Matematica Discreta

Domenico Luminati

a.a. 1998/99

Questo è il diario "in tempo reale" del corso, corredato da brevi note delle lezioni. Alla fine del corso servirà come programma d'esame. Non vuole sostituire i libri di testo, che restano quelli indicati nel programma del corso, ma soltanto una traccia da seguire per la preparazione dell'esame.

Programma svolto a lezione

Lezione 1 (22 febbraio 1999 h. 9.30-10.30)

L'assioma di buon ordinamento dei numeri naturali

Assioma 1.1 (di buon ordinamento) *Se $S \subset \mathbb{N}$ è un sottoinsieme non vuoto allora S ha minimo, ossia esiste $m \in S$ tale che per ogni $s \in S$ si ha $m \leq s$.*

Principio di induzione: prima forma

Teorema 1.2 (prima forma dell'induzione) *Sia $P(n)$ una successione di proposizioni indicizzate sui naturali. Si supponga che*

1. *$P(0)$ sia vera.*
2. *$\forall n \in \mathbb{N}\ P(n) \Rightarrow P(n+1)$*

allora $P(n)$ è vera per ogni n.

Dim. Sia $S = \{n \in \mathbb{N} \mid P(n) \text{ non è vera}\}$, se per assurdo $S \neq \varnothing$, per l'assioma di buon ordinamento (1.1) esiste m il minimo di S. $m > 0$ dato che $P(0)$ è vera per l'ipotesi 1, mentre $P(m)$ è falsa in quanto $m \in S$. Ma allora $m - 1 \in \mathbb{N}$ e, dato che $m - 1 < m$ e m è il minimo di S, $m - 1 \notin S$ ossia $P(m-1)$ è vera. Ma allora, per l'ipotesi 2 si ha che $P(m-1+1) = P(m)$ è vera, ossia $m \notin S$, che è assurdo. Quindi $S = \varnothing$ ossia $P(n)$ è vera per ogni $n \in \mathbb{N}$. ❑

Principio di induzione: seconda forma

Teorema 1.3 (seconda forma dell'induzione) *Sia $P(n)$ una successione di proposizioni indicizzate sui naturali. Si supponga che*

1. *$P(0)$ sia vera.*
2. *$\forall n > 0$ se $P(k)$ è vera per ogni $k < n$ allora anche $P(n)$ è vera*

allora $P(n)$ è vera per ogni n.

Dim. Come nella dimostrazione precedente sia $S = \{n \in \mathbb{N} \mid P(n) \text{ non è vera}\}$, e come prima supponiamo per assurdo $S \neq \varnothing$, e sia m il minimo di S. $m > 0$ dato che $P(0)$ è vera per l'ipotesi 1, mentre $P(m)$ non è vera in quanto $m \in S$. Inoltre, dato che m è il minimo di S, se $k < m$ allora $k \notin S$ e quindi $P(k)$ è vera. Ma allora, per l'ipotesi 2 si ha che $P(m)$ è vera, ossia $m \notin S$, che è assurdo. Quindi $S = \varnothing$ ossia $P(n)$ è vera per ogni $n \in \mathbb{N}$. ❑

Divisione euclidea tra naturali

Proposizione 1.4 *Siano $n, m \in \mathbb{N}$, $m \neq 0$ allora esistono $q, r \in \mathbb{N}$ tali che*

$$n = mq + r \quad \text{con} \quad 0 \leq r < m.$$

Dim. Usiamo il principio di induzione nella seconda forma (teorema 1.3) applicato alla successione di proposizioni

$$P(n) := \forall\, m > 0\ \exists\, q, r \in \mathbb{N} \text{ tali che } n = mq + r \text{ e } 0 \leq r < m$$

Se $n = 0$ basta prendere $q = r = 0$. Sia ora $n > 0$ e supponiamo che $P(k)$ sia vera per ogni $k < n$. Osserviamo che se $m > n$ basta prendere $q = 0$ e $r = n$. Se invece $m \leq n$, consideriamo $k = n - m$. Dato che $0 < m \leq n$ si ha $0 \leq k < n$ e quindi, per ipotesi di induzione $P(k)$ è vera. Ossia esistono $q, r \in \mathbb{N}$ tali che $0 \leq r < m$ e $k = mq + r$. Ma allora $n = k + m = mq + m + r = m(q + 1) + r$. ❑

Lezione 2 (24 febbraio 1999 h. 9.30-10.30)

Divisione euclidea tra interi

Teorema 2.1 (divisione euclidea) *Siano $n, m \in \mathbb{Z}$ con $m \neq 0$ allora esistono unici $q, r \in \mathbb{Z}$ tali che*

$$n = mq + r \quad \text{con} \quad 0 \leq r < |m|\,.$$

Dim. Dimostriamo l'esistenza. Se $n \geq 0$ e $m > 0$ la tesi segue dalla proposizione 1.4 e dall'osservazione che $|m| = m$.

Supponiamo ora $n < 0$ e $m > 0$. Allora $-n > 0$ e quindi per il caso precedente si ha che esistono $q, r \in \mathbb{Z}$ tali che $-n = mq + r$ e $0 \leq r < m = |m|$. E quindi $n = m(-q) - r$. Se $r = 0$ abbiamo finito, se invece $0 < r < m$ allora $0 < m - r < m = |m|$ e $n = m(-q) - r = m(-q) - m + m - r = m(-1-q) + (m-r)$.

Sia infine $m < 0$ allora $-m > 0$, quindi per i due casi precedenti esistono $q, r \in \mathbb{Z}$ tali che $n = (-m)q + = m(-q) + r$ con $0 \leq r < -m = |m|$.

Dimostriamo ora l'unicità. Supponiamo che $n = mq + r = mq' + r'$ con $0 \leq r, r' < |m|$. Supponiamo che $r' \geq r$, allora $m(q - q') = r' - r$ e quindi passando ai moduli si ha $|m|\,|q - q'| = |r' - r| = r' - r < |m|$,da cui $0 \leq |q - q'| < 1$ e quindi $|q - q'| = 0$ ovvero $q = q'$. Ma allora da $mq + r = mq' + r'$ segue che anche $r = r'$. ❑

Scrittura in base arbitraria degli interi

Teorema 2.2 (scrittura degli interi in base arbitraria) *Sia $b \geq 2$ un intero. Allora per ogni $n \in \mathbb{N}$ esiste una successione $\{\varepsilon_i\}_{i \in \mathbb{N}}$ di interi tali che:*

1. *$\{\varepsilon_i\}$ è definitivamente nulla (i.e. esiste $i_0 \in \mathbb{N}$ tale che $\varepsilon_i = 0$ per ogni $i > i_0$);*

2. *$0 \leq \varepsilon_i < b$ per ogni $i \in \mathbb{N}$;*

3. *$n = \sum_{i=0}^{\infty} \varepsilon_i b^i$.*

Tale successione è unica, ovvero se $\{\varepsilon_i\}_{i\in\mathbb{N}}$ e $\{\varepsilon'_i\}_{i\in\mathbb{N}}$ verificano la 1, 2 e 3 allora $\varepsilon_i = \varepsilon'_i$ per ogni $i \in \mathbb{N}$.

Dim. Dimostriamo l'esistenza per induzione su n. Se $n = 0$ basta prendere $\varepsilon_i = 0$ per ogni $i \in \mathbb{N}$. Supponiamo ora $n > 0$ e che la tesi sia vera per ogni $k < n$. Siano q, r tali che $n = bq + r$ con $0 \leq r < b$. Dato che $b \geq 2$ si ha che $0 \leq q < bq \leq bq + r = n$ e quindi per ipotesi di induzione esiste una successione definitivamente nulla $\{\delta_i\}$, costituita di interi tali che $0 \leq \delta_i < b$ per ogni i e tale che $q = \sum\limits_{i=0}^{\infty} \delta_i b^i$. Ma allora

$$n = bq + r = b\sum_{i=0}^{\infty} \delta_i b^i + r = \sum_{i=0}^{\infty} \delta_i b^{i+1} + r = \sum_{i=1}^{\infty} \delta_{i-1} b^i + r = \sum_{i=0}^{\infty} \varepsilon_i b^i$$

dove si è posto $\varepsilon_0 = r$ e $\varepsilon_i = \delta_{i-1}$ per ogni $i > 0$. La successione $\{\varepsilon_i\}$ è definitivamente nulla, dato che lo è $\{\delta_i\}$ ed inoltre $0 \leq \varepsilon_i = \delta_{i-1} < b$ per ogni $i > 0$ e $0 \leq \varepsilon_0 = r < b$.

Dimostriamo ora l'unicità. Procediamo per induzione su n. Se $n = 0 = \sum_i \varepsilon_i b^i$ allora ogni addendo della somma essendo nonnegativo, deve essere nullo e quindi $\varepsilon_i = 0$ per ogni i.

Supponiamo ora $n > 0$ e che l'espressione in base b sia unica per tutti i numeri $k < n$. Sia n tale che $n = \sum\limits_{i=0}^{\infty} \varepsilon_i b^i = \sum\limits_{i=0}^{\infty} \varepsilon'_i b^i$. Allora possiamo scrivere

$$n = b\sum_{i=1}^{\infty} \varepsilon_i b^{i-1} + \varepsilon_0 = b\sum_{i=1}^{\infty} \varepsilon'_i b^{i-1} + \varepsilon'_0$$

ma per l'unicità della divisione euclidea (teorema 2.1) si ha che $\varepsilon_0 = \varepsilon'_0$ e $q = \sum\limits_{i=1}^{\infty} \varepsilon_i b^{i-1} = \sum\limits_{i=1}^{\infty} \varepsilon'_i b^{i-1}$. Come prima $q < n$ e quindi per ipotesi di induzione si ha anche che $\varepsilon_i = \varepsilon'_i$ per ogni $i \geq 1$. ❑

Lezione 3 (25 febbraio 1999 h. 10.30-11.30)

Divisibilità e sue prime proprietà

Definizione 3.1 *Dati due interi n, m si dice che n è un* divisore *di m (o che m è un* multiplo *di n) se esiste un $k \in \mathbb{Z}$ tale che $m = nk$. Si indica con $n|m$ (si legge n* divide *m).*

Esempio 3.2 $n|0$ per ogni n mentre se $n \neq 0$ allora $0 \not| n$, si ha inoltre che $\pm 1|n$ e $\pm n|n$ per ogni n.

Proposizione 3.3

1. *Se $n|m$ e $m|q$ allora $n|q$.*

2. *Se $n|m$ e $m|n$ allora $n = \pm m$.*

Dim. 1. Se $m = kn$ e $q = hm$ allora $q = hkm = (hk)m$ ossia $n|q$.

2. Se $n = mk$ e $m = nh$ allora $m = hkm$ e quindi $m(1 - hk) = 0$ e quindi o $m = 0$ e quindi anche $n = 0$, oppure $1 - hk = 0$ ma allora o $h = k = 1$ e quindi $n = m$ oppure $n = m = -1$ e quindi $n = -m$. ❑

Definizione 3.4 *Il numero n si dice* primo *se i suoi unici divisori sono $\pm 1, \pm n$.*

Il massimo comun divisore: definizione, esistenza e unicità

Definizione 3.5 *Dati due interi n, m non entrambi nulli, si dice che d è* un massimo comun divisore*tra n e m se:*

1. *$d|n$ e $d|m$;*

2. *Se $c|n$ e $c|m$ allora $c|d$.*

Proposizione 3.6 *Se d e d' sono due massimi comun divisori tra n e m allora $d' = \pm d$.*

Dim. d è un divisore comune di n e m, quindi poiché d' è un massimo comun divisore si ha che $d|d'$. Scambiando i ruoli di d e d' si ha allora che anche $d'|d$ e quindi per 3.3 si ha che $d' = \pm d$. ❑

Definizione 3.7 *Diremo che d è* il massimo comun divisore *di n e m se è un massimo comun divisore positivo. La proposizione precedente garantisce che se esiste il massimo comun divisore è unico. Esso verrà indicato con (n, m).*

Teorema 3.8 *Dati due numeri $n, m \in \mathbb{Z}$ non entrambi nulli esiste il massimo comun divisore di n ed m.*

Dim. Si consideri l'insieme $S = \{s \in \mathbb{Z} \mid s > 0, \exists x, x \in \mathbb{Z} : s = nx + my\}$. $S \neq \varnothing$ dato che $nn + mm > 0$ (dato che n e m non sono entrambi nulli). Sia $d = nx + my = \min S$, dimostriamo che d è il massimo comun divisore. Se $c|n$ e $c|m$ allora $n = ck$ e $m = ch$, quindi $d = nx + my = ckx + chy = c(kx + hy)$ ossia $c|d$. Dimostriamo ora che $d|n$. Consideriamo la divisione euclidea tra n e d ossia $n = dq + r$ con $0 \leq r < d$, se $r > 0$ allora $r = n - dq = n - (nx + my)q = n(1 - qx) + (-m)y$ è un elemento di S. Ciò è assurdo perché $r < d$ e $d = \min S$. Quindi $r = 0$ ossia $d|n$. In modo analogo si prova che $d|m$. ❑

Osservazione 3.9 Dalla dimostrazione precedente segue che dati $n, m \in \mathbb{Z}$ esistono $x, y \in \mathbb{Z}$ tali che $(n, m) = nx + my$ e che gli interi della forma $nx + my$ con $x, y \in \mathbb{Z}$ sono tutti e soli i multipli di (n, m).

Definizione 3.10 *$n, m \in \mathbb{Z}$ non entrambi nulli si dicono* coprimi *se* $(n, m) = 1$.

Osservazione 3.11 $(n, m) = 1$ se e solo se esistono $x, y \in \mathbb{Z}$ tali che $nx + my = 1$. Ad esempio $(n, n+1) = 1$ per ogni n. Infatti $1 = (n+1)1 + n(-1)$.

Proposizione 3.12 *Sia* $d = (n, m)$, *allora* $(\frac{n}{d}, \frac{m}{d}) = 1$.

Dim. $d = nx + my$ e quindi $1 = \frac{n}{d}x + \frac{m}{d}y$. ❑

Lezione 4 (1 marzo 1999 h. 9.30-10.30)

L'algoritmo di Euclide per il calcolo del M.C.D.

Proposizione 4.1 (algoritmo di Euclide) *Siano* $n, m \in \mathbb{Z}$, $m \neq 0$. *Sia* $n = mq + r$ *la divisione euclidea di* n *per* m *allora* $\{c \in \mathbb{Z} \mid c|n \text{ e } c|m\} = \{c \in \mathbb{Z} \mid c|m \text{ e } c|r\}$, *in particolare quindi* $(n, m) = (m, r)$.

Dim. Se $c|n$ e $c|m$ allora $n = ch$ e $m = ck$ e quindi $r = n - mq = ch - ckq = c(h - kq)$ ossia $c|r$ e $c|m$. Viveversa se $c|r$ e $c|m$ allora $m = ch$ e $r = ck$ e quindi $n = mq + r = chq + ck = c(hq + r)$ ossia $c|n$ e $c|m$. ❑

La proposizione precedente assieme all'osservazione che $(n, 0) = n$ per ogni $n \neq 0$ permette di costruire un algoritmo (*algoritmo di Euclide*) per il calcolo del M.C.D.

ALGORITMO DI EUCLIDE

- INPUT: n, $m \in \mathbb{Z}$.
- $n = 0 \Rightarrow$ OUTPUT: m
- $m = 0 \Rightarrow$ OUTPUT: n
- $n \neq 0$ e $m \neq 0$ esegui la divisione euclidea $n = mq + r$ e applica l'algoritmo di Euclide a m, r.

Proprietà dei numeri coprimi e caratterizzazione dei numeri primi

Proposizione 4.2

1. *se* $(n, m) = 1$ *e* $n|mq$ *allora* $n|q$.
2. *se* $(n, m) = 1$ *e* $n|q$ *e* $m|q$ *allora* $nm|q$.

Dim. 1. Se $(n,m)=1$ allora esistono $x,y\in\mathbb{Z}$ tali che $1=nx+my$ e quindi $q=nqx+mqy$. Ma allora se $n|mq$ esiste h tale che $mq=nh$ e quindi $q=nqx+nhy=n(qx+hy)$.

2. $n|q$ quindi $q=nh$, dato che $m|q=nh$ e $(n,m)=1$ allora per la 1 si ha che $m|h$ ossia $h=km$ e quindi $q=nh=nmk$, ovvero $nm|q$. ❑

Corollario 4.3 *p è primo se e solo se per ogni $n,m\in\mathbb{Z}$ si ha che $p|nm\Rightarrow p|n$ oppure $p|m$.*

Dim. Supponiamo che $p|nm$, dato che p è primo, se $p\not|n$ allora $(p,n)=1$, per lo proposizione precedente si ha allora che $p|m$.

Viceversa supponiamo che per ogni $n,m\in\mathbb{Z}$ si ha che $p|nm\Rightarrow p|n$ oppure $p|m$, allora se $p=dh$ allora $p|dh$ e quindi $p|d$, e quindi per 3.3 si ha che $d=\pm p$ e $h=\pm1$ oppure $p|h$ e quindi $h=\pm p$ e $d=\pm1$. ❑

Esercizio 4.1 Siano $n_1,\dots,n_k\in\mathbb{Z}$ e sia p un primo tale che $p|n_1n_2\dots n_k$. Si provi che allora esiste i tale che $p|n_i$.

Il minimo comune multiplo: definizione, esistenza e unicità

Definizione 4.4 *Dati due interi $n,m\in\mathbb{Z}$ si dice che M è un minimo comune multiplo di n e m se*

1. *$n|M$ e $m|M$;*
2. *se $n|c$ e $m|c$ allora $M|c$.*

Come nel caso del massimo comun divisore si dimostra che due minimi comuni multipli sono uguali a meno del segno e quindi si chiama il minimo comune multiplo *quello positivo e sarà indicato con $[n,m]$.*

Teorema 4.5 (esistenza del m.c.m.) *Siano $n,m\in\mathbb{Z}$ non entrambi nulli allora esiste il minimo comune multiplo tra n e m.*

Dim. Sia $M=\frac{nm}{(n,m)}=n'm'(n,m)$ dove si è posto $n=n'(n,m)$ e $m=m'(n,m)$. Chiaramente allora $M=nm'=n'm$ e quindi $n|M$ e $m|M$.

Se $n|c$ e $m|c$ allora $(n,m)|c$ e quindi posto $c=c'(n,m)$ si ha che $n'|c'$ e $m'|c'$. Dato che $(n',m')=1$, per 4.2 si ha che $n'm'|c'$ e quindi che $M=n'm'(n,m)|c'(n,m)=c$. ❑

Lezione 5 (3 marzo 1999 h. 9.30-10.30)

Il teorema fondamentale dell'Aritmetica

Teorema 5.1 (Teorema fondamentale dell'aritmetica) *Per ogni $n \in \mathbb{Z}$, $n \geq 2$ esistono numeri primi $p_1, p_2, \ldots, p_k > 0$ tali che $n = p_1 p_2 \ldots p_k$. Se anche $q_1, \ldots, q_h$ sono primi positivi tali che $n = q_1 q_2 \ldots q_h$, esiste una bigezione $\sigma : \{1, 2, \ldots, h\} \to \{1, 2, \ldots, k\}$ tale che $q_i = p_{\sigma(i)}$.*

In altre parole, ogni intero maqggiore di 1 si scrive in modo unico, a meno dell'ordine, come prodotto di numeri primi positivi.

