora } x \in I \text{ oppure } y \in I.$$

**Esempio.** *(i)* L'ideale $p\mathbf{Z}$ di $\mathbf{Z}$, generato da un numero primo $p$, è un ideale primo. Questo fatto è il contenuto della Proposizione 0.7.
*(ii)* Consideriamo l'ideale generato da $X-1$ nell'anello $\mathbf{R}[X]$. Per la Prop.13.3, l'applicazione $\Psi : \mathbf{R}[X] \longrightarrow \mathbf{R}$ data da $\Psi(f) = f(1)$ ha nucleo uguale a $(X-1)$. Cioè

$$(X-1) = \{f \in \mathbf{R}[X] : f(1) = 0\}.$$

Supponiamo che $f, g \in \mathbf{R}[X]$ soddisfino $fg \in (X-1)$. Allora $f(1)g(1) = 0$ e quindi, siccome $\mathbf{R}$ 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.11.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.

**Teorema (14.1).** *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 $I$ è un ideale primo. Per definizione $I \neq R$ e quindi $R/I$ non è l'anello zero. Supponiamo che $x, y \in R$ soddisfano $\overline{x} \cdot \overline{y} = \overline{0}$ 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.

**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 14.2 il quale ci dà un criterio molto utile per decidere se un dato ideale è massimale o meno.

**Teorema (14.2).** *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 l'ideale $J/I = \{\overline{y} : y \in J\}$ è un ideale di $R/I$. Siccome $R/I$ è un campo, è anche un anello con divisione e, per la Prop.12.4, 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.

**Corollario (14.3).** *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 14.1 e 14.2.

**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 $p\mathbf{Z}$ di $\mathbf{Z}$ è massimale perchè l'anello quoziente $\mathbf{Z}/p\mathbf{Z}$ è un campo (Si veda la Prop.11.6). Per l'esempio *(i)*, l'ideale $\{0\}$ di $\mathbf{Z}$ è primo. Esso non è, però, massimale:

$$\{0\} \underset{\neq}{\subset} 2\mathbf{Z} \underset{\neq}{\subset} \mathbf{Z}.$$

Vediamo dunque che esistono ideali primi che non sono massimali.
*(iii)* L'ideale $(X^2 + 1)$ di $\mathbf{R}[X]$ è massimale perché

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

come abbiamo visto nella Proposizione 13.4.

*(iv)* Sia $I$ l'ideale $(5, Y+1, X^2+Y+2) \subset \mathbf{Z}[X,Y]$. Calcoliamo l'anello quoziente $\mathbf{Z}[X]/I$:

$$\begin{aligned}
\mathbf{Z}[X,Y]/(5, X^2+Y+1) &\cong (\mathbf{Z}/5\mathbf{Z})[X,Y]/(Y+1, X^2+Y+\overline{2}), && \text{(per 12.9(ii))}\\
&\cong (\mathbf{Z}/5\mathbf{Z}[Y]/(Y+1))/(X^2+Y+\overline{2}), && \text{(per 12.9(ii))}\\
&\cong (\mathbf{Z}/5\mathbf{Z})[X]/(X^2-\overline{1}+\overline{2}), && \text{(per 13.3(iii))}\\
&\cong (\mathbf{Z}/5\mathbf{Z})[X]/(X-\overline{2}) \times (\mathbf{Z}/5\mathbf{Z})[X]/(X+\overline{2}), && \text{(per 12.10)}\\
&\cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}. && \text{(per 12.9(i))}
\end{aligned}$$

Abbiamo utilizzato il fatto che $X^2+\overline{1} = (X-\overline{2})(X+\overline{2})$ in $(\mathbf{Z}/5\mathbf{Z})[X]$.

Siccome l'anello $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ ha divisori di zero, l'anello $\mathbf{Z}[X,Y]/(5, X^2+Y+1)$ non è un dominio di integrità. Dunque $I$ non è primo e non è massimale.
*(iv)* Sia $n$ un intero positivo e sia $R = \mathbf{R}[X_1, X_2, \ldots, X_n]$ l'anello dei polinomi in $n$ variabili su $\mathbf{R}$. L'ideale generato da $X_1$ è primo perché

$$\begin{aligned}
\mathbf{R}[X_1, X_2, \ldots, X_n]/(X_1) &\cong (\mathbf{R}[X_2, \ldots, X_n])[X_1]/(X_1)\\
&\cong \mathbf{R}[X_2, \ldots, X_n]
\end{aligned}$$

e questo anello è un dominio di integrità. Similmente, l'ideale $(X_1, X_2)$ è primo perché

$$\begin{aligned}
\mathbf{R}[X_1, X_2, \ldots, X_n]/(X_1, X_2)), &\cong (\mathbf{R}[X_2, X_3, \ldots, X_n]/(X_2))[X_1]/(X_1), && \text{(per 11.9)}\\
&\cong \mathbf{R}[X_3, \ldots, X_n].
\end{aligned}$$

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 è un ideale massimale perché $\mathbf{R}[X_1, X_2, \ldots, X_n]/(X_1, X_2, \ldots, X_n)$ è isomorfo al campo $\mathbf{R}$.

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 dello *Lemma di Zorn* (Si veda il libro di P.R. Halmos: *Teoria elementare degli insiemi,* Feltrinelli, Milano 1970).

**Lemma di Zorn.** *Sia $\Omega$ un insieme parzialmente ordinato. Se ogni catena in $\Omega$ ha un limite superiore in $\Omega$, allora $\Omega$ contiene un elemento massimale.*

Ricordiamo il significato di alcune parole: un'*ordine parziale* su l'insieme $\Omega$ 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 $\Omega$ 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 $x = y$.

**Teorema (14.5).** *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 $\Omega$ l'insieme degli ideali $I \neq R$ di $R$. L'insieme $\Omega$ è parzialmente ordinato per l'inclusione. Verifichiamo che ogni catena ha un limite superiore in $\Omega$: 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 $I_\alpha$ e $I_\beta$ 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.12.8*(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.12.8*(ii)* l'anello quoziente $R/J \cong (R/I)/(J/I)$ è un campo. Vediamo che $J$ è massimale come richiesto.

Ci sono rapporti profondi fra la struttura algebrica di certi anelli commutativi e la geometria di varietà algebriche. Per esempio, l'anello $\mathbf{R}[X_1, X_2, \ldots, X_n]$ entra nella geometria dello spazio $\mathbf{R}^n$. Ad un punto $P = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ di $\mathbf{R}^n$ si può associare l'ideale

$$M_P = \{f \in \mathbf{R}[X_1, X_2, \ldots, X_n] : f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0\}.$$

L'ideale $M_P$ è un ideale massimale perché è il nucleo dell'omomorfismo $\mathbf{R}[X_1, X_2, \ldots, X_n] \longrightarrow \mathbf{R}$ dato da $f \mapsto f(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Un'applicazione ripetuta della Prop.13.3*(ii)* fa vedere che $M_P = (X - \alpha_1, X - \alpha_2, \ldots, X - \alpha_n)$.

La corrispondenza è quasi biietiva. Basta sostituire $\mathbf{R}$ per il campo $\mathbf{C}$. Questa corrispondenza è un fenomeno generale e occorre anche per altre varietà: un punto $(\alpha, \beta)$ sul parabolo $y = x^2$ in $\mathbf{R}^2$ corrisponde all'ideale massimale $(X - \alpha, Y - \beta)$ dell'anello $\mathbf{R}[X, Y]/(Y - X^2)$. La corrispondenza diventa biietiva se si sostituisce $\mathbf{R}$ per $\mathbf{C}$.

Si può tradurre le proprietà geometriche in termini dell'algebra dell'anello corrispondente e viceversa. Per esempio, il fatto che la figura in $\mathbf{R}^2$ data dalla equazione $y^3 - yx$ si spezza in due (in una retta ed in una parabola) significa per l'anello $\mathbf{R}[X, Y]/(Y^3 - YX)$ che si spezza in un prodotto

$$\mathbf{R}[X, Y]/(Y) \times \mathbf{R}[X, Y]/(Y^2 - X).$$

Nella *geometria algebrica* si studia questa reciproca fra l'algebra e la geometria. In fatti, i tentativi di vedere l'insieme dei numeri primi di anelli come $\mathbf{Z}$, come "punti" di una curva algebrica hanno durante gli ultimi 20 anni, serviti ai teoremi più importanti nella teoria dei numeri. Si veda il libro di R. Hartshorne: *Algebraic Geometry,* Graduate Texts in Mat. **52**, Springer-Verlag, Berlin Heidelberg New York 1977.

Finalmente generalizziamo il concetto di numero primo in un terzo modo. Questa volta assumiamo che $R$ non ha divisori di zero.

**Definizione.** Sia $R$ un dominio di integrità. Un elemento $\alpha \in R$, $\alpha \neq 0$ si dice *irriducibile* se $\alpha \notin R^*$ e se per ogni $\beta, \gamma \in R$ vale

$$\text{se } \alpha = \beta\gamma \text{ allora } \beta \in R^* \text{ oppure } \gamma \in R^*.$$

**Proposizione (14.4).** *Sia $R$ un dominio di integrità e sia $\alpha \in R$ un elemento non zero. Allora, se l'ideale $(\alpha)$ è primo, l'elemento $\alpha$ è irriducibile.*

**Dimostrazione.** Per definizione $(\alpha) \neq R$ e quindi $\alpha \notin R^*$. Supponiamo che esistono $\beta, \gamma \in R$ con

$$\alpha = \beta\gamma.$$

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 $\gamma$ è un'unità. In modo simile si dimostra che $\beta$ è un'unità nel caso $\gamma \in (\alpha)$. Questo completa la dimostrazione della proposizione.

Abbiamo quindi, per $\alpha \neq 0$ in un dominio di integrità $R$:

$$(\alpha) \text{ è massimale} \quad \Rightarrow \quad (\alpha) \text{ è primo} \quad \Rightarrow \quad \alpha \text{ è irriducibile.}$$

Abbiamo visto sopra che esistono ideali primi che non sono massimali. Per esempio l'ideale $\{0\}$ di $\mathbf{Z}$ è primo, però non è massimale. Similmente esistono anche elementi $\alpha$ irriducibili in certi domini tale che gli ideali $(\alpha)$ non sono primi. Diamo un esempio:

**Esempio.** Sia $R$ l'anello $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$. In altre parole, $R$ è l'anello dato da

$$R = \mathbf{Z}[X]/(X^2 + 5).$$

La mappa $\Phi : \mathbf{Z}[X]/(X^2 + 5) \longrightarrow \mathbf{Z}[\sqrt{-5}]$ data da $\Phi(f) = f(\sqrt{-5})$ dà un isomorfismo fra le due descrizioni di $R$. Definiamo la *norma* $N$ su $R$:

$$\begin{aligned} N(a + b\sqrt{-5}) &= (a + b\sqrt{-5})(a - b\sqrt{-5}) \qquad \text{per } a, b \in \mathbf{Z} \\ &= a^2 + 5b^2. \end{aligned}$$

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 $2 \in \mathbf{Z}[\sqrt{-5}]$. Abbiamo

$$\begin{aligned} \mathbf{Z}[\sqrt{-5}]/(2) &\cong \mathbf{Z}[X]/(2, X^2 + 5), \\ &\cong (\mathbf{Z}/2\mathbf{Z})[X]/(X^2 + \overline{1}) \\ &\cong (\mathbf{Z}/2\mathbf{Z})[X]/((X + \overline{1})^2) \end{aligned}$$

Siccome l'anello $(\mathbf{Z}/2\mathbf{Z})[X]/((X + \overline{1})^2)$ ha divisori di zero: $(X + \overline{1})(X + \overline{1}) = 0$, l'ideale generato da $2 \in \mathbf{Z}[\sqrt{-5}]$ non è un ideale primo.

Per vedere che 2 è invece, irriducibile, supponiamo che abbiamo $2 = \beta\gamma$ per certi $\beta, \gamma \in \mathbf{Z}[\sqrt{-5}]$. Per la moltiplicatività della norma abbiamo

$$4 = N(2) = N(\beta)N(\gamma).$$

Scriviamo $\beta = a + b\sqrt{-5}$ dove $a, b \in \mathbf{Z}$. La norma di $\beta$ è uguale a $a^2 + 5b^2$. Siccome l'equazione $a^2 + 5b^2 = 2$ non ha soluzioni $a, b \in \mathbf{Z}$, 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 $\beta$ o $\gamma$ è un'unità e quindi che 2 è irriducibile.

**Esercizi.**

(14.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 $R[X,Y]$.

(14.B) Far vedere che l'ideale generato da 5 in $\mathbf{Z}[i]$ non è un ideale primo.

(14.C) Sia $K$ un campo e siano $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Far veder che l'ideale $(X - \alpha_1, X - \alpha_2, \ldots, X - \alpha_n)$ è un ideale massimale di $K[X_1, X_2, \ldots, X_n]$.

(14.D) Decidere se i seguenti ideali di $\mathbf{Z}[X]$ sono primi o massimali:
- (a) $(X, 3)$;
- (b) $(X^2 - 3)$;
- (c) $(7, X^2 - 3)$.

(14.E) Decidere se i seguenti ideali di $\mathbf{Q}[X,Y]$ sono primi o massimali:
- (a) $(X^2 + 1)$;
- (a) $(X - Y, Y^2 - Y)$;
- (a) $(X^2 + 1, Y^2 + 1)$;
- (a) $(X^2 + 1, Y^2 - 2)$.

(14.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.

(14.G) Sia $f : R \longrightarrow R'$ un omomorfismo di anelli commutativi. Sia $I'$ un ideale di $R'$.
- (i) Far veder che $I = f^{-1}(I')$ è un ideale di $R$. Dimostrare che $R/I$ è isomorfo con un sotoanello 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 falso.

(14.H) Sia $R$ un anello di Boole (Si veda l'Eserc.11.G).
- (i) Dimostrare che $R$ è un dominio se e soltanto se $R$ è un campo se e soltanto se $R \cong \mathbf{Z}/2\mathbf{Z}$.
- (ii) Sia $I$ un ideale di $R$. Far vedere che $I$ è primo se e soltanto se $I$ è massimale se e soltanto se $R/I \cong \mathbf{Z}/2\mathbf{Z}$.