Dim. Procediamo per induzione su n. Se $n = 2$ non c'è nulla da dimostrare in quanto 2 è primo. Supponiamo $n > 2$ e che la tesi sia vera per ogni $k < n$. Se n è primo non c'è nulla da dimostrare, se n non è primo allora esistono due numeri $d_1 d_2$ con $1 < d_1, d_2 < n$ tali che $n = d_1 d_2$. Per ipotesi di induzione esistono dei primi positivi p_i e q_j tali che $d_1 = p_1 \ldots p_{k_1}$ e $d_2 = q_1 \ldots q_{k_2}$, ma allora $n = p_1 \ldots p_{k_1} q_1 \ldots q_{k_2}$ è prodotto di primi positivi.

Unicità. Sia $n = p_1 \ldots p_k = q_1 \ldots q_h$ con p_i e q_j primi positivi e $k \leq h$. Procediamo per induzione su k. Se $k = 1$ allora $n = p_1 = q_1 \ldots q_h$, quindi $q_j \big| p_1$ per ogni j, e dato che p_1 è primo ogni $q_j = 1$ oppure $q_j = p_1$. Poiché per ipotesi ogni $q_j > 1$ allora $q_j = p_1$ per ogni j. Se ora fosse $h > 1$ si avrebbe $n = q_1 \ldots q_h \geq q_1 q_2 = p_1^2 > p_1 = n$ e questo è assurdo, e quindi $h = 1$ e $q_1 = p_1$.

Sia $k > 1$, allora $p_k \big| n = q_1 \ldots q_h$, quindi per l'esercizio 4.1 esiste un j tale che $p_k \big| q_j$. Dato che sia p_k che q_j sono primi positivi, allora $p_k = q_j$. Ma allora $p_1 \ldots p_{k-1} = q_1 \ldots q_{j-1} q_{j+1} \ldots q_h$, per ipotesi di induzione possiamo allora dire che le due fattorizzazioni hanno lo stesso numero di elementi, ossia $k - 1 = h - 1$, e che esiste una bigezione $\delta : \{1, \ldots, j-1, j+1, \ldots, k\} \to \{1, \ldots, k-1\}$ tale che $q_i = p_{\delta(i)}$ per ogni i. Definendo allora $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$

$$\sigma(i) = \begin{cases} k & \text{se } i = j \\ \delta(i) & \text{se } i \neq j \end{cases}$$

si ottiene una bigezione tale che $q_i = p_{\sigma(i)}$ per ogni i. ❑

Esistenza di infiniti numeri primi

Corollario 5.2 *I numeri primi sono infiniti.*

Dim. Per assurdo supponiamo che $p_1, p_2, \ldots, p_n$ siano tutti iprimi. Si consideri $n = p_1 p_2 \ldots p_n + 1$. Chiaramente $n > 1$ e non è divisibile per nessun p_i e quindi n sarebbe un numero maggiore di 1 che non è divisibile per nessun primo e ciò contraddice il teorema fondamentale dell'aritmetica (5.1). ❑

Calcolo del M.C.D. e del m.c.m. usando la fattorizzazione in primi

Se $a, b \in \mathbb{N}$ denotiamo con $a \vee b = \max\{a, b\}$ e con $a \wedge b = \min\{a, b\}$ (si veda la definizione di reticolo (24.1) per giustificare tale notazione).

Proposizione 5.3 *Siano* $n = \prod_{i=1}^{s} p_i^{k_i}$, $m = \prod_{i=1}^{s} p_i^{h_i}$ *con* p_i *numeri primi, allora* $(n, m) = \prod_{i=1}^{s} p_i^{k_i \wedge h_i}$ *e* $[n, m] = \prod_{i=1}^{s} p_i^{k_i \vee h_i}$.

Dim. Chiaramente $\prod_{i=1}^{s} p_i^{k_i \wedge h_i}$ è un divisore comune a n e m. Inoltre se c è un divisore comune non può avere fattori primi diversi dai p_i, quindi $c = \prod_{i=1}^{s} p_i^{l_i}$. Dal fatto che $c \big| n$ segue allora che $l_i \leq k_i$ e dal fatto che $c \big| m$ segue che $l_i \leq h_i$ per ogni i, e quindi $l_i \leq k_i \wedge h_i$.

La formula per il m.c.m. segue allora dal fatto che $[n, m] = |nm| / (n, m)$, e che per ogni coppia di numeri reali si ha che $h + k - h \wedge k = h \vee k$. ❑

Lezione 6 (8 marzo 1999 h. 9.30-10.30)

Definizione di congruenza e prime proprietà

Definizione 6.1 *Siano* $a, b \in \mathbb{Z}$, *si dice che* a *è congruo a* b *modulo* n *(in simboli* $a \equiv b \mod n$*) se* $n \big| a - b$.

Proposizione 6.2 *Valgono le seguenti proprietà:*

1. *(proprietà riflessiva)* $a \equiv a \mod n$ *per ogni* $a, n \in \mathbb{Z}$;
2. *(proprietà simmetrica)* $a \equiv b \mod n \Rightarrow b \equiv a \mod n$ *per ogni* $a, b, n \in \mathbb{Z}$;
3. *(proprietà transitiva)* $a \equiv b \mod n$ *e* $b \equiv c \mod n \Rightarrow a \equiv c \mod n$ *per ogni* $a, b, c, n \in \mathbb{Z}$.

Dim. 1. $n \big| 0 = a - a$ per ogni $n \in \mathbb{Z}$.

2. Se $n \big| a - b$ allora $a - b = kn$ e quindi $b - a = (-k)n$ e quindi $n \big| b - a$ ossia $b \equiv a \mod n$.

3. Se $a \equiv b \mod n$ e $b \equiv c \mod n$ allora $a - b = kn$ e $b - c = hn$ e quindi $a - c = a - b + b - c = kn + hn = (k + h)n$ e quindi $a \equiv c \mod n$. ❑

Classi di congruenza

Definizione 6.3 *Siano* $a, n \in \mathbb{Z}$, *si chiama classe di congruenza di* a *modulo* n *l'insieme*

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \mod n\}.$$

Indicheremo $\mathbb{Z}/_{(n)} = \left\{ [a]_n \,\middle|\, a \in \mathbb{Z} \right\}$

Osservazione 6.4 $x \equiv a \mod n$ se e solo se $n|(x-a)$ se e solo se esiste $k \in \mathbb{Z}$ tale che $x - a = kn$ se e solo se esiste $k \in \mathbb{Z}$ tale che $x = a + kn$ e quindi

$$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}.$$

Proposizione 6.5 *1. per ogni $a \in \mathbb{Z}$ $a \in [a]_n$*

2. per ogni $a, b \in \mathbb{Z}$ $[a]_n = [b]_n$ se e solo se $a \equiv b \mod n$.

3. per ogni $a, b \in \mathbb{Z}$ $[a]_n \cap [b]_n \neq \varnothing \Rightarrow [a]_n = [b]_n$.

Dim. 1. Segue dalla proprietà riflessiva (1 di 6.2).

2. Se $[a]_n = [b]_n$ in particolare $b \in [b]_n = [a]_n$ e quindi $a \equiv b \mod n$. Viceversa sia $a \equiv b \mod n$. Se $x \in [a]_n$ allora $x \equiv a \mod n$; per la proprietà transitiva (3 di 6.2) $x \equiv b \mod n$ ossia $x \in [b]_n$. Analogamente se $x \in [b]_n$ allora $x \in [a]_n$ e quindi le due classi coincidono.

3. Se $x \in [a]_n \cap [b]_n$ allora $x \equiv a \mod n$ e $x \equiv b \mod n$, usando le proprietà simmetrica e transitiva si ha allora che $a \equiv b \mod n$ e quindi, per la (2), appena dimostrata, $[a]_n = [b]_n$. ❑

Le classi modulo n sono esattamente n

Proposizione 6.6 *Se r è il resto della divisione euclidea di a per n allora $a \equiv r \mod n$.*

Dim. $a = nq + r$ quindi $n|nq = a - r$. ❑

Corollario 6.7 *$\mathbb{Z}/_{(n)}$ ha esattamente n elementi.*

Dim. Da 6.6 e dalla 2 di 6.5 segue immediatamente che l'insieme in questione ha al più n elementi e precisamente $[0]_n, [1]_n, \dots, [n-1]_n$. D'altra parte se $0 \leq h < k < n$ allora $0 < k - h < n$ e quindi $n \not| (k-h)$ e quindi (sempre per la 2 di 6.5) $[h]_n \neq [k]_m$. ❑

Somma e prodotto di classi di congruenza

Proposizione 6.8 *Siano $a, b, a', b', n \in \mathbb{Z}$ e si supponga che $a \equiv a' \mod n$ e $b \equiv b' \mod n$. Allora*

1. $a + b \equiv a' + b' \mod n$;

2. $ab \equiv a'b' \mod n$.

Dim. (1). Se $n|(a-a')$ e $n|(b-b')$ allora $n|((a-a')+(b-b')) = ((a+b)-(a'+b'))$.

(2). Esistono $k, h \in \mathbb{Z}$ tali che $a = a' + kn$ e $b = b' + hn$, ma allora, moltiplicando membro a membro si ottiene $ab = a'b' + a'hn + b'kn + hkn^2 = a'b' + n(a'h + b'k + hkn)$ e quindi la tesi. ❑

Osservazione 6.9 La proposizione precedente permette di definire le operazioni di somma e prodotto tra classi modulo n. Ponendo

$$\begin{aligned}
[a]_n + [b]_n &= [a+b]_n \\
[a]_n [b]_n &= [ab]_n
\end{aligned}$$

si ottengono delle buone definizioni. Infatti se $[a]_n = [a']_n$ e $[b]_n = [b']_n$ allora per la 2 di 6.5 si ha che $a \equiv a' \mod n$ e $b \equiv b' \mod n$ e quindi per la proposizione precedente si ha che $a + a' \equiv b + b' \mod n$ e $aa' \equiv bb' \mod n$ e quindi di nuovo per la 2 di 6.5 si ha che $[a+b]_n = [a'+b']_n$ e $[ab]_n = [a'b']_n$.

Il Teorema cinese del resto

Teorema 6.10 (teorema cinese del resto) *Il sistema di congruenze*

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

ha soluzione se e solo se $(n,m)\big|b-a$.

Se c *è una soluzione del sistema, allora gli elementi di* $[c]_{[n,m]}$ *sono tutte e sole le soluzioni del sistema.*

Dim. Sia c una soluzione del sistema allora esistono $h, k \in \mathbb{Z}$ tali che $c = a + hn = b + km$ e quindi $a - b = km - hn$. Ma allora dal fatto che $(n,m)\big|n$ e $(n,m)\big|m$ si ha che $(n,m)\big|a-b$. Viceversa, supponiamo che $(n,m)\big|a-b$, allora, per quanto osservato in 3.9, esistono $h, k \in \mathbb{Z}$ tali che $a - b = hn + km$. Ma allora $a - hn = b + kn$, detto quindi $c = a - hn = b + kn$, si ha evidentemente che c risolve entrambe le congruenze.

Sia $S = \{x \in \mathbb{Z} \mid x \text{ risolve il sistema}\}$. Dobbiamo provare che se c è una soluzione allora $S = [c]_{[n,m]}$.

$S \subseteq [c]_{[n,m]}$. Sia c' un'altra soluzione, allora $c = a + hn = b + km$ e $c' = a + h'n = b + k'm$ e quindi sottraendo si ha

$$\begin{aligned}
c - c' &= a + hn - a' - h'n = (h - h')n &\Rightarrow\ & n\big|(c - c') \\
c - c' &= b + km - b' - k'm = (k - k')m &\Rightarrow\ & m\big|(c - c')
\end{aligned}$$

Ma allora $[n,m]\big|c - c'$ ossia $c' \equiv c \mod [n,m]$ ovvero $c' \in [c]_{[n,m]}$.

$[c]_{[n,m]} \subseteq S$. Sia $c' \in [c]_{[n,m]}$, ovvero $c' = c + h[n,m]$. Dal fatto che $c \equiv a \mod n$ e che $h[n,m] \equiv 0 \mod n$ segue (per la 1 di 6.8) che $c' = c + h[n,m] \equiv a \mod n$. In modo analogo si ha che $c' \equiv b \mod m$ e quindi che $c' \in S$. $\square$

Lezione 7 (15 marzo 1999 h. 9.30-10.30)

Relazioni d'equivalenza: definizione e prime proprietà

Definizione 7.1 *Sia* X *un insieme una relazione su* X *è un sottoinsieme di* $X \times X$. *Se* $\mathcal{R}$ *è una relazione su* X *si scriverà* $x\mathcal{R}x$ *piuttosto che* $(x_1, x_2) \in \mathcal{R}$

Diremo che $\mathcal{R}$ *è una* relazione d'equivalenza *se verifica le seguenti proprietà:*

1. *(proprietà riflessiva)* $x\mathcal{R}x$ *per ogni* $x \in X$*;*

2. *(proprietà simmetrica)* $x_1\mathcal{R}x_2 \Rightarrow x_2\mathcal{R}x_1$ *per ogni* $x_1, x_2 \in X$*;*

3. *(proprietà transitiva)* $x_1\mathcal{R}x_2$ *e* $x_2\mathcal{R}x_3 \Rightarrow x_1\mathcal{R}x_3$ *per ogni* $x_1, x_2, x_3 \in X$.

Se $\mathcal{R}$ *è una relazione d'equivalenza su* X *e* $x \in X$ *si chiama* classe d'equivalenza di x *l'insieme*

$$[x]_{\mathcal{R}} = \{y \in X \mid y\mathcal{R}x\}.$$

Osservazione 7.2 Per ogni n la congruenza modulo n è una relazione d'equivalenza.

Proposizione 7.3 *Se* $\mathcal{R}$ *è una relazione d'equivalenza su* X *allora:*

1. *per ogni* $x \in X$ $x \in [x]_{\mathcal{R}}$.

2. *per ogni* $x_1, x_2 \in X$ $[x_1]_{\mathcal{R}} = [x_2]_{\mathcal{R}}$ *se e solo se* $x_1\mathcal{R}x_2$

3. *per ogni* $x_1, x_2 \in X$ $[x_1]_{\mathcal{R}} \cap [x_2]_{\mathcal{R}} \neq \varnothing \Rightarrow [x_1]_{\mathcal{R}} = [x_2]_{\mathcal{R}}$.

Dim. Si osservi che nella dimostrazione della proposizione 6.5 non si è usato il fatto che si stesse parlando di congruenze, ma soltanto il fatto che la relazione di congruenza verifica le proprietà riflessiva, simmetrica e transitiva (proposizione 6.2); basta allora ripetere parola per parola quella dimostrazione. ❏

Partizioni e insieme quoziente

Definizione 7.4 *Sia* X *un insieme e* $\mathcal{R}$ *una relazione d'equivalenza su* X*, l'insieme delle classi d'equivalenza di* X *si chiama* insieme quoziente *di* X *modulo* $\mathcal{R}$ *e si denota con* $X/_{\mathcal{R}}$.

È definita l'applicazione

$$\begin{aligned} \pi_{\mathcal{R}} &: X \longrightarrow X/_{\mathcal{R}} \\ \pi_{\mathcal{R}} &: x \longmapsto [x]_{\mathcal{R}} \end{aligned}$$

che ad ogni elemento associa la sua classe d'equivalenza e che si chiama proiezione a quoziente.

Osservazione 7.5 La proiezione a quoziente è evidentemente surgettiva.

Definizione 7.6 *Sia* X *un'insieme. Un sottoinsieme* $\mathcal{P}$ *delle parti di* X *si dice una* partizione *di* X *se:*

1. $\bigcup_{A \in \mathcal{P}} A = X$*;*

2. $A \cap B = \varnothing$ *per ogni* $A, B \in \mathcal{P}$ *con* $a \neq B$.

Osservazione 7.7 Alla luce di queste due definizioni i punti 1 e 3 della proposizione precedente (7.3) possono essere riassunti dicendo che l'insieme quoziente $X/_{\mathcal{R}}$ è una partizione di X.

Esercizio 7.1 Sia X un insieme. Si dimostri che gli insiemi

$$R = \{\mathcal{R} \mid \mathcal{R} \text{ è una relazione d'equivalenza su } X\}$$
$$P = \{\mathcal{P} \mid \mathcal{P} \text{ è una partizione di } X\}$$

sono in bigezione.

Il teorema di omomorfismo per insiemi

Esercizio 7.2 Siano X e Y insiemi e sia $f : X \to Y$ un'applicazione. Si definisca la relazione su X

$$x_1 \overset{f}{\sim} x_2 \iff f(x_1) = f(x_2).$$

Si provi che $\overset{f}{\sim}$ è una relazione d'equivalenza su X. La relazione $\overset{f}{\sim}$ si chiama *relazione indotta da* f.

Teorema 7.8 *Siano* X, Y *insiemi e* $f : X \to Y$ *un'applicazione. Esiste una unica applicazione* $\widetilde{f} : X/_{\overset{f}{\sim}} \to Y$ *tale che* $\widetilde{f} \circ \pi = f$.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/_{\overset{f}{\sim}} \arrow[ur, "\widetilde{f}"'] & \end{tikzcd}$$

Si ha inoltre che:

1. $\widetilde{f}$ *è iniettiva;*

2. $\widetilde{f}$ *è surgettiva se e solo se* f *è surgettiva.*

Dim. Definiamo $\widetilde{f}$. Sia $[x] \in X/_{\overset{f}{\sim}}$ allora affinché $\widetilde{f} \circ \pi = f$, dovrà risultare che $\widetilde{f}([x]) = \widetilde{f}(\pi(x)) = f(x)$. Quindi se $\widetilde{f}$ esiste è necessariamente unica e definita da $\widetilde{f}([x]) = f(x)$.

Dimostriamo che questa è una buona definizione, ossia che la definizione non dipende dal rappresentante della classe, ossia che se $[x_1] = [x_2]$ allora $\widetilde{f}([x_1]) = \widetilde{f}([x_2])$. Ma:

$$[x_1] = [x_2] \iff x_1 \overset{f}{\sim} x_2 \iff f(x_1) = f(x_2) \tag{1}$$

e quindi la definizione è ben posta.

La catena di equivalenze in (1) mostra anche che $\widetilde{f}$ è iniettiva.

Supponiamo ora che f sia surgettiva, allora dato $y \in Y$ esiste $x \in X$ tale che $f(x) = y$ ma allora $\widetilde{f}([x]) = f(x) = y$. Viceversa se $\widetilde{f}$ è surgettiva, allora dato $y \in Y$ esiste $[x] \in X/_{\underset{\sim}{f}}$ tale che $\widetilde{f}([x]) = y$. Ma allora $f(x) = \widetilde{f}([x]) = y$, ossia f è surgettiva. ❏

Lezione 8 (17 marzo 1999 h. 9.30-10.30)

Definizione di semigruppo

Definizione 8.1 *Sia X un insieme. Un'*operazione binaria *su X è un'applicazione $X \times X \to X$. Se $* : X \times X \to X$ è un'operazione si scriverà $x_1 * x_2$ piuttosto che $*(x_1, x_2)$.*

Un'operazione $*$ si dice associativa *se*

$$x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3 \qquad \forall x_1, x_2, x_3 \in X \tag{2}$$

Una coppia $(X, *)$ dove X è un insieme e $*$ è un'operazione associativa su X si dice un semigruppo*.*

Di norma, se non ci saranno ambiguità, l'operazione di un semigruppo viene denotata con $\cdot$ (notazione moltiplicativa) o con $+$ (notazione additiva). Nel primo caso il punto viene quasi sempre omesso.

Definizione di monoide

Definizione 8.2 *Sia $(X, *)$ un monoide, un elemento $e \in X$ si dice una* unità sinistra *se*

$$e * x = x \quad \forall x \in X \tag{3}$$

un elemento $e \in X$ si dice una unità destra *se*

$$x * e = x \quad \forall x \in X \tag{4}$$

un elemento che sia contemporaneamente una unità sinistra e destra si dice una unità*.*

Un semigruppo si dice un monoide *se possiede una unità.*

Proposizione 8.3 *Sia $(X, *)$ un semigruppo e siano e una unità sinistra e e' una unità destra, allora $e = e'$.*

Dim. Si ha $e' = e * e' = e$, dove la prima uguaglianza vale poiché e è una unità sinistra e la seconda in quanto e' è una unità destra. ❏

Osservazione 8.4 In particolare dalla proposizione precedente (8.3) segue che in un monoide l'unità è unica.

L'unità di un monoide viene usualmente denotata con 1 se si sta usando la notazione moltiplicativa o con 0 se si sta usando la notazione additiva.

Definizione di gruppo

Definizione 8.5 *Sia X un monoide, e sia $x \in X$, un elemento $y \in X$ si dice un* inverso sinistro *di x se $yx = 1$, si dice un inverso destro se $xy = 1$ si dice un inverso se è inverso sia destro che sinistro.*

Un monoide in cui ogni elemento possiede un inverso si chiama un gruppo

Proposizione 8.6 *Sia X un monoide, $x \in X$ e siano y e y' rispettivamente un inverso destro ed un inverso sinistro di x, Allora $y = y'$.*

Dim. $y = y1 = y(xy') = (yx)y' = 1y' = y'$. ❑

Osservazione 8.7 In particolare la proposizione precedente (8.6) garantisce che in un gruppo ogni elemento ha un unico inverso.

L'inverso di un elemento x viene denotato con x^{-1} con la notazione moltiplicativa e con $-x$ con la notazione additiva.

Definizione 8.8 *Una operazione sull'insieme X si dice* commutativa *se per ogni $x_1, x_2 \in X$ si ha $x_1x_2 = x_2x_1$. Se l'operazione di un semigruppo [risp. monoide, gruppo] è commutativa, il semigruppo [risp. monoide, gruppo] sarà detto commutativo.*

Esercizio 8.1 Siano X, Y insiemi e sia $*$ un'operazione su Y. Su Y^X si definisca l'operazione, $\bullet$ ponendo

$$f \bullet g(x) = f(x) * g(x) \qquad \forall x \in X$$

Si provi che

1. se $(Y, *)$ è un semigruppo, anche $(Y^X, \bullet)$ lo è;
2. se $(Y, *)$ è un monoide, anche $(Y^X, \bullet)$ lo è;
3. se $(Y, *)$ è un gruppo, anche $(Y^X, \bullet)$ lo è;
4. se $*$ è commutativa, allora anche $\bullet$ lo è.

Esercizio 8.2 Si dimostri che se G è un gruppo allora per ogni $g \in G$ si ha che $(g^{-1})^{-1} = g$.

Esercizio 8.3 Sia G un gruppo e siano $g_1, g_2 \in G$ si provi che $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$.

Si dimostri che $(g_1g_2)^{-1} = g_1^{-1}g_2^{-1}$ per ogni $g_1, g_2 \in G$ se e solo se il gruppo è commutativo.

Esercizio 8.4 Sia M un monoide e sia $G = \{m \in M \mid m \text{ è invertibile}\}$. Si dimostri che G con l'operazione del monoide è un gruppo.

Definizione di sottosemigruppo, sottomonoide, sottogruppo

Definizione 8.9 *Sia $Y \subseteq X$. Se X è un semigruppo, diremo che Y è un* sottosemigruppo *di X se*

1. $y_1, y_2 \in Y \Rightarrow y_1 y_2 \in Y$

Se X è un monoide diremo che Y è un sottomonoide *di X se è un sottosemigruppo ed in più*

2. $1 \in Y$

Se X è un gruppo, diremo che Y è un sottogruppo *di X se è un sottomonoide ed in più*

3. $y \in Y \Rightarrow y^{-1} \in Y$

Per indicare che Y è un sottogruppo di X si scriverà anche $Y \leq X$.

Criterio del sottogruppo

Proposizione 8.10 (criterio del sottogruppo) *Sia G un gruppo e sia $H \subseteq G$, $H \neq \varnothing$. H è un sottogruppo se e solo se*

$$\forall h_1, h_2 \in H \qquad h_1 h_2^{-1} \in H \tag{5}$$

Dim. Se H è un sottogruppo, e $h_1, h_2 \in H$, allora per la 3 della definizione di sottogruppo (8.9) si ha che $h_2^{-1} \in H$ e quindi per la 1 $h_1 h_2^{-1} \in H$.

Viceversa, supponiamo che valga la (5). Dato che $H \neq \varnothing$ esiste $h \in H$, ma allora per (5) si ha che $1 = hh^{-1} \in H$ e quindi vale la 2 di 8.9. Dato $h \in H$, visto che $1 \in H$ si ha allora che $h^{-1} = 1h^{-1} \in H$ ossia vale anche la 3 di 8.9. Infine, se $h_1, h_2 \in H$, allora $h_2^{-1} \in H$ e quindi $h_1(h_2^{-1})^{-1} \in H$. D'altra parte, per l'esercizio 8.2, $(h_2^{-1})^{-1} = h_2$ e quindi $h_1 h_2 \in H$, ovvero vale la 1 di 8.9. ❏

Esercizio 8.5 Si provi che i sottogruppi di $\mathbb{Z}$ sono tutti e soli gli insiemi della forma $n\mathbb{Z} = \{m \in \mathbb{Z} \mid n \big| m\}$.

Esercizio 8.6 Sia X un gruppo, per ogni $x \in X$ e $n \in \mathbb{Z}$ si definisce x^n ponendo

$$\begin{array}{rcll} x^0 & = & 1 & \\ x^{n+1} & = & xx^n & \forall n \geq 0 \\ x^n & = & (x^{-1})^{-n} & \forall n < 0 \end{array}$$

Si provi che per ogni $n, m \in \mathbb{Z}$ e per ogni $x \in X$ si ha

$$x^{-n} = (x^{-1})^n \tag{6}$$

$$x^n x^m = x^{n+m} \tag{7}$$

$$(x^n)^{-1} = x^{-n} \tag{8}$$

$$(x^n)^m = x^{nm} \tag{9}$$

Lezione 9 (18 marzo 1999 h. 10.30-11.30)

Definizione di permutazione

Definizione 9.1 *Sia X un insieme, una* permutazione *di X è una applicazione bigettiva $X \to X$.*

L'insieme di tutte le permutazioni di X si denota con S_X. Se $n \in \mathbb{N}$ e $n \geq 1$ l'insieme delle permutazioni di $\{1, 2, \ldots, n\}$ si denota semplicemente con S_n.

Proposizione 9.2 *L'insieme S_X con l'operazione di composizione è un gruppo. Viene chiamato il* gruppo simmetrico *di X.*

Dim. La composizione è associativa. Infatti per ogni $x \in X$ $f \circ (g \circ h)(x) = f(g \circ h(x)) = f(g(h(x))) = f \circ g(h(x)) = (f \circ g) \circ h(x)$.

L'applicazione identica $I_X \in S_X$ è l'unità.

Per definizione ogni $f \in S_X$ è bigettiva e quindi esiste l'inversa f^{-1} tale che $f \circ f^{-1} = f^{-1} \circ f = I_X$. Chiaramente $f^{-1} \in S_X$. ❑

Numero di applicazioni iniettive e di permutazioni

Proposizione 9.3 *Se $k, n \in \mathbb{N}$, $k \leq n$ allora l'insieme delle applicazioni iniettive $\{1, \ldots, k\} \to \{1, \ldots, n\}$ ha esattamente $n!/(n-k)!$ elementi.*

Dim. Un'applicazione $f : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, n\}$ è univocamente determinata dalla k-upla $(f(1), \ldots, f(k))$. Ora $f(1)$ può essere scelto in n modi diversi, se si vuole che f sia iniettiva $f(2)$ potrà essere scelto tra tutti i numeri da 1 a n tranne $f(1)$, quindi per $f(2)$ si hanno esattamente $n-1$ possibilità di scelta, analogamente per $f(3)$ si hanno $n-2$ scelte possibili e così vaia, supposto di aver scelto $f(1), \ldots, f(i)$, per $f(i+1)$ si hanno $n-i$ scelte possibili.Si arriva in tal modo fino ad $f(k)$ per il quale si hanno $f(n-k+1)$ scelte. In totale si ottengono quindi $n(n-1)(n-2)\ldots(n-k+1) = n!/(n-k)!$ applicazioni iniettive diverse. ❑

Osservazione 9.4 Lo stesso modo di ragionare della dimostrazione precedente, mostra che l'insieme di tutte le funzioni $\{1, \ldots, k\} \to \{1, \ldots, n\}$ ha n^k elementi. Infatti, non avendo restrizioni su f, ad ogni passo della sua costruzione si hanno n possibilità di scelta.

Lo stesso modo di ragionare non funziona per cercare di calcolare il numero delle applicazioni surgettive.

Proposizione 9.5 *Se $n \in \mathbb{N}$, $n \geq 1$ allora S_n ha esattamente $n!$ elementi.*

Dim. Segue dalla proposizione precedente applicata al caso $n = k$. ❑

Definizione di ciclo

Definizione 9.6 *Una permutazione $\sigma \in S_n$ si dice un* ciclo *se esistono a_1, $a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ tali che*

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

Una tale permutazione si denota con $(a_1\ a_2 \ldots a_k)$ e l'intero k si chiama la lunghezza *del ciclo. I cicli di lunghezza 2 sono chiamati* trasposizioni. *La permutazione identica è l'unico ciclo di lunghezza 1 e viene denotata con (1). Due cicli $(a_1 \ldots a_k)$ e $(b_1 \ldots b_h)$ si dicono disgiunti se $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_h\} = \varnothing$.*

Decomposizione in cicli disgiunti

Proposizione 9.7 *Siano $\sigma_1 = (a_1 \ldots a_k)$ e $\sigma_2 = (b_1 \ldots b_h)$ due cicli disgiunti, allora $\sigma_1\sigma_2 = \sigma_2\sigma_1$.*

Dim. Dal fatto che i due cicli sono disgiunti, si ha che l'insieme $\{1, 2, \ldots, n\}$ si spezza nell'unione di tre pezzi a due a due disgiunti: $A \cup B \cup X$ essendo $A = \{a_1, \ldots, a_k\}$ $B = \{b_1, \ldots, b_k\}$. Ora se $x \in X$ si ha che $\sigma_1(x) = \sigma_2(x) = x$ e quindi $\sigma_1\sigma_2(x) = \sigma_1(\sigma_2(x)) = \sigma_2(x) = x$ e $\sigma_2\sigma_1(x) = \sigma_2(\sigma_1(x)) = \sigma_1(x) = x$, in particolare $\sigma_1\sigma_2(x) = \sigma_2\sigma_1(x)$.

Se $x \in A$ allora $\sigma_1(x) \in A$ e quindi $\sigma_2(\sigma_1(x)) = \sigma_1(x)$ (si ricordi che σ_2 lascia fissi gli elementi non in B). E analogamente $\sigma_2(x) = x$ e quindi $\sigma_1(\sigma_2(x)) = \sigma_1(x)$. Anche in questo caso si ha che $\sigma_1\sigma_2(x) = \sigma_2\sigma_1(x)$.

Completamente analoga è la verifica che se $x \in B$ allora $\sigma_1\sigma_2(x) = \sigma_2\sigma_1(x)$. In altre parole $\sigma_1\sigma_2(x) = \sigma_2\sigma_1(x)$ per ogni $x \in \{1, \ldots, n\}$, ossia $\sigma_1\sigma_2 = \sigma_2\sigma_1$. ❏

Teorema 9.8 (decomposizione in cicli) *Ogni permutazione di S_n si decompone nel prodotto di cicli disgiunti. Tale decomposizione è unica a meno dell'ordine dei cicli.*

Osservazione 9.9 Ogni ciclo si scrive come prodotto di trasposizioni, si osservi infatti che $(a_1\ a_2 \ldots a_k) = (a_1\ a_k)(a_1 a_{k-1}) \ldots (a_1\ a_3)(a_1\ a_2)$.

Corollario 9.10 *Ogni permutazione si scrive come prodotto di trasposizioni.*

Dim. Segue immediatamente dal teorema e dall'osservazione precedenti (9.8 e 9.9). ❏

Lezione 10 (22 marzo 1999 h. 9.30-10.30)

Dimostrazione del Teorema di decomposizione in cicli disgiunti (9.8)

Dim. Se $\sigma(i) = i$ per ogni $i = \{1, \ldots, n\}$ non c'è nulla da dimostrare. Sia i_1 il primo numero in $\{1, \ldots, n\}$ tale che $\sigma(i_1) \neq i_1$. Scriviamo

$$i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^k(i_1), \sigma^{k+1}(i_1), \ldots$$

dato che le espressioni $\sigma^k(i_1)$ sono infinite, ma i loro valori sono un numero finito, esistono almeno due diversi naturali, $k < m$ tali che $\sigma^k(i_1) = \sigma^m(i_1)$ (i.e. l'applicazione $\mathbb{N} \to \{1, 2, \ldots, n\}$, $k \mapsto \sigma^k(i_1)$ non può essere iniettiva). Posto $m = k + h$, si ha che $\sigma^k(i_1) = \sigma^k(\sigma^h(i_1))$ e dato che σ^k è bigettiva si ha che $i_1 = \sigma^h(i_1)$. Sia h_1 il primo naturale positivo tale che $i_1 = \sigma^{h_1}(i_1)$.

Si noti che gli elementi $i_1, \sigma(i_1), \ldots, \sigma^{h_1-1}(i_1)$ sono tra loro distinti, infatti se così non fosse si contradirebbe la minimalità di h_1 (si ragioni come si è fatto per mostrare l'esistenza di h_1). Cosideriamo allora il ciclo $\pi_1 = (i_1\ \sigma(i_1) \ldots \sigma^{h_1-1}(i_1))$. Osserviamo che se $x \in \{i_1, \sigma(i_1), \ldots, \sigma^{h_1-1}(i_1)\}$ allora $\sigma(x) = \pi_1(x)$.

Se $\sigma(x) = x$ per ogni $x \notin \{i_1, \sigma(i_1), \ldots, \sigma^{h_1-1}(i_1)\}$ allora $\sigma(x) = \pi_1(x)$ per ogni x e quindi abbiamo finito, altrimenti sia i_2 il primo elemento per cui $\sigma(i_2) \neq i_2$ e $i_2 \notin \{i_1, \sigma(i_1), \ldots, \sigma^{h_1-1}(i_1)\}$ e sia h_2 il minimo intero positivo per cui $i_2 = \sigma^{h_2}(i_2)$ e sia $\pi_2 = (i_2\ \sigma(i_2) \ldots \sigma^{h_2-1}(i_2))$.

Si osservi che $\{i_1, \sigma(i_1), \ldots, \sigma^{h_1-1}(i_1)\} \cap \{i_2, \sigma(i_2), \ldots, \sigma^{h_2-1}(i_2)\} = \varnothing$ e che se $x \in \{i_1, \sigma(i_1), \ldots, \sigma^{h_1-1}(i_1)\} \cup \{i_2, \sigma(i_2), \ldots, \sigma^{h_2-1}(i_2)\}$ allora $\sigma(x) = \pi_1\pi_2(x)$. Il procedimento si può evidentemente iterare costruendo ad ogni passo un ciclo che è disgiunto da tutti i precedenti e che agisce come σ sul suo supporto.

Dato che stiamo lavorando sull'insieme finito $\{1, 2, \ldots, n\}$, tale procedimente deve terminare, producendo la decomposizione cercata.

L'unicità di tale decomposizione osservando che se $\sigma = \pi_1 \ldots \pi_k$ con π_i cicli a due a due disgiunti, allora i cicli determinati dal procedimento precedente sono proprio i π_i, eventualmente dati in ordine diverso. $\square$

Osservazione 10.1 La dimostrazione della proposizione precedente fornisce un algoritmo per determinare in modo effettivo la decomposizione in cicli di una permutazione.

Segno di una permutazione

Definizione 10.2 *Sia $\sigma \in S_n$, definiamo* segno *di σ il numero*

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{s}(l(\pi_i)-1)} \tag{10}$$

dove $\sigma = \pi_1\pi_2 \ldots \pi_s$ è la decomposizione in cicli disgiunti e $l(\pi_i)$ è la lunghezza del ciclo π_i.

Proposizione 10.3 *Se $\sigma, \tau \in S_n$ allora*

$$\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2) \tag{11}$$

Dim. Osserviamo innanzitutto che dalla definizione segue immediatamente che se τ è una trasposizione allora $\varepsilon(\tau) = -1$.

Supponiamo di sapere che la formula (11) valga quando σ_2 è una trasposizione, ossia che:

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = -\varepsilon(\sigma) \quad \text{per ogni trasposizione } \tau \tag{12}$$

Usando questo fatto, osserviamo allora che se $\sigma = \tau_1\tau_2\ldots\tau_k$ è una decomposizione come prodotto di trasposizioni, si ha

$$\varepsilon(\sigma) = \varepsilon(\tau_1\ldots\tau_n) = -\varepsilon(\tau_1\ldots\tau_{n-1}) = (-1)^2\varepsilon(\tau_1\ldots\tau_{n-2}) = \ldots = (-1)^k \tag{13}$$

Se ora $\sigma_2 = \tau_1\ldots\tau_k$ è una decomposizione in prodotto di trasposizioni, procedendo esattamente come sopra, si ha:

$$\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1\tau_1\ldots\tau_k) = -\varepsilon(\sigma_1\tau_1\ldots\tau_{k-1}) = \ldots = (-1)^k\varepsilon(\sigma_1)$$

e quindi, usando la (13), $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$.

Resta da dimostrare la (12), che viene lasciata per esercizio (non facile). $\square$

Esercizio 10.1 Si osservi che se $(a\ a_1\ldots a_k)$ e $(b\ b_1\ldots b_h)$ sono cicli disgiunti e $(a\ a_1\ldots a_k\ b\ \ b_1\ldots b_h)$ è un ciclo, allora risulta:

$$\begin{array}{rcl}(a\ a_1\ldots a_k\ b\ b_1\ldots b_h)(a\ b) & = & (a\ b_1\ldots b_h)(b\ a_1\ldots a_k)\\ (a\ a_1\ldots a_k)(b\ b_1\ldots b_h)(a\ b) & = & (a\ b_1\ \ldots b_h\ b\ a_1\ldots a_k)\end{array}$$

Si usi questo fatto per provare la (12) nella dimostrazione della proposizione precedente.

Osservazione 10.4 La formula (13) mostra che data una permutazione, il numero di trasposizioni che costituiscono una sua decomposizione deve essere sempre pari o sempre dispari, a secondo che il segno della peremutazione sia 1 oppure -1. Una permutazione sarà detta *pari* se il suo segno è 1, sarà detta *dispari* se il suo segno è -1.

Sottogruppo generato

Proposizione 10.5 *Sia G un gruppo, e siano $\{H_\lambda\}_{\lambda\in\Lambda}$ una famiglia di sottogruppi di G. Allora $\bigcap_{\lambda\in\Lambda} H_\lambda$ è un sottogruppo di G.*

Dim. Indichiamo con $H = \bigcap H_\lambda$. Se $h_1, h_2 \in H$ allora per ogni λ $h_1, h_2 \in H_\lambda$ e poiché questi sono tutti sottogrupi, $h_1 h_2 \in H_\lambda$ per ogni λ ovvero $h_1 h_2 \in H$. (È verificata la (1) della definizione di sottogruppo (8.9)).

Ogni H_λ è un sottogruppo, quindi $1 \in H_\lambda$ per ogni λ e pertanto $1 \in H$ (È verificata la (2) della definizione di sottogruppo (8.9)).