(14.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.

(14.J) Sia $K$ un campo e sia $R = K \times K$. Determinare gli ideali primi e massimali di $R$.

(14.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 $R/I \cong \mathbf{Z}/2\mathbf{Z}$ oppure $R/I \cong \mathbf{Z}/3\mathbf{Z}$.
- (ii) Dimostrare che $I$ è un ideale massimale.

(14.L) Sia $R$ un anello commutativo con la proprietà che ogni ideale è primo. Far vedere che $R$ è un campo.

(14.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 $C([0,1])$. (Sugg. Utilizzare il lemma di Zorn)
- (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 $x_1, x_2, \ldots, x_m \in [0,1]$ tale che

$$\sum_{i=1}^{m} f_{x_i}(x)^2 > 0 \qquad \text{per ogni } x \in [0,1].$$

(Sugg. 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 $x \in [0,1]$.

(14.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 $x = 1$.

(14.O) Sia $R = \{a/b \in \mathbf{Q} : a, b \in \mathbf{Z},\ b \not\equiv 0 \pmod 5\}$. Dimostrare che $R$ è un anello locale. Determinare l'unico ideale massimale $M$ di $R$. Far vedere che $R/M \cong \mathbf{Z}/5\mathbf{Z}$.

(14.P) Decidere se i seguenti elementi di $\mathbf{Z}[\sqrt{-3}]$ sono irriducibili o meno:

$$\sqrt{-3},\ 1,\ 2,\ 1+\sqrt{-3},\ 5.$$

(14.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 $\varepsilon$ di $R$.

(ii) Si dice che due elementi $\alpha, \beta \in R$ sono *associati* se esiste un unità $\varepsilon$ di $R$ tale che $\alpha = \varepsilon\beta$. Far vedere che "essere associato" è una relazione di equivalenza.

(14.R) Far vedere che l'elemento $\sqrt{-6}$ di $\mathbf{Z}[\sqrt{-6}]$ è irriducibile, ma che l'ideale $(\sqrt{-6})$ non è un ideale primo.

(14.S)*Sia $R$ un anello commutativo e supponiamo che $a \in R$ abbia la proprietà che $a^n \neq 0$ per ogni $n \in \mathbf{Z}_{>0}$. 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 $a$.)

(14.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 $R$.

### 15. 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 $\mathbf{Z}$ e l'anello $K[X]$ dei polinomi con coefficienti in un campo $K$ ne sono esempi.

**Definizione.** Un dominio di integrità $R$ si dice un *anello a ideali principali* se ogni ideale di $R$ è un ideale principale.

**Teorema (15.1).** *Sia $R$ un anello a ideali principali. Sia $\alpha \in R$, $\alpha \neq 0$. Allora le seguenti affermazioni sono equivalenti:*

*(i) L'ideale $(\alpha)$ è massimale.*

*(ii) L'ideale $(\alpha)$ è primo.*

*(iii) L'elemento $\alpha$ è irriducibile.*

**Dimostrazione.** Per il paragrafo 14, basta dimostrare che *(iii)* implica *(i)*. Per definizione $\alpha$ non è un'unità e quindi $(\alpha) \neq R$. Supponiamo che $J$ è 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 $\alpha$ 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 $(\alpha)$ è massimale come richiesto.

**Corollario (15.2).** *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 15.1 l'ideale $I$ è dunque massimale.

Ogni campo è un anello a ideali principali. Per l'Esempio 12.4(iv) l'anello $\mathbf{Z}$ è un anello a ideali principali. Se $K$ è un campo, l'anello $K[X]$ è, per il Teorema 13.2, un anello a ideali principali. Tutti questi anelli sono, infatti, anelli *Euclidei.* Adesso introduciamo questo concetto e dimostriamo che ogni anello Euclideo è un anello a ideali principali.

**Definizione.** Un dominio di integrità $R$ si dice *Euclideo* se esiste una funzione

$$N : R - \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$$

con la proprietà: per ogni $x, y \in R$ con $y \neq 0$ esistono $q, r \in R$ con

$$\begin{aligned} &x = qy + r \\ &r = 0 \text{ oppure } N(r) < N(y). \end{aligned}$$

Si dice che $R$ è Euclideo rispetto alla funzione $N$.

Ogni campo $K$ è un anello Euclideo rispetto alla funzione

$$N : K - \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$$

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 0.1 abbiamo dimostrato che $\mathbf{Z}$ è un anello Euclideo rispetto alla funzione

$$N : \mathbf{Z} - \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$$

data da $N(x) = |x|$. La dimostrazione, data soltanto per interi positivi, si estende facilmente al caso generale. Il Teorema 13.1 afferma che l'anello $K[X]$, dove $K$ è un campo, è un anello Euclideo rispetto alla funzione $N(f) = \deg(f)$.

**Teorema (15.3).** *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 $\{N(y) : y \in I - \{0\}\} \subset \mathbf{Z}_{\geq 0}$ 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

$$\begin{aligned} &x = qy + r \\ &r = 0 \text{ oppure } N(r) < N(b). \end{aligned}$$

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.

**Teorema (15.4).** *L'anello $\mathbf{Z}[i]$ degli interi di Gauss è un anello Euclideo rispetto alla funzione*

$$N(a + bi) = a^2 + b^2 \qquad\qquad a, b \in \mathbf{Z}.$$

**Dimostrazione.** Definiamo per ogni $a, b \in \mathbf{R}$ la norma di $a+bi \in \mathbf{C}$ per $N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$. Per l'Eserc.1.F la norma è moltiplicativa e quindi possiamo definirla sul campo quoziente di $\mathbf{Z}[i]$ per $N(\alpha/\beta) = N(\alpha)/N(\beta)$ per $\alpha, \beta \in \mathbf{Z}[i]$, $\beta \neq 0$.

Siccome $N(0) = 0$, possiamo anche dire che l'anello $\mathbf{Z}[i]$ è Euclideo se per ogni due elementi $\alpha, \beta \in \mathbf{Z}[i]$, $\beta \neq 0$, esiste $q \in \mathbf{Z}[i]$ tale che $N(\alpha - q\beta) < N(\beta)$. Dividendo adesso per $N(\beta)$ troviamo: l'anello $\mathbf{Z}[i]$ è Euclideo se per ogni elemento $\alpha/\beta$ nel campo quoziente di $\mathbf{Z}[i]$ esiste un elemento $q \in \mathbf{Z}[i]$ tale che

$$N(\frac{\alpha}{\beta} - q) < 1.$$

Vediamo $\mathbf{Z}[i]$ come sottoanello di $\mathbf{C}$. La norma $a^2 + b^2$ di un elemento $z = a + bi \in \mathbf{Z}[i]$ è uguale al quadrato della valore assoluto $|z| = \sqrt{a^2 + b^2}$ di $\mathbf{C}$. Per dimostare che $\mathbf{Z}[i]$ è un anello Euclideo, basta dunque dimostrare che per ogni $\xi \in \mathbf{C}$ esiste $q \in \mathbf{Z}[i]$ tale che

$$|\xi - q| < 1;$$

in altre parole, basta vedere che i cerchi con raggi 1 e centri in $\mathbf{Z}[i]$ coprono $\mathbf{C}$. Ma questo fatto è ovvio dal disegno:

Questo finisce la dimostrazione.

Per il Teorema 15.3, l'anello $\mathbf{Z}[i]$ degli interi di Gauss è anche un anello a ideali principali. Questo fatto implica il seguente teorema classico sui numeri primi.

**Corollario (15.5).** *Sia $p \neq 2$ un numero primo. Allora $p = a^2 + b^2$ per certi interi $a, b$ se e soltanto se $p \equiv 1 \pmod 4$.*

**Dimostrazione.** Se $p = a^2 + b^2$, allora $(a/b) \equiv -1 \pmod 4$. Per la Prop.13.11 abbiamo dunque $p \equiv 1 \pmod 4$.

Viceversa, se $p \equiv 1 \pmod 4$ esiste per la Prop.13.11 un intero $z \in \mathbf{Z}$ tale che $z^2 \equiv -1 \pmod p$. Possiamo scegliere $z$ tale che

$$-\frac{p}{2} < z < \frac{p}{2}.$$

Consideriamo l'ideale $I = (p, z - i)$ di $\mathbf{Z}[i]$. Siccome $\mathbf{Z}[i]$ è un anello a ideali principali, esiste $a + bi \in \mathbf{Z}[i]$ 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

$I = \mathbf{Z}[i]$, ma si ha

$$\begin{aligned}\mathbf{Z}[i]/I &= \mathbf{Z}[i]/(p, z-i),\\ &\cong \mathbf{Z}[X]/(X^2+1, p, z-X),\\ &\cong \mathbf{Z}/(z^2+1, p), \qquad\qquad \text{(per 11.9)}\\ &\cong \mathbf{Z}/p\mathbf{Z}.\end{aligned}$$

Concludiamo che $a^2 + b^2 = p$ come richiesto.

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 0.8) afferma che $\mathbf{Z}$ è un anello a fattorizzazione unica. La fattorizzazione di numeri interi è unica solo almeno dell'ordine dei fattori e almeno di moltiplicazione per unità. Per esempio, non si considerino le fattorizzazioni

$$\begin{aligned}-15 &= -3 \cdot 5\\ &= 3 \cdot -5\\ &= 5 \cdot -3\\ &= -5 \cdot 3\end{aligned}$$

come essenzialmente distinte. Per trattare problemi di questo tipo diamo la seguente definizione:

**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.15.B).

Due elementi associati hanno le stesse proprietà di divisibilità: se $\alpha$ e $\beta$ sono associati, allora, per ogni $\gamma \in R$, $\alpha$ divide $\gamma$ se e soltanto se $\beta$ divide $\gamma$. In questioni di divisibilità, gli elementi associati non si distinguono in modo essenziale.

**Definizione.** Un dominio di integrità $R$ si dice un *anello a fattorizzazione unica* se si può scrivere ogni elemento $x \in R$ come prodotto di un'unità e un numero finito di elementi irriducibili:

$$x = u \cdot \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_t$$

dove $u \in R^*$, $t \in \mathbf{Z}_{\geq 0}$ 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 $\pi_i'$, si ha $s = t$ e c'è una permutazione $\sigma$ di $\{1, 2, \ldots, t\}$ tale che $\pi_i'$ e $\pi_{\sigma(i)}$ sono associati.

Per i domini a fattorizzazione unica vale una versione debole del Teorema 15.1:

**Proposizione (15.6).** *Sia $R$ un dominio a fattorizzazione unica e sia $\pi \in R$. Allora $\pi$ è irriducibile se e soltanto se l'ideale $(\pi)$ è primo.*

**Dimostrazione.** Se $(\pi)$ è un ideale primo, l'elemento $\pi$ è automaticamente irriducibile. Supponiamo che $\pi$ sia irriducibile. Siano $\beta, \gamma \in R$ con $\beta\gamma \in (\pi)$. Scriviamo $\beta$ e $\gamma$ come prodotto di elementi irriducibili di $R$. Siccome questa fattorizzazione è unica, abbiamo che $\pi$ occorre nella fattorizzazione di $\beta$ o di quella di $\gamma$. In altre parole $\beta \in (\pi)$ o $\gamma \in (\pi)$.

**Teorema (15.7).** *Un anello a ideali principali è un anello a fattorizzazione unica.*

**Dimostrazione.** Sia $R$ un anello a ideali principali. Supponiamo che esiste un elemento $x \in R$, $x \neq 0$ non uguale a un prodotto di un unità ed un numero finito di elementi irriducibili. Costruiamo una successione di elementi $x_i$ di $R$. sia $x_1 = x$. Ovviamente $x$ non è un'unità e non è irriducibile. Sia $x = \beta_1\gamma_1$ una fattorizzazione di $x$ con $\beta_1, \gamma_1 \notin R^*$. Almeno uno degli elementi $\beta_1, \gamma_1$, diciamo $\beta_1$, 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 $(x_1)$ contiene strettamente l'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 $\beta_2, \gamma_2$, diciamo $\beta_2$, 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 $(x_2)$ contiene strettamente l'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 $I = \cup_{i=1}^{\infty}$ è un ideale di $R$ ed è dunque principale. Sia $\alpha$ un generatore. Allora $\alpha$ 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 $x$ avessi 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 dove $x$ ha zero fattori irriducibili.

Supponiamo adesso che $x$ ha 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 $(\pi'_1)$ è primo e abbiamo $\pi_i \in (\pi'_1)$ per un certo indice $i$. Siccome $\pi_i$ 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 $x/\pi_i$ 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.

Gli anelli $\mathbf{Z}$ e $\mathbf{Z}[i]$ 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.

L'anello $\mathbf{Z}[\sqrt{-5}]$ non ha fattorizzazione unica. Per esempio, l'elemento $\in \mathbf{Z}[\sqrt{-5}]$ ha le due fattorizzazioni

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \end{aligned}$$

Per vedere che queste fattorizzazioni sono essenzialmente diverse, utilizziamo la norma $N$ (si veda l'ultimo esempio del paragrafo 14). Si vede facilmente che $\varepsilon \in \mathbf{Z}[\sqrt{-5}]$ è un'unità se e soltanto se $N(\varepsilon) = 1$. Dunque, se uno degli elementi $2, 3, 1 \pm \sqrt{-5}$ non fosse irriducibili, ci dovrebbe esistere fattori irriducibili $a + b\sqrt{-5}$ con la norma $a^2 + 5b^2$ uguale a 2 o 3. Siccome gli equazioni $a^2 + 5b^2 = 2$

e $a^2+5b^2=3$ non hanno soluzioni $a,b\in\mathbf{Z}$, 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 $a=\pm1$ e $b=0$. Dunque, le uniche unità in $\mathbf{Z}[\sqrt{-5}]$ sono $\pm1$. 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 distinti e l'anello $\mathbf{Z}[\sqrt{-5}]$ non ha fattorizzazione unica.