Sia $h \in H$ allora $h \in H_\lambda$ per ogni λ. Essendo gli H_λ dei sottogruppi $h^{-1} \in H_\lambda$ per ogni λ ovvero $h^{-1} \in H$ (È verificata la (3) della definizione di sottogruppo (8.9)). ❑

Osservazione 10.6 I tre passi della dimostrazione precedente, presi uno alla volta, mostrano che la proposizione rimane vera se nell'enunciato si sostituiscono le parole gruppo e sottogruppo con semigruppo e sottosemigruppo oppure con monoide e sottomonoide

Definizione 10.7 *Sia G un gruppo e sia $S \subseteq G$ denoteremo con $\langle S\rangle$ il più piccolo sottogruppo di G che contiene S. Ossia $\langle S\rangle$ è un sottogruppo con le seguenti due proprietà:*

1. *$S \subseteq \langle S\rangle$,*
2. *se H è un sottogruppo di G e $S \subseteq H$ allora $\langle S\rangle \subseteq H$.*

$\langle S\rangle$ si chiama sottogruppo generato *da S.*

Proposizione 10.8 *Se S è un sottinsieme di G, il sottogruppo generato da S esiste ed è unico. E risulta:*

$$\langle S\rangle = \bigcap_{S \subseteq H \leq G} H$$

ossia $\langle S\rangle$ è l'intersezione di tutti i sottogruppi di G che contengono S.

Dim. Osserviamo che $\bigcap_{S \subseteq H \leq G} H$ è un sottogruppo (per la proposizione 10.5) e d'altra parte se $S \subseteq H_0 \leq G$ allora $\bigcap_{S \subseteq H \leq G} H \subseteq H_0$, ossia $\bigcap_{S \subseteq H \leq G} H$ verifica le 1 e 2 della definizione di sottogruppo generato (10.7).

Che il sottogruppo generato sia unico segue dal fatto che se H_1 e H_2 verificano le 1 e 2 della definizione di sottogruppo generato (10.7) allora necessariamente $H_1 \subseteq H_2$ (H_1 è minimo e H_2 è un sottogruppo che contiene S) e, scambiando i ruoli di H_1 e H_2, anche $H_2 \subseteq H_1$. ❑

Osservazione 10.9 La definizione di sottogruppo generato si generalizza immediatamente al caso di monoidi e semigruppi, e la sua esistenza ed unicità si dimostra esattamente nello stesso modo.

Osservazione 10.10 Sia T l'insieme delle trasposizioni di S_n. Il corollario 9.10 ci dice allora che $\langle T\rangle = S_n$.

Lezione 11 (24 marzo 1999 h. 9.30-10.30)

Definizione di ordine

Definizione 11.1 *Sia G un gruppo finito si chiama* ordine *di G il numero dei suoi elementi, e si denota con $o(G)$. Se $g \in G$ chiamiamo* ordine *il numero $o(g) = o(\langle g \rangle)$.*

Esercizio 11.1 Si provi che $g^{o(g)} = 1$.

Esercizio 11.2 Si provi che se $o(g) = \min\{n \in \mathbb{N} \mid n > 0 \text{ e } g^n = 1\}$.

Definizione di classe laterale

Definizione 11.2 *Sia G un gruppo $H \leq G$ e $g \in G$ si chiama* classe laterale sinistra *l'insieme*

$$gH = \{gh \mid h \in H\}.$$

Si chiama classe laterale destra *l'insieme*

$$Hg = \{hg \mid h \in H\}.$$

Relazione d'equivalenza indotta da un sottogruppo

Siano $H \leq G$ e si consideri la relazione

$$g_1 \stackrel{H}{\sim} g_2 \iff \exists h \in H \text{ t.c. } g_2 = g_1 h \qquad (14)$$

Osservazione 11.3 Se $g_1 \stackrel{H}{\sim} g_2$ allora $g_1 = g_2 h$ per qualche $h \in H$, e quindi $g_1^{-1} g_2 = h \in H$. Viceversa se $g_2^{-1} g_1 \in H$ allora $g_1^{-1} g_2 = h$ per qualche $h \in H$ e quindi $g_2 = g_1 h$. Ossia $g_1 \stackrel{H}{\sim} g_2$ se e solo se $g_1^{-1} g_2 \in H$.

Proposizione 11.4 $\stackrel{H}{\sim}$ *è una relazione d'equivalenza, e per ogni $g \in G$ si ha che $[g]_{\stackrel{H}{\sim}} = gH$.*

Dim. $\stackrel{H}{\sim}$ è riflessiva. Dato che H è un sottogruppo, $1 \in H$ e dato che $g = gi$ si ha che $g \stackrel{H}{\sim} g$ per ogni $g \in G$.

$\stackrel{H}{\sim}$ è simmetrica Sia $g_1 \stackrel{H}{\sim} g_2$ ossia esiste $h \in H$ tale che $g_2 = g_1 h$, ma allora, moltiplicando a destra per h^{-1} si ottiene che $g_2 h^{-1} = g_1 h h^{-1} = g_1 1 = g_1$ e dato che H è un sottogruppo $h^{-1} \in H$ e quindi $g_2 \stackrel{H}{\sim} g_1$.

$\stackrel{H}{\sim}$ è transitiva. Siano $g_1 \stackrel{H}{\sim} g_2$ e $g_2 \stackrel{H}{\sim} g_3$ ovvero $g2 = g_1 h_1$ e $g_3 = g_2 h_2$ con $h_1, h_2 \in H$. Sostituendo la prima nella seconda si ottiene che $g_3 = g_1 h_1 h_2$ e dao che H è un sottogruppo $h^{-1} \in H$ e quindi $g_3 \stackrel{H}{\sim} g_1$.

Che $[g]_{\stackrel{H}{\sim}} = gH$ segue immediatamente dalla definizione di classe laterale e dalla definizione di classe d'equivalenza (7.1). ❑

L'insieme quoziente $G/_{\underset{\sim}{H}}$ si denota semplicemente con $G/_H$ e si chiama il *quoziente di G modulo H.*

Corollario 11.5 *Le classi laterali sinistre gH costituiscono una partizione di G.*

Dim. Segue immediatamente dalla proposizione precedente e dall'analoga proprietà dimostrata in generale per le classi di una relazione d'equivalenza qualsiasi (osservazione 7.7). $\square$

Il teorema di Lagrange

Lemma 11.6 *Sia $H \leq G$ e sia $g \in G$. Gli insiemi H e gH sono in bigezione.*

Dim. Si consideri l'applicazione $\varphi : H \to gH$ definita da $\varphi(h) = gh$. L'applicazione è surgettiva per definizione di classe laterale. Dimostriamo che è anche iniettiva. Se $\varphi(h_1) = \varphi(h_2)$ allora $gh_1 = gh_2$ e quindi, moltiplicando a sinistra per g^{-1} si ottiene

$$h_1 = 1h_1 = g^{-1}gh_1 = g^{-1}gh_2 = 1h_2 = h_2.$$

$\square$

Osservazione 11.7 La proprietà dei gruppi usata nella dimostrazione precedente, ossia che

$$gg_1 = gg_2 \Rightarrow g_1 = g_2$$

è nota con il nome di *legge di cancellazione sinistra* (l'analoga ottenuta moltiplicando a destra si chiama *legge di cancellazione destra*). Si osservi che in generale questa non vale nei monoidi, ad esempio in $(\mathbb{Z}, \cdot)$ si ha che $0 \cdot 1 = 0 \cdot 2$ ma $1 \neq 2$

Teorema 11.8 (Lagrange) *Siano G un gruppo finito e $H \leq G$. Allora*

$$o(H) \big| o(G).$$

Dim. Dal lemma precedente segue che le classi laterali di H hano tutte lo stesso numero di elementi pari ad $o(H)$, quindi, detto k il numero di classi laterali (ossia il numero di elementi del quoziente $G/_H$), dato che queste sono una partizione, si ha che $o(G) = ko(H)$ e quindi la tesi. $\square$

Definizione di sottogruppo normale

Definizione 11.9 *Un sottogruppo $H \leq G$ si dice* normale *se per ogni $g \in G$ si ha che $gH = Hg$. Per indicare che H è un sottogruppo normale di G si scriverà anche $H \trianglelefteq G$.*

Osservazione 11.10 Se G è commutativo e $H \leq G$ allora dalla definizione di classe laterale (11.2) segue immediatamente che $gH = Hg$ per ogni $g \in G$ e quindi ogni sottogruppo di un gruppo commutativo è normale.

Comunque in generale, esistono sottogruppi non normali. Si consideri ad esempio $H = \langle(1\ 2)\rangle \leq S_3$. Semplici calcoli mostrano che

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

e quindi H non è normale.

Lezione 12 (25 marzo 1999 h. 10.30-11.30)

Criteri di normalità

Proposizione 12.1 *Sia G un gruppo e $H \leq G$. Le seguenti proposizioni sono equivalenti:*

1. *H è normale*
2. *$\forall g \in G, h \in H \quad g^{-1}hg \in H$*
3. *$\forall g \in G \quad g^{-1}Hg = H$ (dove $g^{-1}Hg$ denota l'insieme $\{g^{-}1hg \mid h \in H\}$).*

Dim. (1) $\Rightarrow$ (2). Siano $g \in G$ e $h \in H$ allora $hg \in Hg$. Dato che H è normale, $Hg = gH$, quindi $hg \in gH$ ossia esiste $h' \in H$ tale che $hg = gh'$, da cui, moltiplicando a sinistra per g^{-1}, $g^{-1}hg = h' \in H$.
(2) $\Rightarrow$ (3). La (2) implica immediatamente (per definizione) che $g^{-1}HG \subseteq H$. Proviamo l'inclusione opposta. Sia $h \in H$, usando la (2) e il risultato dell'esercizio 8.2, si ha che $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h' \in H$, ma allora $h = g^{-1}ghg^{-1}g = g^{-1}h'g \in g^{-1}Hg$.
(3) $\Rightarrow$ (1). Se $h \in H$ allora per la (2) esiste h' tale che $h = g^{-1}hg$, ma allora $gh = h'g \in Hg$, ovvero $gH \subseteq Hg$. Analogamente, sempre per (2), si ha che anche $Hg \subseteq gH$. ❑

Defnizione dell'operazione sui quozienti

Sia $H \leq G$ si vuole definire un'operazione su $G/_H$. Viene naturale cercare di definire un operazione nel modo seguente:

$$g_1Hg_2H = (g_1g_2)H \quad \forall g_1H, g_2H \in G/_H \tag{15}$$

Questa formula definisce una operazione se e solo se

$$\left.\begin{array}{l} g_1H = g_1'H \\ g_2H = g_2'H \end{array}\right\} \Rightarrow (g_1g_2)H = (g_1'g_2')H$$

ossia se e solo se

$$\left.\begin{array}{l} g_1 \overset{H}{\sim} g_1' \\ g_2 \overset{H}{\sim} g_2' \end{array}\right\} \Rightarrow g_1g_2 \overset{H}{\sim} g_1'g_2' \tag{16}$$

Teorema 12.2 *Vale la (16) se e solo se H è un sottogruppo normale.*

Dim. Supponiamo che H sia normale. Se $g_1 \overset{H}{\sim} g_1'$ e $g_2 \overset{H}{\sim} g_2'$ allora esistono $h_1, h_2 \in H$ tali che $g_1' = g_1h_1$ e $g_2' = g_2h_2$. Quindi:

$$(g_1g_2)^{-1}g_1'g_2' = g_2^{-1}g_1^{-1}g_1'g_2' = g_2^{-1}g_1^{-1}g_1h_1g_2h_2 == g_2^{-1}h_1g_2h_2 \in H$$

in quanto $g_2^{-1}h_1g_2 \in H$ per la condizione (2) di proposizione 12.1.

Supponiamo che valga (16). Sia $g \in G$ e $h \in H$. Dato che $g \overset{H}{\sim} g$ e $h \overset{H}{\sim} 1$ si ha che $hg \overset{H}{\sim} 1g$ e quindi esiste h_1 tale che $hg = gh_1$ da cui $g^{-1}hg = h_1 \in H$, per la condizione (2) di proposizione 12.1 si ha allora che H è normale. ❑

Proposizione 12.3 *Se $H \trianglelefteq G$, allora $G/_H$ dotato dell'operazione definita in (15) è un gruppo*

Dim. L'operazione è associativa. Infatti

$$\begin{aligned}(g_1Hg_2H)g_3H &= (g_1g_2)Hg_3H = ((g_1g_2)g_3)H = \\ &= (g_1(g_2g_3))H = g_1H(g_2g_3)H = g_1H(g_2Hg_3H)\end{aligned}$$

$G/_H$ possiede una unità sinistra e destra. Infatti

$$gH1H = (g1)H = gH = (1g)H = 1HgH$$

Ogni elemento di $G/_H$ è invertibile a sinistra e a destra.

$$gHg^{-1}H = (gg^{-1})H = 1H = (g^{-1}g)H = g^{-1}HgH.$$

❑

Definizione di morfismo

Definizione 12.4 *Siano G e G' due gruppi. Un'applicazione $\varphi : G \to G'$ è detta un* morfismo *se*

$$\forall g_1, g_2 \in G \quad \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2).$$

Osservazione 12.5 Se $H \trianglelefteq G$ allora la proiezione a quoziente $\pi : G \to G/_H$, $\pi(g) = gH$ è un morfismo. O meglio la definizione dell'operazione (15) è data in modo da far sì che la proiezione risulti un morfismo.

Esempio 12.6 Si consideri l'applicazione $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot)$ definita da $\exp(x) = e^x$. exp è un morfismo, infatti

$$\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \cdot \exp(y)$$

Lezione 13 (31 marzo 1999 h. 9.30-11.30)

Prime proprietà dei morfismi

Proposizione 13.1 *Sia $\varphi : G \to G'$ un morfismo, allora:*

1. $\varphi(1_G) = 1_{G'}$
2. *$\forall g \in G$ si ha $\varphi(g^{-1}) = (\varphi(g))^{-1}$.*

Dim. $1_G = 1_G 1_G$ e quindi $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$. Moltiplicando a sinistra per l'inverso di $\varphi(1_G)$ segue che $\varphi(1_G) = 1_{G'}$.

$1_G = gg^{-1}$ e quindi $1_{G'} = \varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}$. Moltiplicando entrambi i membri a sinistra per $(\varphi(g))^{-1}$ si ottiene $(\varphi(g))^{-1} = \varphi(g^{-1})$. ❑

Esempio 13.2 Proseguiamo l'esempio 12.6. Le conclusioni della proposizione precedente sono in questo caso le ben note relazioni:

$$\begin{aligned} \exp(0) &= e^0 = 1 \\ \exp(-x) &= e^{-x} = \frac{1}{e^x} = \frac{1}{\exp(x)} \end{aligned}$$

Isomorfismi

Definizione 13.3 *Un morfismo di gruppi si dice un* isomorfismo *se è bigettivo.*

Proposizione 13.4 *Se $\varphi : G \to G'$ è un isomorfismo, allora anche φ^{-1} è un morfismo.*

Dim. Siano $g'_1, g'_2 \in G'$, e chiamiamo $g_1 = \varphi^{-1}(g'_1)$ e $g_2 = \varphi^{-1}(g'_2)$. Dato che φ è un morfismo

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = g'_1 g'_2$$

da cui, per l'invertibilità di φ si ha $g_1 g_2 = \varphi^{-1}(g'_1 g'_2)$, che è la tesi. ❑

Esempio 13.5 Il morfismo exp dell'esempio 12.6 è invertibile, quindi è un isomorfismo. La sua inversa è l'applicazione logaritmo $\log : \mathbb{R}_+ \to \mathbb{R}$, che, in accordo con la proposizione precedente, risulta essere anch'essa un morfismo:

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

Nucleo di un morfismo

Definizione 13.6 *Sia $\varphi : G \to G'$ un morfismo, si chiama* nucleo *di φ l'insieme*

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1\}.$$

Proposizione 13.7 *Se φ è un morfismo allora $\ker \varphi$ è un sottogruppo normale.*

Dim. La 1 della proposizione 13.1, garantisce che $i \in \ker \varphi$, e quindi $\ker \varphi \neq \varnothing$.

Siano $k_1, k_2 \in \ker(\varphi)$, allora, usando la 2 di proposizione 13.1 ed il fatto che $\varphi(k_1) = \varphi(k_2) = 1$,

$$\varphi(k_1 k_2^{-1}) = \varphi(k_1)\varphi(k_2^{-1}) = \varphi(k_1)(\varphi(k_2))^{-1} = 11^{-1} = 1$$

ossia $k_1 k_2^{-1} \in \ker(\varphi)$. Per il criterio del sottogruppo (proposizione 8.10) si ha che $\ker \varphi$ è un sottogruppo.

Sia ora $k \in \ker(\varphi)$ e $g \in G$, allora $\varphi(g^{-1}kg) = \varphi(g)^{-1}\varphi(k)\varphi(g) = 1$, e quindi, per la proposizione 12.1, $\ker(\varphi)$ è normale. ❏

Proposizione 13.8 *Un morfismo φ è iniettivo se e solo se $\ker \varphi = \langle 1 \rangle$.*

Dim. Se φ è iniettivo, allora necessariamente $\ker(\varphi)$ ha un solo elemento (si troverebbero altrimenti due elementi distinti aventi per immagine 1) e poiché $1 \in \ker(\varphi)$ si ha che $\ker(\varphi) = \langle 1 \rangle$.

Viceversa siano $g_1, g_2 \in G$ tali che $\varphi(g_1) = \varphi(g_2)$, allora

$$\varphi(g_2^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1) = \varphi(g_1)^{-1}\varphi(g_1) = 1$$

quindi $g_2^{-1}g_1 \in \ker(\varphi) = \langle 1 \rangle$ e quindi $g_2^{-1}g_1 = 1$ da cui $g_1 = g_2$. ❏

Osservazione 13.9 Nella dimostrazione precedente si è provato che se $\varphi(g_1) = \varphi(g_2)$ allora $g_2^{-1}g_1 \in \ker(\varphi)$. Evidentemente vale anche il viceversa, in quanto se $g_2^{-1}g_1 \in \ker(\varphi)$ allora

$$1 = \varphi(g_2^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1)$$

da cui $\varphi(g_1) = \varphi(g_2)$. In altre parole la relazione d'equivalenza (definita nell'esercizio 7.2) $\overset{\varphi}{\sim}$, indotta da φ, coincide con la relazione d'equivalenza (si veda l'osservazione 11.3) $\overset{K}{\sim}$, indotta dal sottogruppo $K = \ker(\varphi)$. Quindi gli insiemi $G/_{\overset{\varphi}{\sim}}$ e $G/_K$ coincidono.

Primo teorema di omomorfismo

Teorema 13.10 (primo teorema di omomorfismo) *Sia $\varphi : G \to G'$ un morfismo. Allora esiste un unico morfismo di gruppi $\widetilde{\varphi} : G/_{\ker\varphi} \to G'$ tale che $\varphi = \widetilde{\varphi} \circ \pi$.*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ G/_{\ker\varphi} \arrow[ur, "\widetilde{\varphi}"'] & \end{tikzcd} \tag{17}$$

Si ha inoltre che:

1. *$\widetilde{\varphi}$ è iniettiva;*
2. *$\widetilde{\varphi}$ è surgettiva se e solo se φ è surgettiva.*

Dim. Per quanto osservato precedentemente (13.9), l'esistenza di una unica applicazione che faccia commutare il diagramma (17), e che tale applicazione verifichi le condizioni 1 e 2, è garantita dal teorema di omomorfismo per insiemi (teorema 7.8). Per avere la tesi, dobbiamo soltanto mostrare che tale applicazione è un morfismo, ossia che $\widetilde{\varphi}(g_1Hg_2H) = \widetilde{\varphi}(g_1H)\widetilde{\varphi}(g_2H)$. Ma, usando la commutatività del diagramma (17), ed il fatto osservato precedentemente (osservazione 12.5), che π è un morfismo, si ha:

$$\begin{aligned} \widetilde{\varphi}(g_1Hg_2H) &= \widetilde{\varphi}(\pi(g_1)\pi(g_2)) = \widetilde{\varphi}(\pi(g_1g_2)) = \varphi(g_1g_2) \\ &= \varphi(g_1)\varphi(g_2) = \widetilde{\varphi}(\pi(g_1))\widetilde{\varphi}(\pi(g_2)) = \widetilde{\varphi}(g_1H)\widetilde{\varphi}(g_2H) \end{aligned}$$

che è la tesi. ❑

Osservazione 13.11 Si osservi che, dato che $\widetilde{\varphi}$ è sempre iniettiva, allora se φ è surgettiva, la $\widetilde{\varphi}$ risulta essere bigettiva e quindi un isomorfismo.