**Esempio.** *(Elementi irriducibili di $\mathbf{Z}[i]$)*
Determiniamo tutti gli elementi irriducibili di $\mathbf{Z}[i]$. Ogni elemento irriducibile $\pi\in\mathbf{Z}[i]$ divide $\pi\overline{\pi}\in\mathbf{Z}$. Dunque, per trovare tutti gli elementi irriducibili di $\mathbf{Z}[i]$ basta fattorizzare gli interi $n\in\mathbf{Z}$ nell'anello di Gauss. Per fare questo basta fattorizzare i numeri primi $p\in\mathbf{Z}$.

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 $\mathbf{Z}[i]$ (si veda l'Eserc.11.L). L'elemento $1+i$ è irriducibile perché la norma $N(i+1)$ è uguale a 2 (si veda l'Eserc.15.E).

Sia $p\equiv1 \pmod 4$ un primo. Per il Cor.15.5, $p=a^2+b^2$ per certi interi $a,b\in\mathbf{Z}$. In altre parole, $p=\pi\overline{\pi}$ dove $\pi=a+bi$ ha norma $p$ ed è dunque irriducibile. Per l'Eserc.15.E gli elementi $\pi$ e $\overline{\pi}$ non sono associati. Essi sono, dunque, elementi irriducibili essenzialmente distinti. Sia finalmente $p\equiv3 \pmod 4$ un primo. Se $p$ non fosse irriducibile allora $p=\beta\gamma$ con $\beta,\gamma\notin\mathbf{Z}[i]^*$. Siccome $p^2=N(p)=N(\beta)N(\gamma)$, questo implica, per l'Eserc.11.F, che $N(\beta)=N(\gamma)=p$. Se scriviamo $\beta=a+bi$, troviamo $p=a^2+b^2$ contraddicendo il Cor.15.5. Dunque, $p$ è irriducibile in $\mathbf{Z}[i]$.

Concludiamo che i soli elementi primi $\pi$ in $\mathbf{Z}[i]$ sono, almeno di moltiplicazione per le unità 1, $-1$, $i$ e $-i$:

$$\begin{aligned}\pi &= 1+i\\ &= p \qquad \text{dove } p \text{ è un numero primo congruo a 3 (mod 4),}\\ &= a\pm bi \qquad \text{dove } p=a^2+b^2 \text{ è un primo congruo a 1 (mod 4).}\end{aligned}$$

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 almeno 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 $2+i$ è 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 trova 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 $\mathbf{Z}[i]$ è un prodotto di elementi irriducibili. Per esempio

$$180+1992i=-i(1+i)^4\cdot3\cdot(3+2i)\cdot(36-29i).$$

Il fattore $3+2i$ è un divisore di 13 e il fattore $36-29i$ è un divisore del primo 2137.

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 nella altra direzione sono tutte le due false. Per esempio, l'anello

$$\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$$

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.15.N e 15.O per una dimostrazione ad hoc del fatto che l'anello $\mathbf{Z}[(1+\sqrt{-19})/2]$ non è Euclideo, ma è a ideali principali.

Nel paragrafo 16 vedremo che l'anello $\mathbf{Z}[X]$ ha fattorizzazione unica, ma non è un anello a ideali principali.

**Esercizi.**

(15.A) Far vedere che il polinomio $X^2+3 \in \mathbf{Q}[X]$ è irriducibile. Dimostrare che l'anello

$$\mathbf{Q}[X]/(X^2+3)$$

è un campo.

(15.B) Dimostrare che l'anello $\mathbf{Z}[\sqrt{-2}]$ è un anello Euclideo rispetto alla norma $N(a+b\sqrt{-2}) = a^2+2b^2$. Si veda l'Eserc.11.N per la definizione di $\mathbf{Z}[\sqrt{-2}]$. (Sugg. Generalizzare la dimostrazione del Teorema 15.3.)

(15.C) Trovare quoziente $q$ e resto $r$ della divisone di $5+\sqrt{-2}$ per $2+2\sqrt{-2}$ nell'anello $\in \mathbf{Z}[\sqrt{-2}]$ tale che $N(r) < N(2+2\sqrt{-2}) = 8$.

(15.D) Calcolare $\mathrm{mcd}(4+7i, 7-9i)$. Fattorizzare $4+7i$ e $7-9i$ in fattori irriducibili in $\mathbf{Z}[i]$.

(15.E) Siano $a, b \in \mathbf{Z}$ a sia $a+bi \in \mathbf{Z}[i]$.

(i) Dimostrare che $a+bi$ è irriducibile si $a^2+b^2$ 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 $\pi \in \mathbf{Z}[i]$ un elemento irriducibile. Far vedere: se $\pi$ è associato a $\overline{\pi}$ allora $\pi$ è associato a $1+i$ oppure a un numero primo $p \equiv 3 \pmod 4$.

(15.F) Sia $p$ un primo congruo a 3 (mod 4). Far vedere che $\mathbf{Z}[i]/(p)$ è un campo finito di ordine $p^2$.

(15.G) Sia $\rho \in \mathbf{C}$ uno zero del polinomio $X^2+X+1$. Far vedere che l'anello $\mathbf{Z}[\rho]$ è un anello Euclideo ripetto alla norma $N(x) = x\overline{x}$.

(15.H) Sia $p \neq 3$ un numero primo. Dimostrare che le seguenti affermazioni sono equivalenti:

(a) $p \equiv 1 \pmod 3$.

(b) Esiste $z \in \mathbf{Z}$ tale che $z^2+z+1 \equiv 0 \pmod p$.

(c) Esistono $a, b \in \mathbf{Z}$ tali che $p = a^2+ab+b^2$.

(15.I) Sia $m$ un intero positivo che non è un quadrato, e consideriamo l'anello $\mathbf{Z}[\sqrt{m}] = \{a+b\sqrt{-m} : a, b \in \mathbf{Z}\}$ dell'Eserc.11.N. Sia

$$N : \mathbf{Z}[\sqrt{m}] \longrightarrow \mathbf{Z}_{\geq 0}$$

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 $\alpha, \beta \in \mathbf{Z}[\sqrt{m}]$.

Concludere che la norma $N$ sul campo quoziente di $\mathbf{Z}[\sqrt{m}]$ data da $N(\alpha/\beta) = N(\alpha)/N(\beta)$ è ben definita.

(ii) Far vedere che per ogni $\alpha, \beta \in \mathbf{Z}[\sqrt{m}]$ con $\beta \neq 0$ esiste $\gamma \in \mathbf{Z}[\sqrt{m}]$ tale che

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < \frac{1+|m|}{4}$$

(iii) Dimostrare che $\mathbf{Z}[\sqrt{m}]$ è Euclideo per $m = -1$, 2, $-2$ e 3.

Nel 1950 Chatland e Davenport hanno dimostrato che l'anello $\mathbf{Z}[\sqrt{m}]$ 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)

(15.J) 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
(a) $N^*(xy) \geq N^*(x)$ per ogni $x, y \in R - \{0\}$.
(b)*Per ogni $x, y \in R$ con $y \neq 0$ esistono $q, r \in R$ con

$$x = qy + r$$
$$r = 0 \text{ oppure } N^*(r) < N^*(y).$$

(Sugg. Considerare $z \in R$ tale che il resto $r_z$ della divisione di $xz$ per $xy$ ha $N(r_z)$ minimale.

(15.K) Sia $p$ un primo e sia $R = \{r/s \in \mathbf{Q} : p \text{ non divide } s\}$. (Si veda l'Eserc.14.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 $k \in \mathbf{Z}_{\geq 0}$ e questo in modo unico.
(ii) Dimostrare che $R$ è un anello Euclideo rispetto alla norma $N(x) = k$ per $x = u \cdot p^k$ come nella parte $(ii)$.

(15.L) Sia $R$ un anello commutativo. Sia $R[[X]]$ *l'anello delle serie formali:*

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

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 $R$ è un campo. Sia

$$N : R[[X]] - \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$$

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 $N$.

(15.M) Sia

$$\alpha = \frac{1 + \sqrt{-19}}{2} \in \mathbf{C}$$

e sia $R = \mathbf{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbf{Z}\}$ l'anello dell'Eserc.11.O. definiamo la norma

$$N : R \longrightarrow \mathbf{Z}_{\geq 0}$$

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

$$\varphi : R \longrightarrow \mathbf{Z}/2\mathbf{Z}$$

e non esiste neanche un omorfismo di anelli

$$\varphi : R \longrightarrow \mathbf{Z}/3\mathbf{Z}.$$

(Sugg. Dovrebbe essere $\varphi(\alpha)^2 - \varphi(\alpha) + 5 = 0$.)

(15.N)*Lo scopo si questo esercizio è di dimostrare che l'anello $R = \mathbf{Z}[\alpha]$ dell'Eserc.15.M *non* è Euclideo. Supponiamo che $R$ sia Euclideo rispetto una funzione $N : R - \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$. 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 $x \equiv \varepsilon \pmod{(b)}$.

(ii) Far vedere che

$$R/(b) \cong \mathbf{Z}/2\mathbf{Z} \quad \text{oppure} \quad \mathbf{Z}/3\mathbf{Z}.$$

(iii) Far vedere che la conclusione della parte (ii) contraddice l'Eserc.15.K(iv). Concludere che $R$ non è Euclideo.

(15.O)*Lo scopo si questo esercizio è di dimostrare che l'anello $R = \mathbf{Z}[\alpha]$ dell'Eserc.15.M è a ideali principali. Sia $N$ la funzione dell'Eserc.15.M.

(i) Siano $x, y \in R \subset \mathbf{C}$, $y \neq 0$. Far vedere che esistono quoziente e resto $q, r \in R$ tali che

$$\begin{aligned} x &= qy + r \\ r &= 0 \quad \text{oppure } N(r) < N(y) \end{aligned}$$

se e soltanto se l'elemento $x/y \in \mathbf{C}$ 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 $x, y \in R \subset \mathbf{C}$, $y \neq 0$. Dimostrare che se *non* si può dividere $x$ per $y$ con resto piccolo, allora si può dividere $2x$ e uno di $\alpha x$ 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. copiare la dimostrazione del Teorema 13.2).

(15.P) Sia $\alpha = a + bi \in \mathbf{Z}[i]$. Far vedere che $\mathrm{ord}_p(a^2 + b^2)$ è pari per ogni primo $p \equiv 3 \pmod 4$. Concludere che si può scrivere $n \in \mathbf{Z}_{>0}$ come somma di due quadrati se e soltanto se $\mathrm{ord}_p(n)$ è pari per ogni primo $p \equiv 3 \pmod 4$.

(15.Q)*Sia $n \in \mathbf{Z}$. Definiamo

$$r_2(n) = \#\{(a, b) \in \mathbf{Z}^2 : a^2 + b^2 = n\}.$$

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

$$\left( \sum_{n \in \mathbf{Z}} X^{n^2} \right)^2 = \sum_{n \in \mathbf{Z}} r_2(n) X^n$$

(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 $\pi = 3,1415926\ldots$.

## 16. Fattorizzazione di polinomi.

In questo paragrafo studiamo gli anelli di polinomi con coefficienti in un dominio a fattorizzazione unica. L'anello $\mathbf{Z}[X]$ 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.

**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 $\pi$ che occorrono nella fattorizzazione di $x$.

Questa definizione generalizza quella che abbiamo dato per gli interi usuali nel paragrafo 0. 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 $\pi$ e $\pi'$ sono associati.

Con la Prop.0.9*(iii)* in mente, definiamo adesso il *massimo comun divisore* di due elementi $x, y \in R$:

**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 $\pi$ 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: $\mathrm{mcd}(x_1, x_2, \ldots, x_t) = \mathrm{mcd}(x_1, \mathrm{mcd}(x_2, \ldots, x_t))$.

**Proposizione (16.1).** *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 $\pi$.*

*(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.

**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.*

Per esempio, il polinomio $-2X^5 + 4X^3 - 6 \in \mathbf{Z}[X]$ ha contenuto 2 (o anche $-2$). Il polinomio $6X^4 - 10X + 15 \in \mathbf{Z}[X]$ è primitivo. Ogni polinomio monico in $\mathbf{Z}[X]$ è anche primitivo.

**Lemma (16.2).** *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 $\alpha/\beta$ 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 $\delta = \text{cont}(h)$. Per la Prop.16.1*(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

$$\begin{aligned} g &= c \cdot g_0, \\ &= c' \cdot g_0' \end{aligned}$$

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

$$c = \text{cont}(c \cdot g_0) = \text{cont}(c \cdot g_0') = c'$$

e dunque anche $g_0 = g_0'$ come richiesto.

**Lemma (16.3).** *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 $(\pi)$ è, per la Prop.15.6, un ideale primo. Per il Teorema 14.1, l'anello $R/(\pi)$ è dunque un dominio di integrità e per l'Eserc.11.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 $\pi$ divide $\text{cont}(f)$ o $\text{cont}(g)$. Questa contraddizione finisce la dimostrazione.

**Esempio.** *(Fattori di grado 1.)* Sia $R$ un dominio di integrità. Per il Teorema 13.5, 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.

**Proposizione (16.4).** *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 $g = b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \ldots + b_1X + b_0 \in K[X]$. Per il Lemma 16.2, 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

$$a_n = vb_{n-1},$$
$$a_0 = -ub_0.$$

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 $a_n \in R^*$.

Per esempio, sia $f = 2X^3 + X^2 - X + 3 \in \mathbf{Z}[X]$ e sia $u/v \in \mathbf{Q}$, dove $u, v \in \mathbf{Z}$ soddisfano $\mathrm{mcd}(u, v) = 1$, uno zero di $f$. Per la Prop.16.4 può essere $u = \pm 1$ oppure $\pm 3$ e $v = 1$ oppure 2. Si verifica infatti, che $\alpha = -3/2$ è uno zero di $f$.

**Proposizione (16.5).** *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 a meno uno fra $g$ e $h$ avrebbe grado 1.