Classificazione dei gruppi ciclici

Definizione 13.12 *Un gruppo G è detto* ciclico *se esiste $g \in G$ tale che $G = \langle g \rangle$. Un tale elemento g viene chiamato un* generatore *di G.*

Esempio 13.13 $\mathbb{Z}$ è un gruppo ciclico. Per ogni $n \in \mathbb{N}$, $n \geq 1$, il gruppo $\mathbb{Z}/_{n\mathbb{Z}}$ è ciclico e $o(\mathbb{Z}/_{n\mathbb{Z}}) = n$.

Esercizio 13.1 Si provi che se $G = \langle g \rangle$ allora $G = \{g^n \mid n \in \mathbb{Z}\}$.

Proposizione 13.14 *Sia G un gruppo ciclico, allora*

$$G \cong \left\langle \begin{array}{ll} \mathbb{Z} & \text{se } G \text{ è infinito} \\ \mathbb{Z}/_{n\mathbb{Z}} & \text{se } o(G) = n \geq 1 \end{array} \right.$$

Dim. Sia g un generatore di G, e si consideri l'applicazione $\varphi : \mathbb{Z} \to G$ definita da $\varphi(h) = g^h$. Il fatto che (cfr. esercizio (8.6) $g^(h+k) = g^h g^k$, per ogni $h, k \in \mathbb{Z}$ mostra che φ è un morfismo. D'altra parte, dato che g è un generatore di G, φ è surgettivo, ma allora per quanto osservato (osservazione 13.11), G è isomorfo a $\mathbb{Z}/_{\ker\varphi}$. D'altra parte i sottogruppi di $\mathbb{Z}$ sono tutti e soli (vedi esercizio 8.5) della forma $n\mathbb{Z}$ con $n \geq 0$, quindi G è isomorfo o a $\mathbb{Z} \cong \mathbb{Z}/_{0\mathbb{Z}}$, e ciò si ha solo se G è infinito, oppure $G \cong \mathbb{Z}/_{n\mathbb{Z}}$ ed in tal caso $o(G) = n$. ❑

Osservazione 13.15 La proposizione precedente mostra che, a meno di isomorfismo, quelli dati nell'esempio sono tutti e soli i gruppi ciclici.

Esercizio 13.2 Si dimostri che se $\varphi : G \to G'$ è un morfismo di gruppi, allora se $H' \leq G'$ allora $\varphi^{-1}(H') \leq G$. Se H' è normale, allora anche $\varphi^{-1}(H')$ è normale.

Esercizio 13.3 Si dimostri che se $\varphi : G \to G'$ è un morfismo di gruppi e $H \leq G$ allora $\varphi(H) \leq G'$. È vero che se H è normale allora anche $\varphi(H)$ è normale?

Lezione 14 (12 aprile 1999 h. 9.30-10.30)

Definizione di anello

Definizione 14.1 *Si chiama* anello *una terna* $(R, +, \cdot)$ *dove* R *è un insieme e* $+, \cdot$ *sono due operazioni su* R *tali che:*

1. $(G, +)$ *è un gruppo commutativo*
2. $(G, \cdot)$ *è un semigruppo*
3. *per ogni* $a, b, c \in R$ *si ha* $a(b + c) = ab + ac$ *e* $(b + c)a = ba + ca$.

Le due proprietà del punto 3 si dicono proprietà distributive *a sinistra e a destra. L'elemento neutro della somma sarà denotato con* 0 *e l'inverso di* a *per la somma sarà denotato con* $-a$. *Per brevità si scriverà* $a - b$ *invece di* $a + (-b)$.

Un anello si dice commutativo *se l'operazione* $\cdot$ *è commutativa. Si dice che* R *è un* anello con identità *se esiste un elemento non nullo che sia neutro per* $\cdot$ *(i.e.* $(R, \cdot)$ *è un monoide). Tale elemento neutro, che è unico (proposizione 8.3) è detto l'*identità *dell'anello e denotato con* 1.

Esercizio 14.1 Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ dotati delle usuali operazioni di somma e prodotto sono tutti anelli commutativi con identità.

Le classi di resto modulo n con le operazioni di somma e prodotto definite nell'osservazione 6.9 è un anello commutativo con identità.

Il prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}$ con le operazioni $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ e $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$ è un anello commutativo con identità.

L'insieme delle matrici $n \times n$ a coefficienti reali è un anello, in generale non commutativo (è commutativo se e solo se $n = 1$.

Esercizio 14.2 Sia R un anello e X un insieme, si provi che R^X con le operazioni definite da

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

è un anello. Se R è commutativo, anche R^X lo è, se R ha un'identità, anche R^X ne ha una.

Prime proprietà degli anelli

Proposizione 14.2 *Sia R un anello, allora*

1. *per ogni $a \in R$ si ha $a0 = 0a = 0$.*
2. *per ogni $a, b \in R$ si ha $a(-b) = (-a)b = -(ab)$*

Dim. Sia $a \in R$, allora $a0 = a(0+0)$, usando la proprietà distributiva si ha allora $a(0+0) = a0 + a0$ e quindi, $a) = a0 + a0$. Dato che R è un gruppo rispetto alla somma, vale la legge di cancellazione (osservazione 11.7) e quindi $0 = a0$. In modo del tutto analogo si prova che $0a = 0$.

Siano $a, b \in R$, allora usando quanto appena dimostrato e la proprietà distributiva si ha che $0 = a0 = a(b+(-b)) = ab + a(-b)$, da cui $-(ab) = a(-b)$. Analogamente si prova che $(-a)b = -(ab)$. ❏

Sottoanelli

Definizione 14.3 *Sia R un anello, un sottinsieme $S \subseteq R$ sarà detto un* sottoanello *se è contemporaneamente un sottogruppo di $(R,+)$ e un sottosemigruppo di $(R,\cdot)$. Se R è un anello con identità, si richiede anche che $1 \in S$. In altre parole:*

1. *$a, b \in S \Rightarrow a - b \in S$*
2. *$a, b \in S \Rightarrow ab \in S$*
3. *$1 \in R \Rightarrow 1 \in S$.*

Divisori di zero e unità

Definizione 14.4 *Un elemento $a \in R$ è detto un* divisore di 0 *se $a \neq 0$ ed esiste $b \in R$, $b \neq 0$ tale che $ab = 0$ oppure $ba = 0$.*

Un anello commutativo con identità che non contiene divisori di zero viene detto un dominio di integrità.

Definizione 14.5 *Sia R un anello con identità. Un elemento $u \in R$ sarà detto una* unità *se è invertibile (definizione 8.5) rispetto al prodotto, ossia se esiste $v \in R$ tale che $uv = vu = 1$. Tale elemento v se esiste è unico (proposizione 8.6) e viene denotato con u^{-1}.*

Esempio 14.6 La matrice $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ è un divisore di 0 nell'anello delle matrici 2×2. Infatti

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Tutte le coppie del tipo $(a, 0)$ sono dei divisori di 0 nell'anello $\mathbb{Z} \times \mathbb{Z}$, infatti $(a, 0)(0, b) = (0, 0)$ per ogni $a, b \in \mathbb{Z}$, quindi $\mathbb{Z} \times \mathbb{Z}$ non è un dominio di integrità.

Le unità di $\mathbb{Z}$ sono soltanto $1, -1$. Le unità di $\mathbb{Z} \times \mathbb{Z}$ sono $(1, 1)$, $(1, -1)$, $(-1, -1)$ e $(-1, 1)$.

Esercizio 14.3 Si provi che $[a] \in \mathbb{Z}\big/_{n\mathbb{Z}}$ è una unità se e solo se il massimo comun divisore $(a, n) = 1$.

Esercizio 14.4 Si provi che $[a] \in \mathbb{Z}\big/_{n\mathbb{Z}} - \{[0]\}$ è un divisore di 0 se e solo se $(a, n) \neq 1$.

Proposizione 14.7 *L'insieme degli elementi invertibili di un anello con identità R, è un gruppo con l'operazione prodotto. Tale gruppo viene denotato con R^* ed è chiamato il* gruppo delle unità *di R.*

Dim. Indichiamo con $R^* = \{u \in R \mid u \text{ è invertibile}\}$. Se $u, v \in R^*$ allora esistono u^{-1} e $v^{-1} \in R$ tali che $uu^{-1} = u^{-1}u = vv^{-1} = v^{-1}v = 1$, ma allora $(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = u1u^{-1} = uu^{-1} = 1$ e analogamente anche $(v^{-1}u^{-1})(uv) = 1$, quindi uv è una unità ovvero $uv \in R^*$.

Evidentemente $1 \in R^*$ e se u è una unità anche u^{-1} lo è, quindi la tesi. ❑

Esercizio 14.5 Si confronti la dimostrazione della proposizione precedente con la soluzione dell'esercizio 8.4 e si spieghi perché sono "così simili".

Osservazione 14.8 Lo 0 non è mai invertibile, dato che $0x = 0 \neq 1$ per ogni $x \in R$.

Corpi

Definizione 14.9 *Un anello con identità viene detto un* corpo *se ogni suo elemento diverso da 0 è invertibile. Un corpo viene detto un* campo *se è commutativo.*

Lemma 14.10 *Sia R un anello con identità, e sia $u \in R$ una unità. Allora u non è un divisore di 0.*

Dim. Sia u una unità e sia b tale che $ub = 0$, allora $b = u^{-1}ub = u^{-1}0 = 0$, e quindi u non è un divisore di 0. ❑

Corollario 14.11 *In un corpo non ci sono divisori di* 0*, e quindi ogni campo è un dominio di integrità.*

Dim. Ogni elemento diverso da 0 di un corpo è invertibile, e, per quanto appena visto, gli elementi invertibili non sono divisori di zero. ❏

Esercizio 14.6 Si provi che $\mathbb{Z}/_{n\mathbb{Z}}$ è un campo se e solo se n è primo.

Esercizio 14.7 Si provi che il gruppo delle unità di $\mathbb{Z}$ è isomorfo a $\mathbb{Z}/_{2\mathbb{Z}}$.

Lezione 15 (14 aprile 1999 h. 9.30-10.30)

Definizione di morfismo di anelli

Definizione 15.1 *Siano* R, R' *anelli, una applicazione* $f : R \to R'$ *sarà detta un* morfismo di anelli *se:*

1. $f(a + b) = f(a) + f(b)$ *(ossia* $f : (R, +) \to (R', +)$ *è un morfismo di gruppi).*

2. $f(ab) = f(a)f(b)$ *(ossia* $f : (R, \cdot) \to (R', \cdot)$ *è un morfismo di semigruppi).*

Se R *ed* R' *sono anelli con identità, diremo che* f *è un* morfismo di anelli con identità *se in più:*

3. $f(1) = 1$, *(ossia* $f : (R, \cdot) \to (R', \cdot)$ *è un morfismo di monoidi).*

Quozienti e ideali

Sia $S \subset R$ un sottogruppo rispetto alla somma. Dato che la somma è commutativa, S è un sottogruppo normale (osservazione 11.10), quindi è definito il gruppo quoziente $G/_S$ in modo che la proiezione a quoziente $\pi : R \to R/_S$ sia un morfismo di gruppi. E precisamente ponendo

$$(a + S) + (b + S) = (a + b) + S. \tag{18}$$

Si vuole definire anche un'altra operazione su $R/_S$ in modo che con tali operazioni risulti un anello e che la proiezione sia un morfismo di anelli. Ossia si vuole che la seguente

$$(a + S)(b + S) = (ab) + S \tag{19}$$

sia una buona definizione.

Osservazione 15.2 Osserviamo che, come nel caso dei gruppi, tale formula definisce effettivamente una operazione se e solo se

$$\left.\begin{array}{c} a + S = a' + S \\ b + S = b' + S \end{array}\right\} \Rightarrow (ab) + S = (a'b') + S$$

ossia se e solo se

$$\left.\begin{array}{c} a \overset{S}{\sim} a' \\ b \overset{S}{\sim} b' \end{array}\right\} \Rightarrow ab \overset{S}{\sim} a'b' \qquad (20)$$

Definizione 15.3 *Si dice che $I \subset R$ è un ideale se:*

1. *I è un sottogruppo di R rispetto alla somma*

2. *per ogni $a \in R$, $s \in I$ si ha che $sa \in I$ e $as \in I$.*

Teorema 15.4 *La (19) è una buona definizione se e solo se S è un ideale.*

Dim. Supponiamo che S sia un ideale e proviamo che allora vale la (20). Infatti se $a \overset{S}{\sim} a'$ e $b \overset{S}{\sim} b'$ allora $a - a' \in S$ e $b - b' \in S$ e quindi esistono $s, t \in S$ tali che $a - a' = s$ e $b - b' = t$, ovvero $a = a' + s$ e $b = b' + s$. Ma allora, usando le proprietà distributive sia a sinistra che a destra, si ha:

$$ab = (a' + s)(b' + t) = a'b' + a't + sb' + st$$

de cui

$$ab - a'b' = a't + sb' + st \in S$$

dato che S è un sottogruppo rispetto alla somma e, per la proprietà (2) della definizione di ideale (15.3), $a't, sb', st \in S$. Quindi $ab \overset{S}{\sim} a'b'$.

Viceversa, supponiamo che la (19) sia una buona definizione, ossia che valga la (20). Allora se $a \in R$ e $s \in S$ si ha che $a \overset{S}{\sim} a$ e $s \overset{S}{\sim} 0$, quindi $as \overset{S}{\sim} a0 = 0$ ossia $as \in S$. Analogamente si prova che anche $sa \in S$. ❑

Teorema 15.5 *$R/_S$ con le operazioni definita da (18) e (19) è un anello e la proiezione a quoziente è un morfismo di anelli.*

Dim. Che $R/_S$ sia un gruppo commutativo rispetto alla somma, segue dai risultati che si hanno per i quozienti di gruppi.

Proviamo che il prodotto è associativo. Siano $a, b, c \in R$, allora

$$\begin{aligned}(a+S)((b+S)(c+S)) &= (a+S)((bc)+S) = (a(bc))+S = ((ab)c)+S = \\ &= ((ab)+S)(c+S) = ((a+S)(b+S))(c+S)\end{aligned}$$

Proviamo ora che vale la proprietà distributiva.Siano $a, b, c \in R$, allora

$$\begin{aligned}(a+S)((b+S)+(c+S)) &= (a+S)((b+c)+S) = (a(b+c))+S = \\ &= (ab+ac)+S = ((ab)+S)+((ac)+S) = \\ &= ((a+S)(b+S))+((a+S)(c+S))\end{aligned}$$

Che la proiezione a quoziente sia un morfismo segue immediatamente dalla definizione. ❑

Nucleo di un morfismo

Definizione 15.6 *Sia $\varphi : R \to R'$ un morfismo di anelli. Si chiama* nucleo *di φ l'insieme* $\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$.

Proposizione 15.7 *Il nucleo di un morfismo è un ideale.*

Dim. Se $\varphi : R \to R'$ è un morfismo di anelli, allora in particolare è un morfismo di gruppi, rispetto alla somma, quindi $\ker\varphi$ è un sottogruppo di R rispetto alla somma (si veda l'analogo risultato per igruppi (proposizione 13.7)).

Siano ora $a \in R$ e $k \in \ker\varphi$, allora $\varphi(k) = 0$ e quindi

$$\varphi(ak) = \varphi(a)\varphi(k) = \varphi(a)0 = 0.$$

ossia $ak \in \ker\varphi$. Allo stesso modo si prova che anche $ka \in \ker\varphi$ e quindi che $\ker\varphi$ è un ideale. ❑

Osservazione 15.8 Osserviamo che se φ è un morfismo di anelli, allora, usando le proprietà dei morfismi di gruppo (proposizione 13.1), $\varphi(a) = \varphi(a')$ se e solo se $\varphi(a) - \varphi(a') = o$ se e solo se $\varphi(a - a') = 0$ se e solo se $a - a' \in \ker\varphi$. Ossia se chiamiamo $K = \ker\varphi$, si ha che la relazione d'equivalenza $\overset{\varphi}{\sim}$ indotta da φ (esercizio 7.2) e la relazione $\overset{K}{\sim}$ indotta dal sottogruppo (osservazione 11.3) (additivo) K

Osservazione 15.9 Quanto visto sopra, ci dice anche che il morfismo φ è iniettivo se e solo se $\ker\varphi = \{0\}$.

Primo teorema di omomorfismo per anelli

Teorema 15.10 (primo teorema di omomorfismo) *Sia $\varphi : R \to R'$ un morfismo di anelli. Allora esiste un unico morfismo di anelli $\widetilde{\varphi} : R/_{\ker\varphi} \to R'$ tale che $\varphi = \widetilde{\varphi} \circ \pi$.*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & R' \\ R/_{\ker\varphi} \arrow[ur, "\widetilde{\varphi}"'] & \end{tikzcd} \tag{21}$$

Si ha inoltre che:

1. *$\widetilde{\varphi}$ è iniettiva;*
2. *$\widetilde{\varphi}$ è surgettiva se e solo se φ è surgettiva.*

Dim. La dimostrazione è sostanzialmente identica a quella dell'analogo teorema per i gruppi (teorema 13.10), in ogni caso la ripetiamo.

L'esistenza di una $\widetilde{\varphi}$ che faccia commutare il diagramma e che verifichi le condizioni (1) e (2), segue dal teorema di omomorfismo per insiemi (teorema

7.8) e dall'osservazione 15.8. Verifichiamo che $\widetilde{\varphi}$ è un morfismo di anelli. Siano $A, B \in R/_{\ker \varphi}$, e siano $a, b \in R$ tali che $\pi(a) = A$ e $\pi(b) = B$, allora, utilizzando il fatto che π e φ sono dei morfismi e la commutatività del diagramma (21), si ha:

$$\begin{aligned} \widetilde{\varphi}(A+B) &= \widetilde{\varphi}(\pi(a)+\pi(b)) = \widetilde{\varphi}(\pi(a+b)) = \varphi(a+b) = \\ &= \varphi(a)+\varphi(b) = \widetilde{\varphi}(\pi(a)) + \widetilde{\varphi}(\pi(b)) = \widetilde{\varphi}(A) + \widetilde{\varphi}(B). \end{aligned}$$

Analogamente

$$\begin{aligned} \widetilde{\varphi}(AB) &= \widetilde{\varphi}(\pi(a)\pi(b)) = \widetilde{\varphi}(\pi(ab)) = \varphi(ab) = \\ &= \varphi(a)\varphi(b) = \widetilde{\varphi}(\pi(a))\widetilde{\varphi}(\pi(b)) = \widetilde{\varphi}(A)\widetilde{\varphi}(B). \end{aligned}$$

Ciò conclude la dimostrazione. ❏

Esercizio 15.1 Si provi che se I è un ideale di R allora

1. se R è commutativo allora $R/_I$ è commutativo.
2. se R è con identità, allora anche $R/_I$ è con identità e la proiezione a quoziente è un morfismo di anelli con identità.

Esercizio 15.2 Sia $\{I_\lambda\}_{\lambda\in\Lambda}$ una famiglia di ideali dell'anello R. Si provi che $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ è un ideale di R.

Esercizio 15.3 Sia R un anello e $S \subseteq R$ un suo sottinsieme. Si definisca (S) l'ideale generato da S e, si usi l'esercizio precedente per provarne l'esistenza.

Esercizio 15.4 Sia R un anello commutativo, si provi che

$$(a) = \{b \in R \mid a|b\}$$

dove $a|b$ sta a significare che esiste $c \in R$ tale che $b = ca$. (Si confronti con la definizione 3.1).

Esercizio 15.5 Siano I, J ideali dell'anello commutativo R. Si definiscano

$$I + J = \{i + j \mid i \in I, j \in J\}.$$

Si provi che $I + J = (I \cup J)$, ossia è l'ideale generato da $I \cup J$.

Esercizio 15.6 Sia R un anello con identità. Si provi che se I è un ideale di R che contiene una unità, allora $I = R$.

Esercizio 15.7 Si usi l'esercizio precedente per provare che R è un corpo se e solo se gli unici ideali che possiede sono (0) e R.

Lezione 16 (19 aprile 1999 h. 9.30-10.30)

Anello delle serie formali

Sia R un anello commutativo con identità. Consideriamo l'insieme $R^{\mathbb{N}}$ delle successioni a valori in R. Se $a \in R^{\mathbb{N}}$ denoteremo con a_n il valore della funzione a sul naturale n.

Sull'insieme $R^{\mathbb{N}}$ possiamo definire due operazioni:

$$\begin{aligned} (a+b)_n &= a_n + b_n \\ (ab)_n &= \sum_{i=0}^{n} a_i b_{n-i} \end{aligned}$$

Per la commutatività della somma nell'anelle R il termine n-esimo del prodotto di due serie formali si può anche scrivere:

$$(ab)_n = \sum_{i+j=n} a_i b_j$$

intendendo in tal modo dire che la somma è estesa a tutte le coppie di indici i, j la cui somma è n.

Proposizione 16.1 *L'insieme $R^{\mathbb{N}}$ con le due operazioni appena definite è un anello commutativo con identità. Tale anello viene chiamato l'anello delle* serie formali *a coefficienti in R.*

Dim. La verifica che la somma definisca una struttura di gruppo abeliano in cui lo 0 è la successione costantemente nulla (i.e. $0_n = 0$ per ogni n) ad in cui l'opposto della successione a è la successione $(-a)_n = -a_n$ è lasciata per esercizio.

Dalla definizione e dal fatto che R è commutativo segue immediatamente che il prodotto di serie formali è commutativo. Proviamo che il prodotto è associativo.

$$\begin{aligned} (a(bc))_n &= \sum_{i+j=n} a_i (bc)_j = \sum_{i+j=n} a_i (\sum_{h+k=j} b_h c_k) = \\ &= \sum_{i+j=n} \sum_{h+k=j} a_i b_h c_k = \sum_{i+h+k=n} a_i b_h c_k \end{aligned}$$

$$\begin{aligned} ((ab)c)_n &= \sum_{i+j=n} (ab)_i c_j = \sum_{i+j=n} (\sum_{h+k=i} a_h b_k) c_j = \\ &= \sum_{i+j=n} \sum_{h+k=i} a_h b_k c_j = \sum_{j+h+k=n} a_h b_k c_j \end{aligned}$$

quindi $(a(bc))_n = ((ab)c)_n$ per ogni n e quindi $(a(bc)) = ((ab)c)$.

Proviamo ora la proprietà distributiva.

$$\begin{aligned}(a(b+c))_n &= \sum_{i+j=n} a_i(b+c)_j = \sum_{i+j=n} a_i(b_j+c_j) = \sum_{i+j=n} (a_ib_j + a_ic_j) = \\ &= \sum_{i+j=n} a_ib_j + \sum_{i+j=n} a_ic_j = (ab)_n + (ac)_n = (ab+ac)_n\end{aligned}$$

dato che questa relazione vale per ogni n allora $a(b+c) = ab+ac$. L'altr aproprietà distributiva segue dalla commutatività del prodotto.

Consideriamo la successione 1 definita da

$$1_n = \left\langle \begin{array}{ll} 1 & \text{se } n = 0 \\ 0 & \text{se } n \neq 0 \end{array} \right.$$

allora

$$(1a)_n = \sum_{i=0}^{n} 1_i a_{n-i} = 1a_n = a_n$$

poiché tale relazione vale per ogni n allora $1a = a$. Che anche $a1 = a$ segue dalla commutatività del prodotto. ❏

Anello dei polinomi

Definizione 16.2 *Chiameremo* polinomio *una serie formale definitivamente nulla (i.e. esiste n tale che $a_k = 0$ per ogni $k > n$). Se a è un polinomio, chiameremo* grado *di a il numero*

$$\deg a = \max(k \in \mathbb{N} \mid a_k \neq 0\}$$

con la convenzione che $\deg 0 = -\infty$.

Proposizione 16.3 *Se a e b sono polinomi, allora anche $a+b$ e ab lo sono e*

$$\deg(a+b) \leq \max\{\deg a, \deg b\} \tag{22}$$

$$\deg(ab) \leq \deg a + \deg b \tag{23}$$

Se R è un dominio di integrità, allora nella (23) vale l'uguaglianza.

Dim. Se $n > \max\{\deg a, \deg b\}$ necessariamente $a_n = 0$ e $b_n = 0$ e quindi $a_n + b_n = 0$ per ogni $n > \max\{\deg a, \deg b\}$, quindi $a+b$ è un polinomio e vale la (22).

Sia $n > \deg a + \deg b$ e consideriamo $(ab)_n = \sum_{i+j=n} a_ib_j$. Se $i \leq \deg a$ e $j \leq \deg b$ allora $i+j \leq \deg a + \deg b < n$, quindi in ogni addendo della somma che esprime $(ab)_n$ o $i > \deg a$ o $j > \deg b$ ossia almeno uno tra a_i e b_j è nullo. Quindi tutti gli addendi sono nulli e pertanto $(ab)_n = 0$. Pertanto ab è un polinomio e vale la (23).

Sia R un dominio di integrità e siano $h = \deg a$ e $k = \deg b$ e consideriamo $(ab)_{h+k} = \sum_{i+j=h+k} a_ib_j$. Di tutti gli addendi di questa somma, l'unico che può essere non nullo è quello che si ottiene con $i = h$ e $j = k$ (in tutti gli altri casi possibili si ha che o $i > h$ e quindi $a_i = 0$ o $j > k$ e quindi $b_j = 0$). E quindi $(ab)_{h+k} = a_h b_k \neq 0$ in quanto $a_h \neq 0$, $b_k \neq 0$ e R è un dominio di integrità. ❑

Proposizione 16.4 *L'insieme dei polinomi è un sottoanello dell'anello delle serie formali.*

Dim. La proposizione precedente mostra che l'insieme dei polinomi è chiuso per somma e prodotto. D'altra parte è evidente che le successioni 0 e 1 sono dei polinomi e che se a è un polinomio allora anche $-a$ lo è. ❑

Osservazione 16.5 Indichiamo ora con P l'anello dei polinomi a coefficienti in R, e consideriamo l'applicazione $i : R \to P$ definita da $i(r) = (r, 0, \ldots 0, \ldots)$, ossia $i(r)$ è la successione tale che $i(r)_0 = r$ e $i(r)_n = 0$ per ogni $n > 0$.

L'applicazione i è un morfismo di anelli. Infatti

$$\begin{aligned} i(r_1 + r_2)_n &= \begin{cases} r_1 + r_2 & \text{se} \quad n = 0 \\ 0 & \text{se} \quad n > 0 \end{cases} \\ (i(r_1) + i(r_2))_n &= i(r_1)_n + i(r_2)_n = \begin{cases} r_1 + r_2 & \text{se} \quad n = 0 \\ 0 + 0 = 0 & \text{se} \quad n > 0 \end{cases} \end{aligned}$$

e quindi $i(r_1 = r_2) = i(r_1) = i(r_2)$.

$$\begin{aligned} i(r_1 r_2)_n &= \begin{cases} r_1 r_2 & \text{se} \quad n = 0 \\ 0 & \text{se} \quad n > 0 \end{cases} \\ (i(r_1) i(r_2))_n &= \sum_{j=0}^{n} i(r_1)_j i(r_2)_{n-j} = \begin{cases} i(r_1)_0 i(r_2)_0 = r_1 r_2 & \text{se} \quad n = 0 \\ \sum_{i=0}^{n} 0 = 0 & \text{se} \quad n > 0 \end{cases} \end{aligned}$$

Chiaramente il morfismo i è iniettivo, quindi è un isomorfismo con la sua immagine, possiamo, e d'ora in poi lo faremo, identificare R con la sua immagine $i(R)$. Osserviamo ancora che se $r \in R$ e a è un polinomio, allora

$$(ra)_n = r a_n \quad \forall n.$$

Proposizione 16.6 *Sia* $x = (0, 1, 0, \ldots)$. *Allora per ogni* $i \in \mathbb{N}$, x^i *è la successione tale che*

$$(x^i)_n = \begin{cases} 0 & \text{se} \quad n \neq i \\ 1 & \text{se} \quad i = n \end{cases}$$

Dim. Procediamo per induzione su i. Per $i = 0$, dalla definizione di potenza)e:expg, segue che $x^0 = 1$.

Supponiamo latesi vera per i allora

$$(x^{i+1})_n = (x x^i)_n = \sum_{j=0}^{n} x_j (x^i)_{n-j} = \begin{cases} 0 & \text{se } n = 0 \\ x_1 (x^i)_{n-1} = (x^i)_{n-1} & \text{se } n \geq 1 \end{cases}$$

ma per ipotesi di induzione

$$(x^i)_{n-1} = \begin{cases} 0 & \text{se } n-1 \neq i \\ 1 & \text{se } n-1 = i \end{cases}$$

quindi in definitiva

$$(x^{i+1})_n = \begin{cases} 0 & \text{se } n \neq i+1 \\ 1 & \text{se } n = i+1 \end{cases}$$

$\square$

Osservazione 16.7 L'osservazione e la proposizione precedenti permettono allora di scrivere ogni polinomio nel modo usuale. Infatti

$$\begin{aligned}
(a_0, a_1, \ldots, a_n, 0, \ldots, 0\ldots) &= (a_0, 0, \ldots, 0\ldots) + \\
&\quad (0, a_1, 0\ldots, 0\ldots) + \\
&\quad \vdots \\
&\quad (0, \ldots, 0, a_n, 0, \ldots, 0\ldots) = \\
&= (a_0, 0, \ldots, 0\ldots)(1, 0, \ldots, 0, \ldots) + \\
&\quad (a_1, 0, \ldots, 0\ldots)(0, 1, 0\ldots, 0\ldots) + \\
&\quad \vdots \\
&\quad (a_n, 0, \ldots, 0\ldots)(0, \ldots, 0, 1, 0, \ldots, 0\ldots) = \\
&= a_0x^0 + a_1x^1 + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^i
\end{aligned}$$

D'ora in poi si userà questa notazione per i polinomi, e si indicherà con $R[x]$ l'anello dei polinomi a coefficienti in R.

L'anello delle serie formali si denota invece con $R[[x]]$. Il nome serie formali deriva dal fatto che una serie può essere pensata come una “somma infinita” del tipo $\sum_{i=0}^{\infty} a_ix^i$ essenso x come nella proposizione precedente. È chiaro che questa è però soltanto una comoda notazione, in quanto in un anello non si possono fare somme infinite.

Osservazione 16.8 Dalla (16.3) segue che se R è un dominio di integrità allora anche $R[x]$ lo è. Infatti se $P, Q \in R[x]$ e sono non nulli, allora $\deg PQ = \deg P + \deg Q > -\infty$ e quindi $PQ \neq 0$.

D'altra parte è chiaro che se R non è un dominio allora a maggior ragione non lo è $R[x]$ che contiene R come sottanello.

Lezione 17 (21 aprile 1999 h. 9.30-10.30)

Proprietà universale dei polinomi

Teorema 17.1 *Siano R e R' due anelli commutativi con identità, e sia $\varphi : R \to R'$ un morfismo di anelli con identità. Allora per ogni $t \in R'$ esiste un unico morfismo $\varphi_t : R[x] \to R'$ tale che*

1. $\varphi_{t|R} = \varphi$
2. $\varphi_t(x) = t$

Dim. Definiamo $\varphi_t : R[x] \to R'$ ponendo

$$\varphi_t(\sum_i a_i x^i) = \sum_i \varphi(a_i) t^i$$

l'applicazione è ben definita in quanto, trattandosi di polinomi, la somma a secondo membro è finita. Evidentemente l'applicazione φ_t così definita verifica le proprietè (1) e (2). Proviamo che φ_t è un morfismo (definizione 15.1).

Siano $P = \sum_i a_i x^i$ e $Q = \sum_i b_i x^i$

$$\begin{aligned}\varphi_t(P+Q) &= \varphi_t \sum_i (a_i + b_i)x^i = \sum_i \varphi(a_i + b_i)t^i = \sum_i (\varphi(a_i) + \varphi(b_i))t^i = \\ &= \sum_i \varphi(a_i)t^i + \sum_i \varphi(b_i)t^i = \varphi_t(P) + \varphi_t(Q)\end{aligned}$$

$$\begin{aligned}\varphi_t(PQ) &= \varphi_t(\sum_i (\sum_{h+k=i} a_h b_k)x^i) = \sum_i \varphi(\sum_{h+k=i} a_h b_k)t^i = \\ &= \sum_i (\sum_{h+k=i} \varphi(a_h)\varphi(b_k))t^i\end{aligned}$$

D'altra parte

$$\begin{aligned}\varphi_t(P)\varphi_t(Q) &= (\sum_i \varphi(a_i)t^i)(\sum_i \varphi(b_i)t^i) = \sum_{i,j} \varphi(a_i)t^i \varphi(b_j)t^j = \\ &= \sum_{i,j} \varphi(a_i)\varphi(b_j)t^i t^j = \sum_{i,j} \varphi(a_i)\varphi(b_j)t^{i+j} = \sum_k (\sum_{i+j=k} a_i b_j)t^k\end{aligned}$$

dove la terzultima uguaglianza è ootenuta perché l'anello R' è commutativo e l'ultima uguaglanza è ottenuta semplicemente riordinando i termini della somma (cosa che si può fare perché la somma è commutativa). Evidentemente si ha allora che $\varphi_t(PQ) = \varphi_t(P)\varphi_t(Q)$.

Proviamo ora l'unicità. Sia $\psi : R[x] \to R'$ un morfismo con le proprietà richieste. Osserviamo che se $P = \sum_{i=0}^n a_i x^i$, dato che ψ è un morfismo deve risultare:

$$\psi(P) = \psi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \psi(a_i x^i) = \sum_{i=0}^n \psi(a_i)\psi(x)^i = \sum_{i=0}^n \varphi(a_i)t^i$$

ossia $\psi = \varphi_t$. ❑

Polinomi e funzioni polinomiali

Osservazione 17.2 Un caso particolare del precedente teorema è quando $R = R'$ e $\varphi = \mathrm{id}$. In tal caso se $P \in R[x]$ il valore di $\mathrm{id}_t(P)$ viene solitamente indicato con $P(t)$ e viene chiamato la *valutazione* in t di P (e il morfismo id_t viene chiamato il morfismo di valutazione in t). $P(t)$ è ciò che si ottiene dando alla "variabile" x il valore t. Si osservi che in questo modo ad ogni polinomio $P \in R[x]$ si associa una funzione $f_P : R \to R$ definita da $f_P(t) = P(t)$. Si definisce così una applicazione $R[x] \to R^R$ che al polinomio P associa la funzione polinomiale f_P. Osserviamo che tale applicazione non è in generale iniettiva, ossia si possono avere polinomi diversi che definiscono la stessa funzione. Ad esempio si considerino i due polinomi $P, Q \in \mathbb{Z}/2\mathbb{Z}$ dati da $P = 0$ e $Q = x^2 + x$. Chiaramente $P(0) = P(1) = 0$ ma anche $Q(0) = 0$ e $Q(1) = 1^2 + 1 = 1 + 1 = 0$, pur tuttavia i due polinomi sono diversi.

Esercizio 17.1 Si provi che l'applicazione $f : R[x] \to R^R$ definita nell'osservazione precedente ($P \mapsto f_P$ essendo $f_P(t) = P(t) = \mathrm{id}_t(P)$) è un morfismo di anelli.

Divisione euclidea

Teorema 17.3 (divisione euclidea) *Sia K un campo e siano $P_1, P_2 \in K[x]$ con $P_2 \neq 0$, allora esistono unici $Q, R \in K[x]$ tali che*

$$P_1 = P_2 Q + R$$

con $\deg R < \deg P_2$.

Dim. Esistenza. Osserviamo innanzitutto che se $\deg P_1 < \deg P_2$ la tesi segue prendendo $Q = 0$ e $R = P_1$. Supponiamo allora che $\deg P_1 \geq \deg P_2$ e procediamo per induzione su $n = \deg P_1$. Se $\deg P_1 = 0$ allora $\deg P_2 \leq \deg P_1$ e quindi $P_2 = a \in K$ e dato che $P_2 \neq 0$, $a \neq 0$ e quindi è invertibile. Ma allora

$$P_1 = a(a^{-1}P_1) + 0 = P_2(a^{-1}P_1) + 0.$$

Sia ora $\deg P_1 = n > 0$ e supponiamo che la tesi sia vera per ogni polinomio P con $\deg P < n$. Siano allora $P_1 = \sum_{i=0}^{n} b_i x^i$ e $P_2 = \sum_{i=0}^{m} a_i x^i$ con $m \leq n$ e $a_m \neq 0$. Dato che $a_m \neq 0$ è invertibile, si consideri allora il polinomio $P = P_1 - b_n a_m^{-1} x^{n-m} P_2$. Si osservi che $\deg(b_n a_m^{-1} x^{n-m} P_2) = n = \deg P_1$ e quindi il polinomio P ha grado non superiore (proposizione 22) a n. Ma d'altra parte il termine di grado n è dato da $b_n x^n + (-b_n a_m^{-1} x^{n-m} a_m x^m) = 0$ e quindi $\deg P < n$. Possiamo quindi applicare l'ipotesi di induzione per dire che allora esistono $Q, R \in K[x]$ tali che $P = QP_2 + R$ con $\deg R < \deg P_2$. Ma allora

$$\begin{aligned} P_1 &= P + b_n a_m^{-1} x^{n-m} P_2 = \\ &= P_2 Q + R + b_n a_m^{-1} x^{n-m} P_2 = P_2(Q + b_n a_m^{-1} x^{n-m}) + R \end{aligned}$$

e quindi la tesi.