La Prop.16.5 è falsa se il grado di $f$ è più grande. Per esempio, il polinomio $X^4 + 5X^2 + 1$ non ha zeri in $\mathbf{Q}$, ma non è irriducibile perché

$$\begin{aligned} X^4 + 5X^2 + 1 &= (X^2 + 3)^2 - X^2 \\ &= (X^2 + X + 3) \cdot (X^2 - X + 3) \end{aligned}$$

**Teorema (16.6).** *(Lemma di Gauss) Sia $R$ un dominio a fattorizzazione unica e sia $K$ il campo quoziente di $R$.*

*(i) Supponiamo che $f \in R[X]$ sia monico e che*

$$f = g \cdot h$$

*dove $g, h \in K[X]$ sono polinomi monici. Allora $g, h \in R[X]$.*

*(ii) 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.** Per il Lemma 16.2. esistono $\alpha, \beta \in K^*$ tali che $\alpha f$ e $\beta g$ sono polinomi primitivi in $R[X]$. Siccome $g$ e $h$ sono monici, deve essere $\alpha, \beta \in R$. Abbiamo

$$(\alpha\beta)f = (\alpha g)(\beta h).$$

Il polinomio $f$ è monico e dunque primitivo. Per il Lemma 16.3, il polinomio $(\alpha g)(\beta h)$ è primitivo. Quindi, per la parte "unicità" del Lemma 16.2 abbiamo $\alpha\beta \in R^*$ e, dunque, $\alpha, \beta \in R^*$. Concludiamo che $g, h \in R[X]$ come richiesto.

*(ii)* Supponiamo che $f = g \cdot h$ dove $g, h \in K[X]$ con $\deg(g), \deg(h) > 0$. Per il Lemma 16.2 esistono unici $\alpha, \beta \in K^*$ tali che $g = \alpha \cdot g_0$, $h = \beta \cdot h_0$ e $g_0, h_0 \in R[X]$ sono polinomi primitivi. Abbiamo $f = \alpha\beta \cdot g_0h_0$ e per il Lemma 16.2 e 16.3 troviamo che $\alpha\beta \in R^*$. Questo dimostra che $f$ è riducibile in $R[X]$.

Viceversa, supponiamo che $f = g \cdot h \in R[X]$ con $g, h \notin R[X]^*$. Siccome $f$ è primitivo, $g$ e $h$ non sono polinomi costanti. Questo implica che $f = g \cdot h$ è una fattorizzazione non banale in $K[X]$ come richiesto.

Per esempio, siccome $\sqrt{2} \notin \mathbf{Z}$, il polinomio $X^2 - 2 \in \mathbf{Z}[X]$ è irriducibile. Per il Lemma di Gauss, il polinomio $X^2 - 2$ è anche irriducibile nell'anello $\mathbf{Q}[X]$. In altre parole $\sqrt{2} \notin \mathbf{Q}$.

**Corollario (16.7).** *Sia $f \in \mathbf{Z}[X]$ un polinomio monico, supponiamo che esista un numero primo $p$ tale che $f \pmod p \in \mathbf{Z}/p\mathbf{Z}[X]$ è irriducibile; allora $f$ è irriducibile in $\mathbf{Z}[X]$ e in $\mathbf{Q}[X]$.*

**Dimostrazione.** Per il lemma di Gauss, $f$ è irriducibile in $\mathbf{Q}[X]$ se e soltanto se è irriducibile in $\mathbf{Z}[X]$. Se fosse $f = g \cdot h$ con $g, h \in \mathbf{Z}[X]$, allora $f \pmod p = (g \pmod p)(h \pmod p)$ sarebbe una fattorizzazione di $f$ in $\mathbf{Z}/p\mathbf{Z}[X]$.

**Esempio.** Sia $f = X^4 + 3X^3 - X^2 - X + 27 \in \mathbf{Z}[X]$. Prendiamo $p = 2$. Il polinomio $f \pmod 2 = X^4 + X^3 + X^2 + X + 1$ è irriducibile in $\mathbf{Z}/2\mathbf{Z}[X]$ perché non ha zeri in $\mathbf{Z}/2\mathbf{Z}$ e non è divisibile per l'unico polinomio quadratico irriducibile in $\mathbf{Z}/2\mathbf{Z}[X]$, vale a dire $X^2 + X + 1$. Concludiamo che $f$ è irriducibile in $\mathbf{Q}[X]$.

Anche se $f \pmod p$ non è irriducibile, la fattorizzazione di $f \pmod p$ in $\mathbf{Z}/p\mathbf{Z}[X]$ può dare informazione: sia $f = X^4 - X^2 + X + 2$. Utilizzando la Prop.16.4, si verifica che $f$ non ha zeri in $\mathbf{Q}$. Dunque, se $f$ fosse irriducibile, allora sarebbe il prodotto di due fattori di grado 2. Quindi sarebbe anche possibile scrivere $f \pmod 2$ come prodotto di due fattori di grado 2 in $\mathbf{Z}/2\mathbf{Z}[X]$. Ma

$$X^4 - X^2 + X + 2 = X(X^3 + X + 1) \qquad \text{in } \mathbf{Z}/2\mathbf{Z}[X]$$

dove il polinomio $X^3 + X + 1$ è irriducibile. Concludiamo che $f$ è irriducibile in $\mathbf{Z}[X]$ e $\mathbf{Q}[X]$.

**Teorema (16.8).** *(Criterio di Eisenstein). Sia $R$ un dominio a fattorizzazione unica e sia $\pi$ 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*

$$\begin{aligned} &\pi \text{ non divide } a_n, \\ &\pi \text{ divide } a_k \text{ per } k = 0, 1, 2, \ldots, n-1, \\ &\pi^2 \text{ non divide } a_0. \end{aligned}$$

*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 troviamo che

$$g \equiv bX^k \pmod \pi \quad \text{e} \quad h \equiv cX^{n-k} \pmod \pi$$

per certi $b, c \in R$ e $k \in \mathbf{Z}_{>0}$. In particolare, i termini noti di $g$ ed $h$ sono divisibili per $\pi$. Ma questo implica che $\pi^2$ divide $a_0$. Questa contraddizione finisce la dimostrazione.

Per esempio, prendiamo $R = \mathbf{Z}$ e $f = X^5 + 2X^3 - 6$. Questo polinomio è irriducibile perché è un polinomio di Eisenstein rispetto al primo 2.

Prendiamo $R = \mathbf{R}[Y]$. 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 $\mathbf{R}[X, Y]$.

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 $2X^5-4X^2+3 \in \mathbf{Z}[X]$ 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.16.M, il polinomio $g(X) = f(aX + b)$ è irriducibile se e soltanto se $f$ è irriducibile. Per esempio, il polinomio

$$f = X^5 + 2X^4 + 3X^3 + 4X^2 + 5X + 6 \quad \text{in } \mathbf{Q}[X]$$

è irriducibile perchè il polinomio

$$f(X + 1) = X^5 + 7X^4 + 21X^3 + 35X^2 + 35X + 21$$

è di Eisenstein rispetto a 7.

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 $f \in \mathbf{Z}[X]$ sia un polinomio primitivo di grado 4 e che si sia già verificato, utilizzando la Prop.16.4, che $f$ non ha zeri in $\mathbf{Q}$, allora si scrive

$$f = (b_2X^2 + b_1X + b_0)(c_2X^2 + c_1X + c_0)$$

e si risolvono le equazioni

$$\begin{aligned} b_2c_2 &= a_4, \\ b_2c_1 + b_1c_2 &= a_3, \\ b_2c_0 + b_1c_1 + b_0c_2 &= a_2, \\ b_1c_0 + b_0c_1 &= a_1, \\ b_0c_0 &= a_0. \end{aligned}$$

Ci sono soltanto un numero finito di possibilità per $b_2, c_2, b_0, c_0 \in \mathbf{Z}$ 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.

Concludiamo questo paragrafo con un risultato generale.

**Teorema (16.9).** *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 $s, t \in \mathbf{Z}_{\geq 0}$, 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.** 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 16.2 possiamo, cambiando $\alpha$, assumere che i polinomi $g_i$ sono primitivi. Per il Lemma 16.3 anche il

prodotto $g_1 \cdot g_2 \cdot \ldots \cdot g_t$ è primitivo e quindi, per il Lemma 16.2, ha il costante $\alpha$ è in $R$ 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 $\pi_i$ 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 16.9, 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 $\pi_i$ di $R$ oppure a un polinomio primitivo $g_i$ in $R[X]$ che è irriducibile in $K[X]$.

Viceversa, sia $\pi$ un elemento irriducibile di $R$. Se $\pi$ 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 finisce la dimostrazione del Teorema 16.9.

**Corollario (16.10).** *Sia $n$ un intero positivo. Allora*
*(i) L'anello $\mathbf{Z}[X_1, X_2, \ldots, X_n]$ 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 $\mathbf{Z}$ 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.

Abbiamo visto nell'Esempio 12.2 che l'ideale $(2, X) \subset \mathbf{Z}[X, Y]$ non è principale. L'anello $\mathbf{Z}[X]$ 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.16.10, 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 genera 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 $\mathbf{R}[X, Y]$ sono irriducibili e distinti, abbiamo che $\mathrm{mcd}(X, Y) = 1$, ma l'ideale $(X, Y)$ contiene esattamente i polinomi $F(X, Y) \in \mathbf{R}[X, Y]$ con $f(0, 0) = 0$. Dunque $(X, Y) \neq \mathbf{R}[X, Y]$.

**Esercizi.**

(16.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 $\pi$ 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 $R$.

(16.B) (i) Determinare $\mathrm{cont}(f)$ di $f = 2X^3 - 4/3 \in \mathbf{Q}[X]$.

(ii) Sia $g(X,Y) = XY^2 + X^2Y + YX \in \mathbf{R}[X,Y]$. Calcolare il contenuto di $g$ considerato come polinomio in $X$ e coefficienti in $\mathbf{R}[Y]$. Calcolare il contenuto di $g$ considerato come polinomio in $Y$ e coefficienti in $\mathbf{R}[X]$.

(16.C) Dimostrare che $X^n - 3$ è irriducibile in $\mathbf{Z}[X]$ per ogni $n \in \mathbf{Z}_{>0}$.

(16.D) Fattorizzare i polinomi $X^8 - 16$ e $X^6 + 27$ in fattori irriducibili in $\mathbf{Q}[X]$.

(16.E) Sia $p$ un primo.

(i) Far vedere che il polinomio

$$X^{p-1} + X^{p-2} + \ldots + X + 1$$

è irriducibile in $\mathbf{Q}[X]$.

(ii) Far vedere che il polinomio

$$\frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}$$

è irriducibile in $\mathbf{Q}[X]$ per ogni $n \in \mathbf{Z}_{\geq 1}$.

(16.F) Il polinomio $5X^4 + 10X + 10$ è di Eisenstein? È irriducibile in $\mathbf{Q}[X]$. In $\mathbf{Z}[X]$?

(16.G) (i) Trovare un polinomio irriducibile $f(X) \in \mathbf{Z}[X]$ tale che $f(X^2)$ non è irriducibile.

(ii) Sia $f \in \mathbf{Z}[X]$ un polinomio di Eisenstein. Far vedere che $f(X^2)$ è irriducibile in $\mathbf{Z}[X]$.

(16.H) Fattorizzare i seguenti polinomi in fattori irriducibili in $\mathbf{Q}[X]$ e in $\mathbf{Z}[X]$:

$$4X^2 + 4,$$
$$2X^{10} + 4X^5 + 3,$$
$$X^4 - 7X^2 + 5X - 3,$$
$$X^{111} + 9X^{74} + 27X^{37} + 27,$$
$$X^3 + X + 3.$$

(16.I) Fattorizzare i seguenti polinomi in fattori irriducibili in $\mathbf{Q}[X]$ e in $\mathbf{Z}[X]$:

$$\frac{1}{7}((X+1)^7 - X^7 - 1),$$
$$X^3 + 3X^2 + 6X + 9,$$
$$X^4 + 2X^3 + 3X^2 + 9X + 6,$$
$$X^{12} - 1,$$
$$X^4 - X^3 + X^2 - X + 1.$$

(16.J) Fattorizzare i seguenti polinomi in fattori irriducibili in $\mathbf{Q}[X,Y]$:

$$Y^4 + X^2 + 1,$$
$$Y^3 - (X+1)Y^2 + Y + X(X-1),$$
$$X^n + Y^3 + Y \qquad (n \geq 1),$$
$$X^4 + 4Y^4,$$
$$X^4 + 2X^3 + X^2 - Y^2 - 2Y - 1,$$
$$Y^n - 13X^4 \qquad (n \geq 1).$$

(16.K) Determinare tutti i polinomi irriducibili di grado al più 3 in $\mathbf{Z}/2\mathbf{Z}[X]$.

(16.L) Per ciascuno degli anelli

$$\mathbf{Z}[X], \quad \mathbf{Q}[X], \quad \mathbf{R}[X], \quad \mathbf{Z}/11\mathbf{Z}[X]$$

decidere se l'ideale generato da $(X^2 - 3)$ è massimale e se è primo.

(16.M) Provare che il polinomio $X^3 + X + 1$ è irriducibile in $\mathbf{Z}/2\mathbf{Z}[X]$. Dimostrare che l'anello

$$\mathbf{Z}/2\mathbf{Z}[X]/(X^3 + X + 1)$$

è un campo. Quanti elementi ha questo campo?

(16.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.

**17. Campi.**

In questo paragrafo studiamo la teoria generale dei *campi.* Il risultato principale è il Teorema 17.9 che afferma l'esistenza, unica 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.12.4 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.

**Proposizione (17.1).** *Ogni campo primo è isomorfo a* $\mathbf{Q}$ *oppure a* $\mathbf{Z}/p\mathbf{Z}$ *per un numero primo* $p$.

**Dimostrazione.** Sia $K$ un campo. Consideriamo l'omomorfismo dell'Esempio 12.1(v):

$$\varphi : \mathbf{Z} \longrightarrow K$$

dato da $\varphi(m) = m$. Siccome ogni sottocampo di $K$ contiene l'elemento identica, deve anche contenere l'immagine di $\varphi$. Adesso ci sono due possibilità:
(1) La mappa $\varphi$ non è iniettiva. Allora c'è un intero $n \neq 0$ tale che $n\mathbf{Z}$ è il nucleo di $\varphi$. Per il primo Teorema di isomorfismo abbiamo che

$$\mathbf{Z}/n\mathbf{Z} \cong \varphi(\mathbf{Z}) \subset K.$$

Siccome $K$ è un campo, non contiene divisori di 0. Questo implica che $n$ deve essere primo. Per la Prop.11.6, l'anello $\mathbf{Z}/n\mathbf{Z}$ è un campo se $n$ è primo. Quindi esso è il campo primo di $K$.
(2) La mappa $\varphi$ è iniettiva. Definiamo

$$\Phi : \mathbf{Q} \longrightarrow K$$

per $\Phi(a/b) = \varphi(a)/\varphi(b)$ per $a, b \in \mathbf{Z}$, $b \neq 0$. Lasciamo al lettore la verifica che $\Phi$ è un omomorfismo ben definito. L'immagine di $\Phi$ è contenuta in ogni sottocampo di $K$. Siccome $\mathbf{Q}$ è un campo, $\Phi$ è iniettiva e $\Phi(\mathbf{Q})$ è un sottocampo di $K$ isomorfo a $\mathbf{Q}$. Concludiamo che questo sottocampo è il campo primo di $K$, come richiesto.