Unicità. Supponiamo che esistano $Q, R, Q', R' \in K[x]$ con $\deg R < \deg P_2$ e $\deg R' < \deg P_2$ tali che $P_1 = P_2 Q + R = P_2 Q' + R'$. Da quest'ultima relazione segue immediatamente che $P_2(Q - Q') = R' - R$ e quindi, passando ai gradi, $\deg(P_2(Q - Q')) = \deg(R' - R)$. Ma ora, usando le relazioni sui gradi (proposizione 16.3),

$$\deg P_2(Q - Q') = \deg P_2 + \deg(Q - Q')$$

$$\deg(R' - R) \leq \max\{\deg R, \deg R'\} < \deg P_2$$

ma allora $\deg P_2 + \deg(Q - Q') < \deg P_2$. Dato che $P_2 \neq 0$ ciò implica che $\deg(Q - Q') = -\infty$ ossia $Q = Q'$, da cui segue che allora anche $R = R'$. ❑

Teorema di Ruffini

Definizione 17.4 *Sia $P \in R[x]$ un polinomio. Diremo che $\alpha \in R$ è una* radice *di P se $f(\alpha) = 0$. Si dirà anche che α è uno* zero *di P.*

Teorema 17.5 (di Ruffini) *Sia K un campo e sia $P \in K[x]$ allora α è una radice di P se e solo se $(x - a)\big|P$ (i.e. esiste Q tale che $P = (x - a)Q$, si veda anche l'esercizio 15.4).*

Dim. Si esegua la divisione euclidea di P per $(x - \alpha)$ allora si ottiene $P = Q(x - \alpha) + a$ con $a \in K$, dato che $\deg a < \deg(x - a) = 1$. Si osservi allora che $P(\alpha) = a$ e quindi $P(\alpha) = 0$ se e solo se $a = 0$ ossia se e solo se $(x - a)\big|P$. ❑

Lezione 18 (22 aprile 1999 h. 10.30-11.30)

Principio di identità dei polinomi

Proposizione 18.1 *Sia K un campo e sia $P \in K[x]$ un polinomio non nullo. Allora se $n = \deg P$, P ha al più n radici.*

Dim. Procediamo per induzione su $\deg P$. Se $\deg P = 0$ P non ha radici. Supponiamo che $\deg P = n+1$, se P non ha radici, allora la tesi è vera. Supponiamo allora che α sia una radice di P; per il teorema di Ruffini (teorema 17.5) esiste un polinomio Q tale che $P = (x - \alpha)Q$. Dato che K è un campo, è in particolare un dominio di integrità (corollario 14.11) e quindi per le relazioni sui gradi (proposizione 16.3) si ha che $\deg Q = n$, quindi Q ha, per ipotesi di induzione, al più n radici. Osserviamo ancora che se $\beta \in K$ allora

$$P(\beta) = (\beta - \alpha)Q(\beta)$$

e sempre per il fatto che K è un dominio di integrità, si ha che $P(\beta) = 0$ se e solo se $\beta - \alpha = 0$ oppure $Q(\beta) = 0$ ossia se e solo se $\beta = \alpha$ oppure β è una radice di Q. Quindi P ha al più $n + 1$ radici. ❑

Osservazione 18.2 Segue immediatamente dalla proposizione precedente, che se P è un polinomio ha con $\deg P \leq n$ che ha $n+1$ radici distinte, allora $P = 0$.

Corollario 18.3 (principio di identità dei polinomi) *Sia K un campo con infiniti elementi. Se $P, Q \in K[x]$ sono tali che $P(t) = Q(t)$ per ogni t allora $P = Q$*

Dim. Si applichi l'osservazione precedente al polinomio $P - Q$, per il quale si possono trovare infinite radici. ❑

Osservazione 18.4 Il corollario precedente mostra che se K è infinito, allora l'applicazione dell'osservazione 17.2 è iniettiva.

Esercizio 18.1 Si provi che il morfismo $K[x] \to K^K$ definito nell'osservazione 17.2 e nell'esercizio 17.1, è iniettivo se e solo se il campo K è infinito. Quando il campo K è finito si determini il nucleo di tale morfismo.

Matrice di Vandermonde

Lemma 18.5 *Sia K un campo e siano $\alpha_1, \ldots, \alpha_k \in K$. Si consideri la matrice $k \times k$ a coefficienti in K*

$$V(\alpha_1, \ldots, \alpha_k) = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_k & \alpha_k^2 & \cdots & \alpha_k^{k-1} \end{pmatrix}.$$

La matrice $V(\alpha_1, \ldots, \alpha_k)$ è invertibile se e solo se gli α_i sono tra loro distinti.

Dim. Consideriamo il sistema lineare $V(\alpha_1, \ldots, \alpha_k)x = 0$ e supponiamo che $\lambda = (\lambda_0, \ldots, \lambda_{k-1}) \in K^k$ sia una sua soluzione, ciò vuol dire che

$$\sum_{i=0}^{k-1} \lambda_i \alpha_j^1 = 0 \quad \forall j = 1, \ldots, k$$

Si consideri il polinomio $P(x) = \sum_{i=0}^{k-1} \lambda_i x^i \in K[x]$, allora il sistema precedente non dice altro che ogni α_i è una radice di P. Dato che $\deg P \leq k-1$, se gli α_i sono distinti, per l'osservazione 18.2, $P = 0$ ossia $\lambda_i = 0$ per ogni i. Quindi il sistema lineare ha solo la soluzione banale e quindi la matrice è invertibile.

Viceversa, se due dedgli α_i sono uguali, la matrice ha due righe uguali e quindi non è invertibile. ❑

Molteplicità di una radice

Definizione 18.6 *Sia $P \in K[x]$ un polinomio non nullo a coefficienti in un campo e sia α una sua radice. Si chiama* molteplicità *della radice α il massimo tra gli interi m tali che $(x-\alpha)^m | P$.*

Definizione 18.7 *Sia $P \in R[x]$, $p = \sum_{i=1}^{n} a_i x^i$. Definiamo* derivata formale *del polinomio P il polinomio $P' = \sum_{i=0}^{n} i a_i x^{i-1}$.*

Proposizione 18.8 *Si provi che se $P, Q \in R[x]$ allora*

$$\begin{aligned} (P+Q)' &= P' + Q' \\ (PQ)' &= P'Q + PQ' \end{aligned}$$

Dim. Lasciata per esercizio. ❑

Proposizione 18.9 *Sia $P \in K[x]$ un polinomio a coefficienti in un campo, e sia α una sua radice. α ha molteplicità maggiore di 1 se e solo se $P'(\alpha) = 0$.*

Dim. Dato che α è una radice allora per il teorema di Ruffini (teorema17.5) $P = (x-\alpha)Q$. Derivando si ha $P' = Q + (x-\alpha)Q'$ e quindi $P'(\alpha) = Q(\alpha)$ e pertanto α è radice di P' se e solo se è radice di Q e quindi, ancora per il teorema di Ruffini (teorema17.5), se e solo se esiste R tale che $Q = (x-\alpha)R$ ovvero se e solo se $P = (x-\alpha)^2 R$, che è la tesi. ❑

Esercizio 18.2 Sia K un campo e sia $Q \in K[x]$ siano $\alpha \neq \beta \in K$ $s \in \mathbb{N}$. Detto $P = (x-\alpha)^s Q$ si provi che β è radice di P con molteplicità m se e solo se β è radice di Q con molteplicità m.

Caratteristica

Definizione 18.10 *Sia K un campo. Si consideri l'insieme $S = \{n \in \mathbb{N} \mid n > 0 \text{ e } n1_K = 0\}$. Se $S \neq \varnothing$ allora ha minimo (assioma 1.1). Tale minimo si chiama* caratteristica *di K, e si indica con* $\operatorname{char} K$. *Se invece $S = \varnothing$ si dirà che* $\operatorname{char} K = 0$.

Esercizio 18.3 Si provi che la caratteristica di un campo è un numero primo.

Esercizio 18.4 Si provi che se $\operatorname{char} K = p$ allora per ogni $k \in K$ si ha che $pk = 0$.

Molteplicità in caratteristica 0

Teorema 18.11 *Sia K un campo di caratteristica 0 e sia $P \in K[x]$ e α una sua radice e indichiamo con $\mu(\alpha)$ la sua molteplicità. Allora $\mu(\alpha) \geq m$ se e solo se $P(\alpha) = P'(\alpha) = P''(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$.*

Lezione 19 (26 aprile 1999 h. 9.30-10.30)

Dimostrazione del teorema 18.11

Dim. Supponiamo che α abbia molteplicità $\mu(\alpha) \geq m$ e proviamo che allora è radice di tutte le derivate fino all'ordine $m-1$. Procediamo per induzione su m. Se $m = 1$ la tesi è data dal teorema di Ruffini (teorema17.5). Supponiamo la tesi vera per m. Sia quindi $\mu(\alpha) \geq m+1$, ovvero $P = (x-\alpha)^{m+1}$ allora derivando si ottiene

$$P' = (m+1)(x-\alpha)^m Q + (x-\alpha)^{m+1} Q' = (x-\alpha)^m ((m+1)Q + (x-\alpha)Q')$$

ovvero $(x-\alpha)^m \big| P'$ quindi α è radice di P' con molteplicità almeno m, per ipotesi di induzione si ha allora che $P'(\alpha) = (P')'(\alpha) = \ldots (P')^{(m-1)}(\alpha) = 0$, ossia $P'(\alpha) = P''(\alpha) + \ldots P^{(m)}(\alpha) = 0$ che insieme al fatto che α è radice di P dà la tesi.

Viceversa. Procediamo per induzione su m. Per $m = 1$ la tesi è ovvia. Supponiamo la tesi vera per $m \geq 1$. Sia P un polinomio e sia α tale che

$$P(\alpha) = P'(\alpha) = \ldots P^{(m-1)}(\alpha) = P^{(m)}(\alpha) = 0 \tag{24}$$

L'ipotesi di induzione e le prime m di queste uguaglianze garantiscono che α è una radice di molteplicità almeno m, ossia che esiste Q tale che $P = (x-\alpha)^m Q$, da cui derivando si ottiene

$$P' = m(x-\alpha)^{m-1} Q + (x-\alpha)^m Q' = (x-\alpha)^{m-1}(mQ + (x-\alpha)Q') \tag{25}$$

Le ultime m uguaglianze delle (24), garantiscono invece che α è anche radice di P' con molteplicità almeno m ovvero che esiste R tale che $P' = (x-\alpha)^m R$. Uguagliando con la (25) si ottiene quindi

$$(x-\alpha)^m R = (x-\alpha)^{m-1}(mQ + (x-\alpha)Q')$$

da cui

$$(x-\alpha)^{m-1}(mQ + (x-\alpha)(Q' - R)) = 0.$$

Dato che $K[x]$ è un dominio di integrità (osservazione 16.8) e $(x-\alpha)^{m-1} \neq 0$, allora $mQ + (x-\alpha)(Q'-R)$. Valutando in α si ottiene allora $mQ(\alpha) = 0$, dato che $\operatorname{char} K = 0$ ciò implica che $Q(\alpha) =$). Ma allora, per il teorema di Ruffini (teorema17.5), $Q = (x-\alpha)S$ e quindi $P = (x-\alpha)^m Q = (x-\alpha)^m (x-\alpha) S = (x-\alpha)^{m+1} S$, che è la tesi. ❏

Equazioni ricorsive lineari

Sia $x \in \mathbb{R}^{\mathbb{N}}$ una successione, diremo che x risolve una *equazione ricorsiva*, se ogni elemento è funzione dei precedenti, in simboli se esistono delle funzioni $f_n : \mathbb{R}^{n+1} \to \mathbb{R}$ tali che

$$x_n = f_n(x_0, x_1, \ldots, x_{n-1}) \quad \forall n \geq 1. \tag{26}$$

Supponendo di avere date le equazioni ricorsive, il problema di ricavare informazioni sulle successioni che le risolvono non è in generale di facile soluzione. Analizzeremo un caso di equazioni ricorsive di tipo particolare, per le quali si riescono a determinare esplicitamente tutte le soluzioni.

Considereremo equazioni ricorsive che hanno *storia finita* ovvero per le quali esiste un $k \geq 1$ tale che ogni termine è funzione soltanto dei k precedenti (i.e. le f_n hanno come dominio tutte $\mathbb{R}^k$) e in cui le f_n sono tutte uguali e lineari, ossia equazioni del tipo

$$x_{n+k} = \sum_{i=0}^{k-1} a_i x_{n+i} \quad \forall n \geq 0 \tag{27}$$

con $a_i \in \mathbb{R}$ e $a_0 \neq 0$. Una tale equazione ricorsiva la chiameremo *lineare a coefficienti costanti di ordine k.*

Osservazione 19.1 La condizione $a_0 \neq 0$ viene posta in modo che si abbia una effettiva dipendenza di ogni termine della successione dai precedenti k. Se infatti fosse $a_0 = 0$ si avrebbe che ogni termine dipenderebbe soltanto dai $k-1$ termini preceedenti.

Anche se nella pratica le equazioni ricorsive che si incontrano sono definite sui numeri reali (si pensi al calcolo della complessità di un algoritmo, ossia il numero di passi necessario per ottenere l'output in funzione dell'input), può essere comodo ambientare il problema nel campo dei numeri complessi. Nel seguito denoteremo con $\mathbb{K}$ un campo che può essere o quello dei numeri reali o quello dei numeri complessi.

Supponiamo allora di avere fissata l'equazione ricorsiva (27), ossia di aver fissati $a_0, \ldots, a_{k-1} \in \mathbb{K}$ e di cercare le successioni $x \in \mathbb{K}^{\mathbb{N}}$ che verificano la (27). Sia

$$\mathcal{V} = \{x \in \mathbb{K}^{\mathbb{N}} \mid x_{n+k} = \sum_{i=0}^{k-1} a_i x_{n+i} \quad \forall n \geq 0\}$$

Proposizione 19.2 *L'insieme $\mathcal{V}$ è uno spazio vettoriale (i.e. è un sottospazio di $\mathbb{K}^{\mathbb{N}}$.*

Dim. Siano $x, y \in \mathcal{V}$ allora per ogni n si ha $x_{n+k} = \sum_{i=0}^{k-1} a_i x_{n+i}$ e $y_{n+k} = \sum_{i=0}^{k-1} a_i y_{n+i}$ sommando membro a membro si ha allora che

$$x_{n+k} + y_{n+k} = \sum_{i=0}^{k-1} a_i x_{n+i} + \sum_{i=0}^{k-1} a_i y_{n+i} = \sum_{i=0}^{k-1} a_i (x_{n+i} + y_{n+i})$$

ossia

$$(x+y)_{n+k} = \sum_{i=0}^{k-1} a_i (x+y)_{n+i}$$

ossia $x + y \in \mathcal{V}$. Analogamente se $\lambda \in \mathbb{K}$ e $x \in \mathcal{V}$ si ha

$$(\lambda x)_{n+k} = \lambda x_{n+k} = \lambda \sum_{i=0}^{k-1} a_i x_{n+i} = \sum_{i=0}^{k-1} a_i \lambda x_{n+i} = \sum_{i=0}^{k-1} a_i (\lambda x)_{n+i}$$

ossia $\lambda x \in \mathcal{V}$. ❏

Lezione 20 (28 aprile 1999 h. 9.30-10.30)

Lo spazio $\mathcal{V}$ ha dimensione finita

Proposizione 20.1 *La dimensione di $\mathcal{V}$ è minore o uguale a k.*

Dim. Si consideri l'applicazione $\varphi : \mathcal{V} \to \mathbb{K}^k$ definita da $\varphi(x) = (x_0, \ldots, x_{k-1})$. Dimostreremo che φ è lineare e iniettiva da cui seguirà allora la tesi.

φ è lineare. Infatti se x, y sono successioni e $\lambda \in \mathbb{K}$, allora

$$\begin{aligned} \varphi(x+y) &= ((x+y)_0, \ldots, (x+y)_{k-1}) = (x_0 + y_0, \ldots, x_{k-1} + y_{k-1}) = \\ &= (x_0, \ldots, x_{k-1}) + (y_0, \ldots, y_{k-1}) = \varphi(x) + \varphi(y) \end{aligned}$$

$$\begin{aligned} \varphi(\lambda x) &= ((\lambda x)_0, \ldots, (\lambda x)_{k-1}) = (\lambda x_0, \ldots, \lambda x_{k-1}) = \\ &= \lambda(x_0, \ldots, x_{k-1}) = \lambda \varphi(x) \end{aligned}$$

φ è iniettiva. Per fare ciò proviamo che $\ker \varphi = \{0\}$. Sia $x \in \ker \varphi$, proviamo per induzione su n che allora $x_n = 0$ per ogni n. Se $n \leq k-1$ $x_n = 0$ dato che $\varphi(x) = 0$. Supponiamo $n \geq k$ e supponiamo che la tesi sia vera per ogni $h < n$. Allora

$$x_n = x(n-k) + k = \sum_{i=0}^{k-1} a_i x_{n-k} + i \sum_{i=0}^{k-1} a_i 0 = 0$$

dave si è usato il fatto che $n - k + i < n$ per ogni $i = 0, \ldots, k-1$ e quindi l'ipotesi di induzione. ❏

Polinomio caratteristico

Definizione 20.2 *Chiameremo* polinomio caratteristico *dell'equazione (27) il polinomio*

$$P(t) = t^k - \sum_{i=0}^{k-1} a_i t^i \in \mathbb{K}[t].$$

Osservazione 20.3 Osserviamo che 0 non può essere radice del polinomio caratteristico di una equazione ricorsiva, infatti $P(0) = a_0$ e quindi 0 è radice se e solo se $a_0 = 0$. Ma se fosse $a_0 = 0$ allora vorrebbe dire che l'equazione ricorsiva avrebbe ordine $k-1$ (osservazione 19.1).

Base di $\mathcal{V}$ (caso delle radici distinte)

Proposizione 20.4 *La successione $\{\alpha^n\}$ è soluzione dell'equazione (27) se solo se α è radice del polinomio caratteristico.*

Dim. La successione $\{\alpha^n\}$ è soluzione dell'equazione ricorsiva (27) se e solo se si ha

$$\alpha^{n+k} = \sum_{i=1}^{k-1} a_i \alpha^{n+i} \qquad \forall n \geq 0$$

ossia se e solo se

$$\alpha^n \bigl(\alpha^k - \sum_{i=1}^{k-1} \alpha^i\bigr) = 0 \qquad \forall n \geq 0.$$

Dato che la successione $\{0^n\} = (1, 0, 0 \ldots)$ non è soluzione dell'equazione ricorsiva (per questa successione $x_k = 0$ mentre $\sum a_i x^i = a_0 \neq 0$),e per quanto osservato sopra (osservazione 20.3) 0 non è radice del polinomio caratteristico, possiamo dividere per α^n l'equazione precedente ottenendo che $\{\alpha^n\}$ è soluzione se e solo se

$$\alpha^k - \sum_{i=1}^{k-1} a_i \alpha^i = 0$$

che è la tesi. ❑

Lemma 20.5 *Siano $\alpha_1, \ldots, \alpha_s \in \mathbb{R}$ numeri a due a due distinti, allora le successioni $\{\alpha_1^n\}_n, \ldots, \{\alpha_s^n\}_n$ sono linearmente indipendenti.*

Dim. Siano $\lambda_1, \ldots, \lambda_s \in \mathbb{K}$ tali che la successione $\{\sum_{i=1}^s \lambda_i \alpha_i^n\}_n$ sia la successione nulla, ovvero

$$\sum_{i=1}^{s} \lambda_i \alpha_i^n = 0 \qquad \forall n \geq 0$$

in particolare allora

$$\sum_{i=1}^{s} \lambda_i \alpha_i^n = 0 \qquad \forall n = 0, \ldots, s-1.$$

Tale relazione può essere riscritta in termini matriciali come:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_s \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_s^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{s-1} & \alpha_2^{s-1} & \cdots & \alpha_s^{s-1} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \vdots \\ \lambda_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ma la matrice di tale sistema è invertibile (lemma 18.5) e quindi $\lambda_i = 0$ per ogni $i = 1, \ldots, s$. ❑

Teorema 20.6 *Supponiamo che il polinomio caratteristico dell'equazione (27) abbia k radici distinte $\alpha_1, \ldots, \alpha_k$ allora le successioni $\{\alpha_1^n\}_n, \ldots, \{\alpha_k^n\}_n$ sono una base di $\mathcal{V}$.*

Dim. Per la proposizione 20.4 le successioni $\{\alpha_1^n\}_n, \ldots, \{\alpha_k^n\}_n$ sono soluzioni dell'equazione ricorsiva; per il lemma precedente (20.5) sono linearmente indipendenti. Dato che $\dim \mathcal{V} \leq k$ (proposizione 20.1), costituiscono una base di $\mathcal{V}$. ❑

Osservazione 20.7 Si osservi che come immediata conseguenza del teorema precedente si ha che la dimensione di $\mathcal{V}$ è proprio k e quindi l'applicazione $\varphi : \mathcal{V} \to \mathbb{R}^k$ definita nella dimostrazione della proposizione 20.1 è un isomorfismo. Pertanto, dati k numeri $u_0, \ldots, u_{k-1}$, il problema di Cauchy di trovare una successione tale che

$$\begin{cases} x_{n+k} & = & \sum_{i=0}^{k-1} a_i x_i \qquad \forall n \geq 0 \\ x_0 & = & u_0 \\ & \vdots & \\ x_{k-1} & = & u_{k-1} \end{cases}$$

ha una e una sola soluzione. Si ha anche un metodo per determinarne una soluzione esplicita: una generica soluzione è data da $\sum_{i=1}^{k} C_i \alpha_i^n$ con $C_i \in \mathbb{K}$. Basterà quindi determinare le costanti $C_i \in \mathbb{K}$ in modo da verificare le condizioni inizialoi e precisamente in modo che

$$\sum_{i=1}^{k} C_i \alpha_i^j = u_j \qquad \forall j = 0, \ldots, k-1$$

e questo è un sistema lineare, che si sa risolvere.