La *caratteristica* $\mathrm{car}(K)$ di un campo $K$ si dice $p$ se il campo primo di $K$ è isomorfo a $\mathbf{Z}/p\mathbf{Z}$. La caratteristica si dice 0 se il campo primo è isomorfo a $\mathbf{Q}$. Ogni campo di caratteristica $p$ ammette un omomorfismo speciale:

**Proposizione (17.2).** *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 finisce la dimostrazione.

L'omomorfismo $F$ si dice iL'*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.

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 ($V_1$), …, ($V_4$).

**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* $K$.

Per esempio, $\mathbf{e}_1 = 1$ e $\mathbf{e}_2 = i$ è una base di $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}$ come spazio vettoriale su $\mathbf{R}$. Dunque $\mathbf{C}$ è uno spazio vettoriale su $\mathbf{R}$ di dimensione 2 e $[\mathbf{C} : \mathbf{R}] = 2$.

**Proposizione (17.3).** *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 finisce la dimostrazione.

**Definizione.** Sia $K \subset L$ un'estensione di campi e sia $\alpha \in L$. Definiamo

$$K[\alpha] = \{\sum_{i}^{<\infty} a_i \alpha^i : a_i \in K\},$$

$$K(\alpha) = \text{il più piccolo sottocampo di } L \text{ che contiene sia } K \text{ che } \alpha.$$

Si noti che $K[\alpha]$ è un sottoanello di $L$. 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 $\alpha_1, \alpha_2, \ldots, \alpha_n$.

**Definizione.** Sia $K \subset L$ un'estensione di campi e sia $\alpha \in L$. L'elemento $\alpha$ 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.*

Il prossimo teorema dà varie caratterizzazioni di elementi algebrici.

**Teorema (17.4).** *sia $K$ un campo e sia $L$ un'estensione di $K$. Sia $\alpha \in L$. Allora le seguenti affermazioni sono equivalenti:*
*(i)* $K[\alpha] = K(\alpha)$.
*(ii)* $K[\alpha]$ *è un campo.*
*(iii) Esiste un polinomio irriducibile* $f \in K[X]$ *tale che* $f(\alpha) = 0$.
*(iv) Esiste un polinomio* $f \in K[X]$, $f \neq 0$ *tale che* $f(\alpha) = 0$. *(Cioè* $\alpha$ *è algebrico).*
*(v)* $[K(\alpha) : K]$ *è finito.*

**Dimostrazione.** *(i)* $\iff$ *(ii)* È banale che *(i)* implica *(ii)*. Viceversa, se $K[\alpha]$ è un campo deve essere uguale a $K(\alpha)$ perché questo è il campo più piccolo che contiene sia $K$ che $\alpha$.
*(ii)* $\iff$ *(iii)* Consideriamo l'omomorfismo

$$\Phi : K[X] \longrightarrow K[\alpha]$$

dato da $\Phi(g) = g(\alpha)$. Per definizione di $K[\alpha]$, la mappa $\Phi$ è suriettiva. Se $K[\alpha]$ è un campo, il nucleo di $\Phi$ è un ideale massimale. Siccome $K[X]$ è un anello a ideali principali abbiamo, per il Teorema 15.1, che $\ker(\Phi) = (f)$ con $f$ un polinomio irriducibile. Siccome $f(\alpha) = 0$, segue la parte *(iii)*. Viceversa, se $f \in K[X]$ è un polinomio irriducibile con $f(\alpha) = 0$, l'applicazione

$$K[X]/(f) \longrightarrow K[\alpha]$$

è ben definita. Per definizione di $K[\alpha]$ questa mappa è suriettiva e siccome $K[X]/(f)$ è un campo, è anche iniettiva. Concludiamo che $K[\alpha]$ è un campo.
*(iii)* $\iff$ *(iv)* È banale che *(iii)* implica *(iv)*. Supponiamo che $f \in K[X]$ non sia nullo e $f(\alpha) = 0$. Siccome l'anello $K[X]$ è un dominio a fattorizzazione unica, possiamo scrivere

$$f = f_1 \cdot f_2 \cdot \ldots \cdot f_t$$

dove i polinomi $f_i \in K[X]$ sono irriducibili. Siccome $0 = f(\alpha) = f_1(\alpha)f_2(\alpha)\cdot\ldots\cdot f_t(\alpha)$ nel campo $L$, abbiamo che $f_i(\alpha) = 0$ per un certo $i$, come richiesto.
*(iv)* $\iff$ *(v)* Supponiamo *(v)*: la dimensione di $K(\alpha)$ come spazio vettoriale su $K$ è $d < \infty$. Allora i $d+1$ "vettori" $1, \alpha, \alpha^2, \ldots, \alpha^d$ sono necessariamente dipendenti. Esistono dunque $\lambda_0, \lambda_1, \ldots, \lambda_d$ in $K$, non tutti nulli, tali che

$$\lambda_0 + \lambda_1\alpha + \ldots + \lambda_d\alpha^d = 0.$$

In altre parole, il polinomio

$$f = a_dX^d + \ldots + a_1X + a_0$$

non è nullo e soddisfa $f(\alpha) = 0$. Questo implica *(v)*.

Viceversa, supponiamo *(iv)*: esiste un polinomio $f \in K[X]$, $f \neq 0$ con $f(\alpha) = 0$. Sia $d = \deg(f)$. Affermiamo che ogni elemento $x \in K[\alpha]$ si può scrivere come

$$x = \lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1}$$

dove $\lambda_i \in K$ per $0 \leq i \leq d-1$. In effetti, sia $x = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_m\alpha^m \in K[\alpha]$. Sia $G \in K[X]$ il polinomio $G = a_mX^m + \ldots + a_1X + a_0$. Abbiamo $x = G(\alpha)$. Per il Teorema 13.1, possiamo dividere il polinomio $G$ per $f$ con quoziente $q$ e resto $r$ tale $r = 0$ oppure $\deg(r) < d$:

$$G = q \cdot f + r.$$

Sostituendo $\alpha$ troviamo

$$x = G(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$$

e quindi, se scriviamo $r = \lambda_{d-1}X^{d-1} + \ldots + \lambda_1X + \lambda_0$ con $\lambda_i \in K$ per $0 \leq i \leq d-1$, abbiamo

$$x = \lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1}$$

come affermato.

Sappiamo già che la parte *(iv)* implica la parte *(i)*, cioè sappiamo che $K(\alpha) = K[\alpha]$. La nostra affermazione implica dunque che per ogni $x \in K(\alpha)$ si ha

$$x = \lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1}$$

per certi $\lambda_0, \lambda_1, \ldots, \lambda_{d-1} \in K$. Questo dimostra *(v)* e finisce la dimostrazione del teorema.

**Corollario (17.5).** *Sia $K$ un campo e sia $L$ un'estensione di $K$ di grado finito, allora ogni elemento di $L$ è algebrico su $K$.*

**Dimostrazione.** Per ogni $\alpha \in L$, il campo $K(\alpha)$ è un sottocampo di $L$. Siccome $L$ ha dimensione finita come spazio vettoriale su $K$, anche $K(\alpha)$ ha dimensione finita. Dunque, il corollario segue dal Teorema 17.4.

**Corollario (17.6).** *Sia $K$ un campo e sia $L$ un'estensione di $K$. Sia $\alpha \in K$. Le seguenti affermazioni sono equivalenti:*
*(i) Non esiste un polinomio $f \in K[X]$, $f \neq 0$ tale che $f(\alpha) = 0$. (Cioè $\alpha$ è trascendente.)*
*(ii) C'è un isomorfismo di anelli $K[\alpha] \cong K[X]$.*
*(iii) La dimensione di $K(\alpha)$ è infinita.*

**Dimostrazione.** Lasciata al lettore.

**Corollario (17.7).** *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 $K$. Siccome $K(\alpha) = K(-\alpha) = K(1/\alpha)$ concludiamo che gli elementi $-\alpha$ e $1/\alpha$ sono algebrici su $K$.

Siano $\alpha, \beta \in F$. Allora $K(\alpha)$ ha grado finito su $K$. Siccome $\beta$ 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 abbiamo dunque $\alpha + \beta$, $\alpha\beta \in F$. Adesso si conclude facilmente che $F$ è un campo.

Il campo

$$\{\alpha \in \mathbf{C} : \alpha \text{ è algebrico su } \mathbf{Q}\}$$

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.

Sia $K$ un campo e sia $\alpha$ un elemento algebrico su $K$, contenuto in un'estensione $L$ di $K$. Per il Teorema 17.4 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 $\alpha$ (rispetto a $K$).* Notazione: $f^{\alpha}_{\min}$ oppure $f^{\alpha}_{\min,K}$.

**Proposizione (17.8).** *Siano $K \subset L$ campi. Sia $\alpha \in L$ un elemento algebrico su $K$. Allora*
*(i)*

$$K[X]/(f^{\alpha}_{\min}) \cong K(\alpha).$$

*(ii)* $\deg(f_{\min}) = [K(\alpha) : K]$.

**Dimostrazione.** Siccome $f_{\min}(\alpha) = 0$, l'omomorfismo

$$\Phi : K[X]/(f_{\min}) \longrightarrow K[\alpha]$$

è ben definito. Per definizione di $K[\alpha]$, la mappa $\Phi$ è suriettiva. Siccome $f_{\min}$ è irriducibile, $K[X]/(f_{\min})$ è un campo e, quindi, $\Phi$ è iniettivo. Per il Teorema 17.4, abbiamo $K[\alpha] = K(\alpha)$. Per l'Eserc.17.G la dimensione di $K[X]/(f_{\min})$ come spazio vettoriale su $K$ è uguale a $d = \deg(f_{\min})$. Adesso la dimostrazione è completa.

**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

(1) esistono $\alpha_1, \alpha_2, \ldots, \alpha_d \in L$ tali che

$$f = (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_d) \qquad \text{in } L[X],$$

(2) $L = K(\alpha_1, \alpha_2, \ldots, \alpha_d)$.

**Teorema (17.9).** *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 con 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 $\alpha = \overline{X} = X \pmod f \in F$ soddisfa $f(\alpha) = 0$ e quindi, $f$ è il polinomio minimo di $\alpha$. Per la Prop.17.8 abbiamo $K(\alpha) \subset F$.

Dividiamo $f$ per $X - \alpha$:

$$f(X) = (Y - \alpha) f_1(X)$$

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 $\tau$ ristretto a $K_1$ è $\sigma$.*

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 $\sigma$, 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 $\sigma$. Per il Teorema 17.4 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 $\sigma$.

$$\begin{array}{ccc} L_1 & & L_2 \\ \cup & & \cup \\ K_1(\alpha_1) & \xrightarrow{\sigma'} & K_2(\alpha_2) \\ \cup & & \cup \\ K_1 & \xrightarrow{\sigma} & K2 \end{array}$$

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 finisce la dimostrazione del teorema.

**Esercizi.**

(17.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 $K^\sigma$ se $K = \mathbf{C}$ e $\sigma$ è la coniugazione complessa.

(iii) Dimostrare che $\sigma(x) = x$ per ogni $x$ nel campo primo $K_0$ di $K$.

(17.B) Sia $\sigma : K \longrightarrow L$ un omomorfismo di campi. Far vedere che $\sigma$ induce un isomorfismo fra i campi primi di $K$ e $L$. Far vedere che $\mathrm{car}(K) = \mathrm{car}(L)$.

(17.C) Provare che la caratteristica di un campo finito non è 0. Far vedere che i campi finiti sono perfetti.

(17.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.

(17.E) Consideriamo $\sqrt{2} \in \mathbf{R}$ e sia $K = \mathbf{Q}(\sqrt{2})$.
(i) Far vedere che $[K : \mathbf{Q}] = 2$.
(ii) Dimostrare che ogni elemento $\alpha \in K$ è algebrico su $\mathbf{Q}$.

(17.F) Far vedere che

$$f_{\min}^{\sqrt[n]{2}} = X^n - 2$$

per ogni intero $n > 0$.

(17.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

$$\dim_K K[X]/(f) = \deg(f).$$

(17.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 $\beta$ soddisfa $\beta^3 + 3\beta - 3$.

(17.I) Consideriamo $\sqrt{2}, \sqrt{7} \in \mathbf{R}$.
(i) Far vedere che $\mathbf{Q}(\sqrt{2}, \sqrt{7}) = \mathbf{Q}(\sqrt{2} + \sqrt{7})$.
(ii) Calcolare $f_{\min}^{\sqrt{2}+\sqrt{7}}$.
(iii) Dimostrare che $[\mathbf{Q}(\sqrt{2}, \sqrt{7}) : \mathbf{Q}] = 4$.

(17.J) Sia $\alpha \in \mathbf{R}$ con $\alpha^3 - \alpha - 1 = 0$. Scrivere i seguenti elementi nella forma $a + b\alpha + c\alpha^2$ dove $a, b, c \in \mathbf{Q}$:

$$\alpha^{10}, \quad (\alpha^2 + \alpha + 1)^2, \quad (\alpha^2 + 1)^{-1}.$$

(17.K) Sia $K$ un campo e supponiamo che $\alpha$ e $\beta$ 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 $\alpha$ a $\beta$.

(17.M) Sia $K$ un campo e siano $\alpha, \beta$ elementi algebrici su $K$. Dimostrare

$$[K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K].$$

(17.N) (i) Far vedere che non esistono $a, b \in \mathbf{Q}$ tali che $(a + b\sqrt{2})^2 = 3$.
(ii) Dimostrare che il polinomio $X^2 - 3$ è irriducibile nell'anello $\mathbf{Q}(\sqrt{2})[X]$.
(iii) Provare

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4.$$

(17.O) Sia $L$ un'estensiona finita del campo $K$ e sia $\alpha \in L$. Dimostrare che $\deg(f_{\min}^{\alpha})$ è un divisore di $[L : K]$.

(17.P) Sia $K$ un campo e sia $f \in K[X]$ un polinomio irriducubile. Sia $\alpha$ uno zero di $f$ contenuto in un'estensione di $K$. Dimostrare che se $g \in K[X]$ soddisfa $g(\alpha) = 0$, allora $f$ divide $g$. (Sugg. Appplicare il Teorema 13.1).

(17.Q) Sia $K$ un campo e sia $\alpha$ un elemento algebrico su $K$. Supponiamo che $[K(\alpha) : K]$ sia *dispari.* Far vedere che $K(\alpha^2) = K(\alpha)$.

(17.R) 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

$$[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K].$$

(17.S) Sia $K$ un campo e sia $\alpha$ un elemento trascendente su $K$. Sia $\beta \in K(\alpha)$, $\beta \notin K$.
  (i) Mostrare che $\alpha$ 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 $\beta$ è trascendente su $K$.

(17.T) 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 $L = K(\alpha_1, \ldots, \alpha_{n-1})$.

(17.U) 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 $n!$.

(17.V) Sia $\zeta$ una radice primitiva di ordine 3, cioè $\zeta^2 + \zeta + 1 = 0$. Dimostrare che il campo $\mathbf{Q}(\sqrt[3]{2}, \zeta)$ è il campo di spezzamento di $X^3 - 2$ su $\mathbf{Q}$.

(17.W) Sia $i$ una radice primitiva di ordine 4, cioè $i^2 + 1 = 0$. Far vedere che il campo $\mathbf{Q}(\sqrt[4]{2}, i)$ è il campo di spezzamento di $X^4 - 2$ su $\mathbf{Q}$.

(17.X) Sia $\zeta$ uno zero del polinomio $f = X^4 + X^3 + X^2 + X + 1$.
  (i) Far vedere che $\zeta^5 = 1$.
  (ii) Far vedere che $\zeta^2$, $\zeta^3$ e $\zeta^4$ sono gli altri zeri di $f$.
  (iii) Dimostrare che $\mathbf{Q}(\zeta)$ è un campo di spezzamento di $f$.

## 18. Campi finiti.

Un campo $K$ si dice *finito* se il numero degli elementi di $K$ è finito. In questo paragrafo studiamo la teoria dei *campi finiti.* I campi finiti sono stati studiati per la prima volta dal matematico francese Évariste Galois (1811-1832).

**Proposizione (18.1).** *Sia $K$ un campo finito di ordine $q$. Allora*

$$\alpha^q = \alpha \qquad \text{per ogni } \alpha \in K.$$

**Dimostrazione.** La cardinalità del gruppo moltiplicativo $K^*$ è $q - 1$. Quindi, per il Cor.4.7 si ha che $\alpha^{q-1} = 1$ per ogni $\alpha \in K^*$. Moltiplicando per $\alpha$, si trova il risultato.

**Teorema (18.2).** *Sia $K$ un campo finito. Allora*
*(i) La cardinalità di $K$ è $q = p^n$ dove $p$ è un numero primo.*
*(ii) Per ogni potenza di un primo $q$ esiste un campo finito di $q$ elementi. Questo campo è unico a meno di isomorfismi.*

**Dimostrazione.** *(i)* Sia $K$ un campo finito e sia $K_0$ il suo campo primo. Per la Prop.17.1 ed il fatto che $K$ è finito, abbiamo

$$K_0 \cong \mathbf{Z}/p\mathbf{Z}$$

per un certo numero primo $p$. Siccome $K$, essendo un'estensione di $K_0$ è uno spazio vettoriale su $\mathbf{Z}/p\mathbf{Z}$, abbiamo che $\#K = p^f$ per un certo intero $f \geq 1$.
*(ii)* Sia $q = p^f$ una potenza di un numero primo $p$. Per il Teorema 17.7 esiste un'estensione $K$ di $\mathbf{Z}/p\mathbf{Z}$ che è un campo di spezzamento del polinomio $X^q - X \in \mathbf{Z}/p\mathbf{Z}[X]$. Consideriamo il sottoinsieme

$$F = \{x \in K : x^q = x\}.$$

Siano $x, y \in F$. Per l'Eserc.17.D, l'insieme $F$ è un *sottocampo* di $K$. Gli elementi di $F$ sono esattamente gli zeri del polinomio $X^q - X$. Siccome $K$ è un campo di spezzamento di $X^q - X$ deve essere $F = K$.

Il polinomio derivato è uguale a $qX^{q-1} - 1 = -1$ e non ha zeri. Quindi, per la Prop.13.13, il polinomio $X^q - X$ non ha zeri doppi. Questo implica che la cardinalità di $K = F$ è uguale a $q$. Questo dimostra l'esistenza di un campo con $q$ elementi.

L'unicità, a meno di isomorfismi, segue dal fatto che ogni campo con $q$ elementi è un campo di spezzamento del polinomio $X^q - X$ su $\mathbf{F}_p$ e dal Teorema 17.9.

Per una potenza $q$ di un primo $p$, si scrive $\mathbf{F}_q$ per un campo finito di cardinalità $q$. Dunque $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ per primi $p$.

**Esempio.** (i) Costruiamo un campo con 4 elementi. L'unico polinomio irriducibile di grado 2 in $\mathbf{F}_2[X]$ è $X^2 + X + 1$. Sia

$$\mathbf{F}_4 = \mathbf{F}_2[X]/(X^2 + X + 1).$$

Scriviamo $\zeta$ per uno zero di $X^2 + X + 1$ in $\mathbf{F}_4$. Allora $\mathbf{F}_4 = \mathbf{F}_2(\zeta)$ dove $\zeta^2 + \zeta + 1 = 0$. I quattro elementi di $\mathbf{F}_4$ sono 0, 1, $\zeta$ e $\zeta + 1$. Si calcola in $\mathbf{F}_4$ con polinomi in $\zeta$ modulo 2 e modulo la relazione $\zeta^2 + \zeta + 1 = 0$. Per esempio $\zeta(\zeta + 1) = \zeta^2 + \zeta = -1 = 1$. Ecco le tavole di addizione e moltplicazione di $\mathbf{F}_4$:

| | 0 | 1 | $\zeta$ | $\zeta^2$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $\zeta$ | $\zeta^2$ |
| 1 | 1 | 0 | $\zeta^2$ | $\zeta$ |
| $\zeta$ | $\zeta$ | $\zeta^2$ | 0 | 1 |
| $\zeta^2$ | $\zeta^2$ | $\zeta$ | 1 | 0 |

| | 1 | $\zeta$ | $\zeta^2$ |
|---|---|---|---|
| 1 | 1 | $\zeta$ | $\zeta^2$ |
| $\zeta$ | $\zeta$ | $\zeta^2$ | 1 |
| $\zeta^2$ | $\zeta^2$ | 1 | $\zeta$ |

Si noti che $\zeta^2 = \zeta + 1$.
(ii) Costruzione del campo $\mathbf{F}_{81}$: consideriamo il polinomio $X^4 + X - 1 \in \mathbf{F}_3$. Si veda l'Eserc.18.K per una dimostrazione dell'irriducibilità del polinomio. Quindi, l'anello

$$\mathbf{F}_3[X]/(X^4 + X - 1)$$

è un campo. Siccome $X^4 + X + 1$ ha grado 4, il campo ha dimensione 4 su $\mathbf{F}_3$ e ha dunque $3^4 = 81$ elementi.

Esistono molti polinomi irriducibili $f$ di grado 4 in $\mathbf{F}_3[X]$ (si veda l'Eserc.18.K). Per ogni tale $f$, l'anello $\mathbf{F}_3[X]/(f)$ è un campo con 81 elementi. Per il Teorema 18.2 tutti questi campi sono isomorfi.

Studiamo adesso un po' la ricca struttura dei campi finiti. Osserviamo prima una generalizzazione del Teorema 13.7:

**Corollario (18.3).** *Sia $q$ una potenza di un numero primo $p$. Allora*

$$X^q - X = \prod_{\alpha \in \mathbf{F}_q} (X - \alpha) \qquad \textit{nell'anello } \mathbf{F}_q[X].$$

**Dimostrazione.** Questo segue dal fatto, notato nella dimostrazione del Teorema 18.2, che $\mathbf{F}_q$ è un campo di spezzamento del polinomio $X^q - X \in \mathbf{F}_p[X]$.

**Teorema (18.4).** *Sia $q$ una potenza di un numero primo $p$. Allora*
*(i) Il gruppo moltiplicativo $\mathbf{F}_q^*$ è ciclico di ordine $q - 1$.*
*(ii) Si ha*

$$\mathbf{F}_q \cong \mathbf{F}_p[X]/(f)$$

*dove $f \in \mathbf{F}_p[X]$ è un polinomio irriducibile. In altre parole, $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ dove $\alpha$ è un zero di un polinomio irriducibile $f \in \mathbf{F}_p[X]$.*

**Dimostrazione.** *(i)* Siccome $\mathbf{F}_q$ è un campo il gruppo moltiplicativo $\mathbf{F}_q^*$ è finito di ordine $q-1$. Per il Teorema 13.9 è dunque ciclico.
*(ii)* Sia $\alpha \in \mathbf{F}_q^*$ un elemento di ordine $q-1$. Sia $f$ il suo polinomio minimo su $\mathbf{F}_p$. Dunque,

$$\mathbf{F}_p[X]/(f) \cong \mathbf{F}_p(\alpha) \subset \mathbf{F}_q.$$

Siccome $\alpha \in \mathbf{F}_p(\alpha)^*$, l'ordine di $\mathbf{F}_p(\alpha)^*$ è almeno $q-1$. Questo implica che $\mathbf{F}_p(\alpha) = \mathbf{F}_q$ e quindi $\mathbf{F}_p[X]/(f) \cong \mathbf{F}_q$ come richiesto.

Si noti, in particolare, che per ogni primo $p$ ed ogni grado $n$ esiste un polinomio irriducibile in $\mathbf{F}_p[X]$ di grado $n$. Questa osservazione si può precisare.

**Teorema (18.5).** *Sia $p$ un numero primo e sia $q = p^f$ una potenza di $p$.*
*(i) Se $K$ e $L$ sono due sottocampi di $\mathbf{F}_q$ di ordine $p^a$ e $p^b$ rispettivamente, allora*

$$K \subset L \quad \Longleftrightarrow \quad a \text{ divide } b.$$

*(ii) Sia $n$ un intero positivo. Allora*

$$X^{q^n} - X = \prod_f f \qquad \text{in } \mathbf{F}_q[X].$$

*dove $f$ varia fra i polinomi monici* e *irriducibili* $f \in \mathbf{F}_q[X]$ con $\deg(f)$ che divide $n$.

**Dimostrazione.** *(i)* Supponiamo che $K \subset L$, allora $L$ è uno spazio vettoriale su $K$ e quindi $\#L = (\#K)^d$ dove $d = [L:K]$. Questo implica che $p^b = p^{ad}$ e dunque che $a$ divida $b$.

Supponiamo che $a$ divide $b$. Sia $\alpha \in K$. Per la Prop.18.1 abbiamo $\alpha^{p^a} = \alpha$ e questo implica che $\alpha^{p^{ak}} = \alpha$ per ogni $k \in \mathbf{Z}_{\geq 0}$. In particolare $\alpha^{p^b} = \alpha$. Per la Prop.18.1, il sottocampo $L$ contiene i $q$ zeri del polinomio $X^{p^b} - X$ in $\mathbf{F}_q$. Dunque $\alpha \in L$ come richiesto.
*(ii)* Siccome l'anello $\mathbf{F}_q[X]$ è un dominio a fattorizzazione unica, il polinomio $X^{q^n} - X$ è, in modo unico, un prodotto di polinomi irriducibili $f \in \mathbf{F}_q[X]$. Il polinomio derivato $q^n X^{q^n-1} - 1 = -1$ non ha zeri e quindi, per la Prop.13.13, il polinomio $X^{q^n} - X$ non ha zeri doppi. Basta dunque dimostrare che per polinomi monici e irriducibili in $\mathbf{F}_q[X]$.

$$f \text{ divide } X^{q^n} - X \quad \Longleftrightarrow \quad \deg(f) \text{ divide } n.$$

Sia $\mathbf{F}_{q^n}$ una estensione di $\mathbf{F}_q$ di $q^n$ elementi. Sia $f$ un polinomio irriducibile e monico di grado $d$ in $\mathbf{F}_q[X]$ e sia $\alpha$ uno zero di $f$ in un campo di spezzamento $L$ di $f$ *rispetto al campo* $\mathbf{F}_{q^n}$. Siccome $f$ è monico, abbiamo $f = f^{\alpha}_{\min}$ e, per la Prop.17.8*(i)* abbiamo $d = [\mathbf{F}_q(\alpha) : \mathbf{F}_q]$. Quindi $\mathbf{F}(\alpha) \cong \mathbf{F}_{q^d}$. Per il Teorema 18.5*(i)* abbiamo adesso

$$\begin{aligned} d \text{ divide } n &\Longleftrightarrow \mathbf{F}_q(\alpha) \subset \mathbf{F}_{q^n} \\ &\Longleftrightarrow \alpha \in \mathbf{F}_{q^n} \\ &\Longleftrightarrow \alpha \text{ è uno zero di } X^{q^n} - X \\ &\Longleftrightarrow f \text{ divide } X^{q^n} - X \end{aligned}$$

Per l'ultima equivalenza si veda l'Eserc.17.P.

**Corollario (18.6).** *Sia $q$ una potenza di un primo $p$. Per ogni $d \in \mathbf{Z}_{>1}$, sia $x_d$ il numero di polinomi irriducibili di grado $d$ in $\mathbf{F}_q[X]$. Allora per ogni intero $n > 0$:*

$$\sum_{\substack{d|n \\ d>0}} d x_d = q^n$$

**Dimostrazione.** Questo segue dal Teorema, considerando i gradi dei polinomi.

**Teorema (18.7).** *Sia $q = p^n$ una potenza di un numero primo $p$. Allora l'insieme* $\mathrm{Aut}(\mathbf{F}_q)$ *degli automorfismi di $\mathbf{F}_q$ è un gruppo ciclico generato dall'omomorfismo di Frobenius $F$. Abbiamo*

$$\mathrm{Aut}(\mathbf{F}_q) \cong \mathbf{Z}/n\mathbf{Z}.$$

**Dimostrazione.** Lasciamo al lettore la dimostrazione del fatto che l'insieme degli automorfismi di $\mathbf{F}_q$ è, con la composizione, un gruppo. L'omomorfismo di Frobenius $F$ dato da

$$F(\alpha) = \alpha^p \qquad \alpha \in \mathbf{F}_q, .$$

Per la Prop.18.1 si ha $F^n = \mathrm{id}$. Se $F^i = \mathrm{id}$, allora ogni elemento di $\mathbf{F}_q$ è uno zero del polinomio $X^{q^i} - X$. Quindi $n \geq i$.

Dunque, $F$ è un automorfismo di ordine $n$. Per finire la dimostrazione, basta far vedere che $\#\mathrm{Aut}(\mathbf{F}_q) \leq n$.

Per il Teorema 18.4 abbiamo $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ per un certo $\alpha \in \mathbf{F}_q$. Per la Prop.17.8 il polinomio minimo $f$ di $\alpha$ ha dunque grado $n$:

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

dove $a_i \in \mathbf{F}_p$. Sia $\sigma \in \mathrm{Aut}(\mathbf{F}_q)$. Per l'Eserc.17.A, l'automorfismo $\sigma$ ristretto al campo primo $\mathbf{F}_p$ è la mappa identica. Abbiamo

$$\begin{aligned} 0 = \sigma(0) &= \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0) \\ &= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \ldots + a_1\sigma(\alpha) + a_0 \\ &= f(\sigma(\alpha)). \end{aligned}$$

Quindi, per ogni $\sigma \in \mathrm{Aut}(\mathbf{F}_q)$ l'elemento $\sigma(\alpha)$ è uno zero di $f$. Siccome $f$ ha al più $n$ zeri, ci sono al più $n$ possibilità per $\sigma(\alpha)$. Ma $\sigma$ è completamente determinato da $\sigma(\alpha)$ perché

$$\mathbf{F}_q = \mathbf{F}_p(\alpha) = \mathbf{F}_p[\alpha].$$

Concludiamo che $\#\mathrm{Aut}(\mathbf{F}_q) \leq n$ come richiesto.

**Teorema (18.8).** *Sia $q$ una potenza di un numero primo e sia $f \in \mathbf{F}_q[X]$ un polinomio monico e irriducibile. Sia $\alpha$ uno zero di $f$ in un'estensione di $\mathbf{F}_q$. Allora*

$$f = \prod_{i=0}^{n-1} (X - \alpha^{q^i}) \qquad \text{in } \mathbf{F}_q(\alpha)[X],$$

*dove $n = \deg(f)$.*

**Dimostrazione.** Sia

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \qquad a_i \in \mathbf{F}_q$$

La mappa $x \mapsto x^q$ è un automorfismo del campo $\mathbf{F}_q(\alpha)$. Per il Teorema 18.1 abbiamo $a_i^q = a_i$ per ogni $i$ e quindi

$$\begin{aligned} 0 &= \left(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0\right)^q \\ &= \alpha^{qn} + a_{n-1}\alpha^{q(n-1)} + \ldots + a_1\alpha^q + a_0 \\ &= f(\alpha^q). \end{aligned}$$

Dunque, $\alpha^q$ è uno zero di $f$. Similmente, ogni elemento $\alpha^{q^i}$, $i \in \mathbf{Z}\geq 0$ è uno zero di $f$.

Per finire la dimostrazione, vediamo che gli zeri $\alpha^{q^i}$, $0 \leq i \leq n-1$ sono tutti distinti: siccome $[\mathbf{F}_q(\alpha) : \mathbf{F}_q] = n$ abbiamo per la Prop 18.1 che $\alpha^{q^n} = \alpha$. Se fosse $\alpha^{q^i} = \alpha^{q^j}$ allora

$$\alpha^{q^{n+i-j}} = \left(\alpha^{q^i}\right)^{q^{n-j}} = \left(\alpha^{q^j}\right)^{q^{n-j}} = \alpha^{q^n} = \alpha.$$

Questo implica che $\alpha \in \mathbf{F}_{q^{n+i-j}}$. Per l'Eserc.17.O abbiamo dunque che $n$ divide $n+i-j$. Siccome $0 \leq i, j \leq n-1$ concludiamo che $i = j$, come richiesto.

**Esercizi.**

(18.A) Sia $q$ una potenza di un primo $p$. Sia $V$ uno spazio vettoriale su $\mathbf{F}_q$. Far vedere che $\#V = q^d$ dove $d = \dim_{\mathbf{F}_q}(V)$.

(18.B) Esistono campi con 43, 143, 243 e 343 elementi?

(18.C) Sia $F$ un campo e supponiamo che $K$ e $L$ siano due sottocampi finiti di $F$ con la stessa cardinalità. Far vedere che $K = L$ (e non soltanto $K \cong L$).

(18.D) Sia $\varphi$ la funzione di Eulero. Mostrare che ogni campo finito $\mathbf{F}_q$ ha $\varphi(q-1)$ elementi di ordine moltiplicativo $q-1$.

(18.E) Determinare $f^{\alpha}_{\min}$ per ogni $\alpha \in \mathbf{F}_9$. Fattorizare il polinomio $X^8 - 1$ in $\mathbf{F}_3[X]$.

(18.F) Dimostrare che il polinomio $X^4 + 2$ è irriducibile in $\mathbf{F}_5[X]$.

(18.G) (i) Far vedere che $\mathbf{F}_{25}$ contiene un elemento $\alpha$ con $\alpha^2 = 2$.
(ii) Dimostrare che l'elemento $2 + \alpha \in \mathbf{F}_{25}$ è una radice primitiva di $\mathbf{F}_{25}$, cioè l'ordine moltiplicativo di $2 + \alpha$ è $25 - 1 = 24$.

(18.H) Fattorizare i polinomi $X^2 - X$, $X^4 - X$, $X^8 - X$ e $X^{64} - X$ in $\mathbf{F}_2[X]$.

(18.I) (i) Far vedere che per $\alpha \in \mathbf{F}_9^*$ si ha $\alpha^4 = \pm 1$.
(ii) Far vedere che il polinomio $X^4 + X - 1$ è irriducibile in $\mathbf{F}_3[X]$.
(iii) Dimostrare che ci sono esattamente 18 polinomi irriducibili e monici di grado 4 in $\mathbf{F}_3[X]$.

(18.J) Dimostrare che il polinomio $g = X^3 + X - 1 \in \mathbf{F}_5[X]$ è irriducibile. Far vedere che l'ordine moltiplicativo di uno zero $\alpha$ di $g$ in un'estensione di $\mathbf{F}_5$ è uguale a 31.

(18.K) Sia $\mathbf{F}_q$ un campo finito di caratteristica $p$. Sia $n$ un intero positivo non divisibile per $p$.
(i) Dimostrare che il campo di spezzamento di $X^n - 1$ su $\mathbf{F}_q$ è un campo con $q^f$ elementi dove $f$ è l'ordine di $q$ nel gruppo $(\mathbf{Z}/n\mathbf{Z})^*$.
(ii) Fattorizzare il polinomio $X^{20} - 1 \in \mathbf{F}_3[X]$ in fattori irriducibili

(18.L) Sia $\mathbf{F}_q$ un campo finito e sia $x_n$ il numero di polinomi irriducibili e monici in $\mathbf{F}_q[X]$ di grado $n$. Dimostrare che

$$\begin{aligned} x_1 &= q, \\ x_2 &= \frac{1}{2}(q^2 - q), \\ x_3 &= \frac{1}{3}(q^3 - q), \\ x_6 &= \frac{1}{6}(q^6 - q^3 - q^2 + q). \end{aligned}$$

(18.M) (*Polinomi di Artin-Schreier.*) Sia $K$ un campo di caratteristica $p > 0$. Sia $a \in K$ e sia

$$f = X^p - X - a \qquad \text{in } K[X].$$

Sia $\alpha$ uno zero di $f$ in un'estensione di $K$.
(i) Far vedere che

$$X^p - X - a = \prod_{i \in \mathbf{F}_p} (X - \alpha - i)$$

e che $K(\alpha)$ è un campo di spezzamento di $f$.

(ii) Dimostrare che $f$ è o irriducibile in $K[X]$ o uguale a un prodotto di fattori di grado 1. (Sugg. Far vedere che i fattori irriducibili di $f$ hanno lo stesso grado.)

(iii) Far vedere che $X^p - X - a$ è irriducibile in $\mathbf{F}_p[X]$ per ogni $a \in \mathbf{F}_p$.

(18.N) Sia $p > 2$ un primo e sia $\zeta$ un elemento in un'estensione di $\mathbf{F}_p$ con $\zeta^4 + 1 = 0$.

(i) Mostrare che l'ordine moltiplicativo di $\zeta$ è 8.

(ii) Far vedere che l'elemento $\zeta + \zeta^{-1}$ ha il quadrato uguale a 2.

(iii) Far vedere che $\zeta + \zeta^{-1} \in \mathbf{F}_p$ se e soltanto se $p \equiv \pm 1 \pmod 8$. (Sugg. Calcolare $(\zeta + \zeta^{-1})^p$.)

(iv) Dimostrare che 2 è un quadrato modulo $p$ se e soltanto se $p \equiv \pm 1 \pmod 8$.

(v) Dimostrare che $p = a^2 - 2b^2$ per certi interi $a, b$ se e soltanto se $p \equiv \pm 1 \pmod 8$. (Sugg. l'anello $\mathbf{Z}[\sqrt{2}]$ è un anello Euclideo.)

(18.O) Sia $p > 2$ un primo e sia $\zeta$ come nell'Eserc.18.N.

(i) Far vedere che l'elemento $\zeta - \zeta^{-1}$ ha il quadrato uguale a $-2$.

(ii) Far vedere che $\zeta - \zeta^{-1} \in \mathbf{F}_p$ se e soltanto se $p \equiv 1 \pmod 8$ o $p \equiv 3 \pmod 8$. (Sugg. Calcolare $(\zeta - \zeta^{-1})^p$.)

(iii) Dimostrare che $-2$ è un quadrato modulo $p$ se e soltanto se $p \equiv 1, 3 \pmod 8$.

(iv) Dimostrare che $p = a^2 + 2b^2$ per certi interi $a, b$ se e soltanto se $p \equiv 1, 3 \pmod 8$.

(18.P)*Sia $\mu : \mathbf{Z}_{>0} \longrightarrow \{-1, 0, +1\}$ la funzione di Möbius:

$$\mu(n) = \begin{cases} 0 & \text{se esiste un numero primo } p \text{ tale che } p^2 \text{ divide } n, \\ (-1)^r & \text{se } n \text{ è un prodotti di } r \text{ primi distinti.} \end{cases}$$

La funzione di Möbius è *una funzione aritmetica* molto importante. Si veda l'Eserc.11.X per la definizione dell'anello $R$ delle funzioni aritmetiche.

(i) Sia $E$ la funzione dell'Eserc.11.X. Far vedere che $\mu \star E = e$.

(ii) Sia $f \in R$ e sia $g = f \star E$. Dimostrare che

$$g(n) = \sum_{\substack{d|n \\ d>0}} f(d), \qquad n \in \mathbf{Z}_{>0}.$$

(iii) Far vedere che $f = \mu \star g$. In altre parole

$$f(n) = \sum_{\substack{d|n \\ d>0}} \mu(d) g(\frac{n}{d}), \qquad n \in \mathbf{Z}_{>0}.$$

(Formula di inversione di Möbius)

(iv) Sia $\mathbf{F}_q$ un campo finito e sia $x_n$ il numero di polinomi irriducibili e monici in $\mathbf{F}_q[X]$ di grado $n$. Dimostrare

$$x_n = \frac{1}{n} \sum_{\substack{d|n \\ d>0}} \mu(d) q^{n/d}, \qquad n \in \mathbf{Z}_{>0}.$$

(18.Q) Sia $\mathbf{F}_q$ un campo finito e sia $x_n$ il numero di polinomi irriducibili e monici in $\mathbf{F}_q[X]$ di grado $n$. Dimostrare che

$$\frac{1}{n} q^n \geq x_n \geq \frac{1}{n} \left( q^n - \frac{q}{q-1} q^{n/2} \right)$$

(18.R)*Sia $\mathbf{F}_q$ un campo finito e sia $x_n$ il numero di polinomi irriducibili e monici in $\mathbf{F}_q[X]$ di grado $n$.

(i) Dimostrare che

$$\sum_{\substack{g \in \mathbf{F}_q[X] \\ \text{monico}}} T^{\deg(g)} = \prod_{\substack{f \in \mathbf{F}_q[X] \\ \text{monico \& irr.}}} \left( 1 + T^{\deg(f)} + T^{2\deg(f)} + T^{3\deg(f)} + \ldots \right)$$

(Sugg. Utilizzare il fatto che $\mathbf{F}_2[X]$ è un dominio a fattorizzazione unica.)

(ii) Concludere che

$$\prod_{n=1}^{\infty} \left( \frac{1}{1 - T^n} \right)^{x_n} = \frac{1}{1 - qT}.$$

## 19. Il campo dei numeri complessi.

**Definizione.** Un campo $K$ si dice *algebricamente chiuso* se per ogni polinomio non nullo $f \in K[X]$ esiste $c \in K^*$ e esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ tali che

$$f(X) = c(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).$$

In questo paragrafo dimostriamo che il campo $\mathbf{C}$ 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.*

**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 $\sigma \in S_n$.

Per esempio, i polinomi

$$\begin{aligned} X_1 + X_2 + \ldots + X_n, \\ X_1 \cdot X_2 \cdot \ldots \cdot X_n, \\ X_1^k + X_2^k + \ldots + X_n^k, \qquad & \text{per } k \in \mathbf{Z}_{\geq 0} \\ X_1 + X_2 + \ldots + X_n + X_1^2 + X_2^2 + \ldots + X_n^2 \end{aligned}$$

sono simmetrici.

**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

$$g(Z) = Z^n - \sigma_1 Z^{n-1} + \sigma_2 Z^{n-2} - \ldots + (-1)^{n-1}\sigma_{n-1} + (-1)^n \sigma_n$$

dove i polinomi $\sigma_i \in R[X_1, X_2, \ldots, X_n]$ sono i cosiddetti *polinomi simmetrici elementari:*

$$\begin{aligned} \sigma_1 &= X_1 + X_2 + \ldots + X_n, \\ \sigma_2 &= X_1X_2 + X_1 + X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_{n-1}X_n, \\ &= \sum_{1 \leq i < j \leq n} X_iX_j, \\ \sigma_3 &= \sum_{1 \leq i < j < k \leq n} X_iX_jX_k, \\ &\vdots \\ \sigma_n &= X_1X_2 \cdot \ldots \cdot X_n. \end{aligned}$$

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 $n = 2$:

$$\begin{aligned} \sigma_1^2 &= X_1^2 + 2X_1X_2 + X_2^2, \\ \sigma_2 - 2\sigma_2 &= X_1^2 + X_2^2, \\ \sigma_1^3 - 3\sigma_1\sigma_2 &= X_1^3 + X_2^3. \end{aligned}$$

Anche il viceversa vale:

**Teorema (19.1).** *(Teorema principale dei polinomi simmetrici.) Sia $R$ un anello commutativo e sia $n$ un intero positivo. Ogni polinomio simmetrico $f(X_1, X_2, \ldots, X_n) \in R[X_1, X_2, \ldots, X_n]$ si può scrivere come polinomio nei polinomi simmetrici $\sigma_1, \sigma_2, \ldots, \sigma_n$ in modo unico.*

**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 $c_1 \geq c_2 \geq \ldots \geq c_n$. Perché se non fosse così, si potrebbero scambiare due variabili e ottenere un termine che dovrebbe occorrere prima in $f$.

Siccome

$$\begin{aligned}
&\sigma_1 \text{ ha primo termine } X_1,\\
&\sigma_2 \text{ ha primo termine } X_1X_2,\\
&\quad\vdots\\
&\sigma_n \text{ ha primo termine } X_1X_2 \cdot \ldots \cdot X_n,
\end{aligned}$$

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* $\text{totdeg}(f)$ 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, $\text{totdeg}(\sigma_i) = i$ 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 $\text{totdeg}(f) \leq c_1 + c_2 + \ldots + c_n$, abbiamo

$$\text{totdeg}(f_1) \leq \text{totdeg}(f).$$

Allora, nella procedura sopra abbiamo che

$$\text{totdeg}(f) \geq \text{totdeg}(f_1) \geq \text{totdeg}(f_2) \geq \dots$$

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 bisogna dell'unicità del modo di scrivere un polinomio simmetrico come polinomio nei polinomi simmetrici elementari. Per la dimostrazione dell'unicità si veda l'Eserc.19.E.

Questo finisce la dimostrazione del Teorema.

**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

$$\begin{aligned}\sigma_1^{c_1-c_2}\sigma_2^{c_2-c_3}\sigma_3^{c_3} &= \sigma_1^2\sigma_2\\ &= (X_1+X_2+X_3)(X_1X_2+X_2X_3+X_2X_3)\end{aligned}$$

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

$$f = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3.$$

**Corollario (19.2).** *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 $f \in K[X_1, X_2, \dots, X_n]$ si ha che*

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) \in K.$$

**Dimostrazione.** Siano $\sigma_1, \sigma_2, \dots, \sigma_n$ i polinomi simmetrici elementari negli zeri $\alpha_1, \alpha_2, \dots, \alpha_n$. Allora, siccome i coefficienti di $h$ stanno in $K$ abbiamo che $\sigma_i \in K$ per $1 \leq i \leq n$. Per il Teorema 19.1 ogni polinomio simmetrico $f \in K[X_1, X_2, \dots, X_n]$ è un'espressione polinomiale con coefficienti in $K$ di polinomi simmetrici elementari. Quindi $f(\alpha_1, \alpha_2, \dots, \alpha_n) \in K$ come richiesto.

Adesso dimostriamo un caso speciale del risultato principale di questo paragrafo:

**Lemma (19.3).** *Ogni polinomio $f \in \mathbf{C}[X]$ di grado due ha gli zeri in $\mathbf{C}$.*

**Dimostrazione.** Dimostriamo prima che per ogni $z \in \mathbf{C}$ anche $\sqrt{z} \in \mathbf{C}$, cioè esiste $w \in \mathbf{C}$ tale che $w^2 = z$. Sia $z = x + yi$ dove $x, y \in \mathbf{R}$. 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 $\alpha$ di $f$:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Nel passato il prossimo teorema si chiamava *Il Teorema Fondamentale dell'Algebra.* Oggigiorno, non si riguarda 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.

**Teorema (19.4).** *(Teorema Fondamentale dell'Algebra) Sia $g \in \mathbf{C}[X]$ un polinomio non nullo. Allora*

$$g(X) = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$$

*dove $c \in \mathbf{C}^*$ e $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbf{C}$.*

**Dimostrazione.** Sia $g \in \mathbf{C}[X]$ un polinomio, $g \notin \mathbf{C}$. Se $\alpha \in \mathbf{C}$ è uno zero di $g$, allora, per la Prop.13.3, si ha $g = (X - \alpha) \cdot g_1$ dove $g_1 \in \mathbf{C}[X]$. Dunque, per induzione rispetto al grado di $g$, basta dimostrare che ogni polinomio non costante in $\mathbf{C}[X]$ ha uno zero in $\mathbf{C}$.

Affermiamo che basta dimostrare che ogni polinomio non costante con coefficienti in $\mathbf{R}$ ha uno zero in $\mathbf{C}$: sia

$$g = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \ \in \mathbf{C}[X]$$

un polinomio non nullo e sia

$$\overline{g} = \overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} + \dots + \overline{a_1} X + \overline{a_0} \ \in \mathbf{C}[X]$$

il polinomio coniugato. Per l'Eserc.19.F il prodotto $G = g\overline{g}$ è un polinomio con coefficienti in $\mathbf{R}$. Se $G(\alpha) = 0$ per un certo $\alpha \in \mathbf{C}$, 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 $\mathbf{C}$.

Sia dunque $G \in \mathbf{R}[X]$ un polinomio non nullo. Senza perdere la generalità assumiamo che $G$ sia monico. Sia $n = \deg(G)$ e sia $k \in \mathbf{Z}_{\geq 0}$ tale che $2^k$ è la più grande potenza di 2 che divide $n$. Dimostreremo con induzione rispetto a $k$ che $G$ ha uno zero in $\mathbf{C}$.

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 $\mathbf{R} \longrightarrow \mathbf{R}$ data da $x \mapsto G(x)$ è continua per la topologia usuale di $\mathbf{R}$. Quindi, per il Teorema "del valor medio" in analisi, $G$ ha uno zero in $\mathbf{R}$ e quindi anche in $\mathbf{C}$.

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 $\mathbf{C}$. Definiamo, per ogni $t \in \mathbf{R}$ il polinomio

$$H_t(X) = \prod_{1 \le i < j \le n} (X - (\alpha_i + \alpha_j + t\alpha_i\alpha_j))$$

Il grado di $H_t$ è $\binom{n}{2} = n(n-1)/2$. I coefficienti di $H_t$ sono espressioni simmetriche negli zeri $\alpha_i$ con coefficienti in $\mathbf{R}$. Per il Cor.19.2, i coefficienti di $H_t$ sono in $\mathbf{R}$.

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 $\mathbf{C}$. Quindi, per ogni $t \in \mathbf{R}$ ci sono $i, j \in \{1, 2, \ldots, n\}$, tali che

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbf{C}.$$

Siccome i numeri reali sono infiniti, ma ci sono soltanto un numero finito di sottoinsiemi $\{i, j\}$ di $\{1, 2, \ldots, n\}$ ci devono esistere $t, t' \in \mathbf{R}$ con $t \neq t'$ e con

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbf{C}$$
$$\alpha_i + \alpha_j + t'\alpha_i\alpha_j \in \mathbf{C}$$

Questo implica facilmente che sia $\alpha_i + \alpha_j$ che $\alpha_i\alpha_j$ sono in $\mathbf{C}$. Quindi, il polinomio

$$X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j = (X - \alpha_i)(X - \alpha_j)$$

è in $\mathbf{C}[X]$. Per il Lemma 19.3, questo polinomio ha gli zeri in $\mathbf{C}$. Concludiamo che $\alpha_i$ e $\alpha_j$ sono contenuti in $\mathbf{C}$. Il polinomio $G$ ha, dunque, uno zero in $\mathbf{C}$, come richiesto.

**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.

**Esempio.** Sia

$$F = \{\alpha \in \mathbf{C} : \alpha \text{ è algebrico su } \mathbf{Q}\}$$

il campo dei numeri algebrici. Affermiamo che $F$ è una chiusura algebrica di $\mathbf{Q}$: per definizione $F$ è una estensione algebrica di $\mathbf{Q}$. Adesso vediamo che $F$ è algebricamente chiuso. Sia $f = a_nX^n + \ldots + a_1X + a_0 \in F[X]$ un polinomio e sia $\alpha \in \mathbf{C}$ uno zero di $f$. Siccome ogni coefficiente $a_i$ è algebrico su $\mathbf{Q}$, abbiamo per il Teorema 17.4, che

$$[\mathbf{Q}(a_n, \ldots, a_1, a_0) : \mathbf{Q}] < \infty.$$

Siccome $\alpha$ è algebrico sul campo $\mathbf{Q}(a_n, \ldots, a_1, a_0)$ abbiamo che

$$[\mathbf{Q}(\alpha, a_n, \ldots, a_1, a_0) : \mathbf{Q}(a_n, \ldots, a_1, a_0)] < \infty$$

e quindi, per la Prop.17.3, che $\mathbf{Q}(\alpha, a_n, \ldots, a_1, a_0)$ è una estensione finita di $\mathbf{Q}$. Questo implica che $\alpha$ è algebrico su $\mathbf{Q}$, cioè $\alpha \in F$.

Siccome $\mathbf{C}$ è algebricamente chiuso,

$$f = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n).$$

dove $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$. Siccome ogni zero di $f$ in $\mathbf{C}$ sta in $F$, concludiamo che $F$ è algebricamente chiuso, come richiesto.

**Teorema (19.5).** *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.**

(19.A) Esprimere il polinomio simmetrico

$$X_1^3 + X_2^3 + X_3^3$$

in termini dei polinomi simmetrici elementari $\sigma_1$, $\sigma_2$ e $\sigma_3$.

(19.B) Siano $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{C}$ tali che

$$X^3 - X - 1 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

sia

$$p_k = \alpha_1^k + \alpha_2^k + \alpha_3^k \qquad \text{per } k \in \mathbf{Z}.$$

Dimostrare che

$$\begin{aligned} &p_{-1} = -1, \quad p_0 = 3, \quad p_1 = 0, \\ &p_k = p_{k-2} + p_{k-3} \qquad \text{per ogni } k \in \mathbf{Z}, \\ &p_k \in \mathbf{Z} \qquad\quad \text{per ogni } k \in \mathbf{Z}. \end{aligned}$$

(19.C) Sia

$$X^3 - X^2 + X - 2 = (X - \alpha)(X - \beta)(X - \gamma).$$

(i) Trovare il polinomio che ha $\alpha^2$, $\beta^2$ e $\gamma^2$ come zeri.
(ii) Trovare il polinomio che ha $\alpha\beta$, $\beta\gamma$ e $\gamma\alpha$ come zeri.

(19.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 $\alpha_i$.
(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 $\Delta(f) = D(a_{n-1}, \ldots, a_1, a_0)$.

(19.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 19.1.
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 $a_i \in \mathbf{Z}_{\geq 0}$.

Ordiniamo i termini di $g$ in tal modo che il termine $rY_1^{a_1-a_2} \cdot Y_2^{a_2-a_3} \cdot \ldots \cdot Y_n^{a_n}$ viene 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 $a_i \neq b_i$.

(ii) 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 19.1 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.*

(19.F) Sia

$$f = a_n X^n + \ldots + a_1 X + a_0 \in \mathbf{C}[X]$$

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 $\mathbf{R}$.

(19.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 $\sigma_i$. Dimostrare che c'è un'isomorfismo di anelli

$$R[\sigma_1, \sigma_2, \ldots, \sigma_n] \cong R[X_1, X_2, \ldots, X_n].$$

(19.H) Dimostrare che un campo algebricamente chiuso è infinito.

(19.I) Sia $K \subset \mathbf{C}$ una estensione finita di $\mathbf{Q}$. Far vedere che la chiusura algebrica $\overline{\mathbf{Q}}$ di $\mathbf{Q}$ è anche una chiusura algebrica di $K$.

(19.J) Sia $\overline{\mathbf{Q}} \subset \mathbf{C}$ la chiusura algebrica di $\mathbf{Q}$ in $\mathbf{C}$. Dimostrare che

$$[\overline{\mathbf{Q}} : \overline{\mathbf{Q}} \cap \mathbf{R}] = 2.$$

(19.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 $\mathbf{Q}$.

(ii) Far vedere che $K_n \subset K_{n+1}$ per ogni $n \in \mathbf{Z}_{\geq 1}$.

(iii) Far vedere che

$$\overline{\mathbf{F}_p} = \bigcup_{n \geq 1} K_n.$$

(19.L) Sia $f \in \mathbf{R}[X]$ 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 $\alpha_1, \ldots, \alpha_k \in \mathbf{R}$, $c \in \mathbf{R}^*$ e

$$f_j = X^2 + \beta_j X + \gamma_j, \qquad \text{per } 1 \leq j \leq m$$

con $\beta_j, \gamma_j \in \mathbf{R}$ e $\beta_j^2 - 4\gamma_j < 0$. Inoltre, questo modo di scrivere è unico a meno dell'ordine dei fattori.