Base di $\mathcal{V}$ (caso generale)

Nel caso generale vale il seguente teorema di cui omettiamo la dimostrazione.

Teorema 20.8 *Sia $\mathbb{K} = \mathbb{C}$ e siano $\alpha_1, \ldots, \alpha_s$ le radici del polinomio caratteristico dell'equazione ricorsiva. Siano $m_1, \ldots, m_s$ le rispettive molteplicità (definizione 18.6). Allora le successioni*

$$\begin{array}{cccc} \alpha_1^n & n\alpha_1^n & \cdots & n^{m_1-1}\alpha_1^n \\ \alpha_2^n & n\alpha_2^n & \cdots & n^{m_2-1}\alpha_2^n \\ \vdots & \vdots & & \vdots \\ \alpha_s^n & n\alpha_s^n & \cdots & n^{m_s-1}\alpha_s^n \end{array}$$

sono una base dello spazio vettoriale $\mathcal{V}$.

Osservazione 20.9 Si vedrà nella prossima lezione che il numero di tali successioni è, anche in questo caso, esattamente k, e quindi tutto quanto detto nell'osservazione precedente (osservazione 20.7) resta vero anche nelle ipotesi di questo teorema.

Lezione 21 (29 aprile 1999 h. 10.30-11.30)

Definizione di campo algebricamente chiuso

Definizione 21.1 *Si dice che un campo K è* algebricamente chiuso *se ogni polinomio non nullo di $K[x]$ ha almeno una radice. In simboli*

$$P \in K[x], P \neq 0 \Rightarrow \exists \alpha \in K : P(\alpha) = 0.$$

Vale il seguente teorema di cui omettiamo la dimostrazione.

Teorema 21.2 (Fondamentale dell'algebra) $\mathbb{C}$ *è algebricamente chiuso*

Fattorizzazione nei campi algebricamente chiusi

Teorema 21.3 *Sia K un campo algebricamente chiuso e sia $P \in K[x]$ con $\deg P = n$. Allora esistono $\alpha, \alpha_1, \ldots, \alpha_n \in K$ tali che*

$$P = \alpha \prod_{i=1}^{n} (x - \alpha_i).$$

Dim. Procediamo per induzione su $\deg P$. Se $\deg P = 0$ non c'è niente da dimostrare. Sia $\deg P = n + 1$ con $n \geq 0$, allora, dato che K è algebricamente chiuso e P non è costante, esiste $\alpha_n \in K$ tale che $P(\alpha_n) = 0$. Per il teorema di Ruffini (17.5) si ha allora che $P = (x - \alpha_n)Q$ e $\deg Q = n$. Ma allora per ipotesi di induzione $Q = \alpha \prod_{i=1}^{n} (x - \alpha_i)$ e quindi

$$P = (x - \alpha_n)Q = (x - \alpha_n)\alpha \prod_{i=1}^{n} (x - \alpha_i) = \alpha \prod_{i=1}^{n+1} (x - \alpha_i).$$

Ciò conclude la dimostrazione. ❏

Osservazione 21.4 Osserviamo che gli α_i che compaiono nella fattorizzazione del teorema precedente sono esattamente le radici di P, e se in tale fattorizzazione si raccolgono tra loro i fattori uguali, si ottiene una fattorizzazione del tipo

$$P = \alpha \prod_{i=1}^{s} (x - \alpha_i)^{m_i}$$

essendo $\alpha_1, \ldots, \alpha_s$ le radici distinte di P e m_i le rispettive molteplicità (definizione 18.6). Si ha pertanto il seguente

Corollario 21.5 *Sia K algebricamente chiuso e $P \in K[x]$. Se $m_1, \ldots, m_s$ sono le molteplicità delle radici di P, allora $\sum_{i=1}^{s} m_i = \deg P$.*

Osservazione 21.6 Grazie a questo corollario ed al fatto che $\mathbb{C}$ è algebricamente chiuso (teorema 21.2) si ha allora che le successioni nella tesi del teorema 20.8 sono esattamente k.

Radici complesse di un polinomio reale

Proposizione 21.7 *Sia $P \in \mathbb{R}[x]$ e sia $\alpha \in \mathbb{C}$ una radice di P di molteplicità m. Allora anche $\overline{\alpha}$ è una radice di P di molteplicità m.*

Dim. Ricordiamo che la coniugazione $\mathbb{C} \to \mathbb{C}$ è un morfismo di anelli e che se $a \in \mathbb{R} \subset \mathbb{C}$ allora $\overline{a} = a$.

Sia $\alpha \in \mathbb{C}$ una radice di $P = \sum_{i=1}^{n} a_i x^i$ con $a_i \in \mathbb{R}$. Allora:

$$0 = \overline{0} = \overline{P(\alpha)} = \overline{\sum_{i=1}^{n} a_i \alpha^i} = \sum_{i=1}^{n} \overline{a_i \alpha}^i = \sum_{i=1}^{n} a_i \overline{\alpha}^i = P(\bar{\alpha})$$

Quindi $\overline{\alpha}$ è una radice di P.

Sia m la molteplicità di α allora $P = (x-\alpha)^m Q$ con $Q(\alpha) \neq 0$. Sia ora n la molteplicità della radice $\overline{\alpha} \neq \alpha$. Il fatto che $\overline{\alpha}$ è una radice di P di molteplicità n e $\overline{\alpha} \neq \alpha$ garantisce e che $\overline{\alpha}$ è una radice di Q con la stessa molteplicità (esercizio 18.2). Ossia $Q = (x-\overline{\alpha})^n R$ con $R(\overline{\alpha}) \neq 0$, ossia $P = (x-\alpha)^m (x-\overline{\alpha})^n R$ con $R(\overline{\alpha}) \neq 0$ e $R(\alpha) \neq 0$. Supponiamo che $m \geq n$ (ciò non è restrittivo a meno di scambiare i ruoli di α e $\overline{\alpha}$), allora $P = ((x-\alpha)(x-\overline{\alpha}))^n (x-\alpha)^{m-n} R$. Osserviamo che

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha\overline{\alpha} \in \mathbb{R}[x]$$

e quindi, per il l'unicità della divisione euclidea (teorema 17.3) anche $S = (x-\alpha)^{m-n} R \in \mathbb{R}[x]$. Se per assurdo $m > n$ allora α sarebbe una radice di S e quindi anche $\overline{\alpha}$ sarebbe radice di S, ma $S(\overline{\alpha}) \neq 0$ dato che $R(\overline{\alpha}) \neq 0$ e $\overline{\alpha} \neq \alpha$. ❑

Base dello spazio delle soluzioni di un equazione ricorsiva (caso reale)

Supponiamo di avere ora una equazione ricorsiva reale e sia $P \in \mathbb{R}[x]$ il suo polinomio caratteristico. P avrà alcune radici reali $\beta_1, \ldots, \beta_s$ di molteplicità $m_1, \ldots, m_s$, ed alcune radici non reali, che, per quanto visto sopra, sono accoppiate dal coniugio. Siano $\alpha_1, \ldots, \alpha_t$ e $\overline{\alpha_1}, \ldots, \overline{\alpha_t}$ le radici non reali e $n_1, \ldots, n_t$ le loro molteplicità (n_i è la molteplicità di α_i e di $\overline{\alpha_i}$).

Teorema 21.8 *Le successioni*

$$
\begin{array}{cccc}
\beta_1^n & n\beta_1^n & \cdots & n^{m_1-1}\beta_1^n \\
\vdots & \vdots & & \vdots \\
\beta_s^n & n\beta_s^n & \cdots & n^{m_s-1}\beta_s^n \\
\frac{\alpha_1^n+\overline{\alpha_1}^n}{2} & n\frac{\alpha_1^n+\overline{\alpha_1}^n}{2} & \cdots & n^{n_1-1}\frac{\alpha_1^n+\overline{\alpha_1}^n}{2} \\
\frac{\alpha_1^n-\overline{\alpha_1}^n}{2i} & n\frac{\alpha_1^n-\overline{\alpha_1}^n}{2i} & \cdots & n^{n_1-1}\frac{\alpha_1^n-\overline{\alpha_1}^n}{2i} \\
\vdots & \vdots & & \vdots \\
\frac{\alpha_t^n+\overline{\alpha_t}^n}{2} & n\frac{\alpha_t^n+\overline{\alpha_t}^n}{2} & \cdots & n^{n_t-1}\frac{\alpha_t^n+\overline{\alpha_t}^n}{2} \\
\frac{\alpha_t^n-\overline{\alpha_t}^n}{2i} & n\frac{\alpha_t^n-\overline{\alpha_t}^n}{2i} & \cdots & n^{n_t-1}\frac{\alpha_t^n-\overline{\alpha_t}^n}{2i}
\end{array}
$$

sono una base reale dello spazio vettoriale $\mathcal{V}$ delle soluzioni dell'equazione ricorsiva reale.

Dim. Per il teorema 20.8 si ha che le successioni

$$
\begin{array}{cccc}
\beta_1^n & n\beta_1^n & \cdots & n^{m_1-1}\beta_1^n \\
\vdots & \vdots & & \vdots \\
\beta_s^n & n\beta_s^n & \cdots & n^{m_s-1}\beta_s^n \\
\alpha_1^n & n\alpha_1^n & \cdots & n^{n_1-1}\alpha_1^n \\
\overline{\alpha_1}^n & n\overline{\alpha_1}^n & \cdots & n^{n_1-1}\overline{\alpha_1}^n \\
\vdots & \vdots & & \vdots \\
\alpha_t^n & n\alpha_t^n & \cdots & n^{n_t-1}\alpha_t^n \\
\overline{\alpha_t}^n & n\overline{\alpha_t}^n & \cdots & n^{n_t-1}\overline{\alpha_t}^n
\end{array}
$$

sono una base dello spazio delle soluzioni complesse dell'equazione ricorsiva. Per ogni h e j indichiamo con $A^{h,j}$ la successione $n^h\alpha_j^n$ e con $\overline{A}^{h,j}$ la successione $n^h\overline{\alpha_j}^n$. Osserviamo che lo spazio generato da $A^{h,j}$ e $\overline{A}^{h,j}$ è lo stesso di quello generato da $(A^{h,j}+\overline{A}^{h,j})/2$ e $(A^{h,j}-\overline{A}^{h,j})/2i$, quindi nella base complessa dello spazio $\mathcal{V}$ si possono sostituire le successioni $A^{h,j}$ e $\overline{A}^{h,j}$ con le successioni $(A^{h,j}+\overline{A}^{h,j})/2$ e $(A^{h,j}-\overline{A}^{h,j})/2i$ ottenendo ancora una base di $\mathcal{V}$. Ma ora

$$
\begin{array}{rcl}
\left(\frac{A^{h,j}+\overline{A}^{h,j}}{2}\right)_n & = & \frac{A_n^{h,j}+\overline{A}_n^{h,j}}{2} = \frac{n^h\alpha_j^n+n^h\overline{\alpha_j}^n}{2} = n^h\frac{\alpha_j^n+\overline{\alpha_j}^n}{2} = n^h\frac{\alpha_j^n+\overline{\alpha_j^n}}{2} \\
\left(\frac{A^{h,j}-\overline{A}^{h,j}}{2i}\right)_n & = & \frac{A_n^{h,j}-\overline{A}_n^{h,j}}{2i} = \frac{n^h\alpha_j^n-n^h\overline{\alpha_j}^n}{2i} = n^h\frac{\alpha_j^n-\overline{\alpha_j}^n}{2i} = n^h\frac{\alpha_j^n-\overline{\alpha_j^n}}{2i}
\end{array}
$$

sono successioni reali. Da ciò segue allora la tesi. ❑

Osservazione 21.9 Si osservi che se $\alpha_i = \rho_i(\cos\theta_i + i\sin\theta_i)$, allora $\alpha_i^n = \rho_i^n(\cos(n\theta_i) + i\sin(n\theta_i))$ e quindi

$$
\begin{array}{rcl}
\frac{\alpha_i^n+\overline{\alpha_i}^n}{2} & = & \frac{\alpha_i^n+\overline{\alpha_i^n}}{2} = \rho_i^n\cos(n\theta_i) \\
\frac{\alpha_i^n-\overline{\alpha_i}^n}{2i} & = & \frac{\alpha_i^n-\overline{\alpha_i^n}}{2i} = \rho_i^n\sin(n\theta_i)
\end{array}
$$

Ma allora la base dello spazio $\mathcal{V}$ data nel teorema precedente può essere riscritta come:

$$\begin{array}{cccc}
\beta_1^n & n\beta_1^n & \cdots & n^{m_1-1}\beta_1^n \\
\vdots & \vdots & & \vdots \\
\beta_s^n & n\beta_s^n & \cdots & n^{m_s-1}\beta_s^n \\
\rho_1^n\cos(n\theta_1) & n\rho_1^n\cos(n\theta_1) & \cdots & n^{n_1-1}\rho_1^n\cos(n\theta_1) \\
\rho_1^n\sin(n\theta_1) & n\rho_1^n\sin(n\theta_1) & \cdots & n^{n_1-1}\rho_1^n\sin(n\theta_1) \\
\vdots & \vdots & & \vdots \\
\rho_t^n\cos(n\theta_t) & n\rho_t^n\cos(n\theta_t) & \cdots & n^{n_t-1}\rho_t^n\cos(n\theta_t) \\
\rho_t^n\sin(n\theta_t) & n\rho_t^n\sin(n\theta_t) & \cdots & n^{n_t-1}\rho_t^n\sin(n\theta_t)
\end{array}$$

Lezione 22 (3 maggio 1999 h. 9.30-10.30)

Definizione di anello booleano

Definizione 22.1 *Sia R un anello con identità, si dice che R è un* anello booleano, *o anche* anello di Boole, *se*

$$a^2 = a \quad \forall a \in R$$

Esempio 22.2 $\mathbb{Z}/_{2\mathbb{Z}}$ è un anello booleano, infatti $0^2 = 0$ e $1^2 = 1$ e 0 e 1 sono gli unici elementi di $\mathbb{Z}/_{2\mathbb{Z}}$.

Esempio 22.3 Sia X un insieme, l'anello $(\mathcal{P}(X), \triangle, \cap)$ è un anello booleano. Infatti $A \cap A = A$ per ogni $A \in \mathcal{P}(X)$.

Esercizio 22.1 Si provi che se R è un anello booleano e X è un insieme, allora R^X è un anello booleano.

Esercizio 22.2 Sia X un insieme, si provi che l'anello $(\mathbb{Z}/_{2\mathbb{Z}})^X$ è isomorfo a $(\mathcal{P}(X), \triangle, \cap)$.

Prime proprietà degli anelli booleani

Proposizione 22.4 *Sia R un anello booleano allora*

1. $\operatorname{char} R = 2$,
2. *R è commutativo.*

Dim. (1). Sia $a \in R$ allora $a = a^2 = (-a)^2 = -a$, quindi $a + a = 0$. In particolare $1 + 1 = 0$, ossia $\operatorname{char} R = 2$.

(2). Siano $a, b \in R$ allora,

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

da cui si ricava che $ab + ba = 0$ e quindi $ab = -ba$. Per quanto visto al punto precedente $-ba = ba$ e quindi $ab = ba$. ❏

Esercizio 22.3 Sia R un anello booleano. Si provi che l'unico elemento invertibile di R è 1.

Esercizio 22.4 Sia $(R, +, \cdot)$ un anello booleano, si provi che anche $(R, \oplus, \odot)$ è un anello booleano, essendo

$$\begin{aligned} a \oplus b &= a + b + 1 \\ a \odot b &= a + b + ab. \end{aligned}$$

Ideali massimali

Definizione 22.5 *Sia R un anello commutativo con identità, diremo che un ideale $M \subseteq R$ è* massimale *se $M \neq R$ e gli unici ideali I tali che $M \subseteq I \subseteq R$ sono I e R. In simboli*

$$I \text{ ideale e } M \subseteq I \subseteq R \Rightarrow I = M \text{ o } I = R.$$

Proposizione 22.6 *Sia R un anello commutativo con identità e $M \subseteq R$ un ideale. $R/_M$ è un campo se e solo se M è massimale.*

Dim. Supponiamo che M sia massimale e sia $a + M \in R/_M$ diverso da $0 + M$ ossia $a \notin M$. Consideriamo l'insieme

$$I = \{xa + M \mid x \in R, m \in M\}$$

I è un ideale (si vedano gli esercizi 15.3, 15.4 e 15.5), $I \supseteq M$ e $a \in I$ quindi $I \neq M$, per la massimalità di M allora $I = R$ e quindi $1 \in I$, ossia esiste $x \in R$ e $m \in M$ tale che $1 = ax + m$ ossia $ax + M = 1 + M$ e pertanto $(a + M)(x + M) = 1 + M$, ovvero $a + M$ è invertibile.

Supponiamo ora che $R/_M$ sia un campo. Sia $I \supsetneq M$ un ideale, e sia $a \in I \setminus M$. Dato che $a + M \neq 0 + M$ e $R/_M$ è un campo, allora esiste $x + M$ tale che $(a + M)(x + M) = 1 + M$ ossia tale che $ax - 1 \in M$. Ma allorea esiste un $m \in M$ tale che $ax - 1 = m$ e quindi $1 = m - ax$. Ora, $m \in M \subset I$, $a \in I$ e quindi $ax \in I$, per cui $1 \in I$. Da ciò segue che $I = R$ (esercizio 15.6) e quindi M è massimale. ❑

Vale il seguente teorema di cui omettiamo la dimostrazione:

Teorema 22.7 *Sia R un anello e sia $r \in R$ un elemento non invertibile. Allora esiste un ideale massimale di R che contiene r.*

Teorema di rappresentazione degli anelli booleani

Lemma 22.8 *Sia R un anello booleano e sia $M \subseteq R$ un ideale massimale. Allora per ogni $r, r' \in R$ si ha*

1. $r + r' \notin M \iff r \notin M$ e $r' \in M$ oppure $r \in M$ e $r' \notin M$

2. $rr' \notin M \iff r \notin M$ e $r' \notin M$

Dim. Sia $\pi : R \to R/_M$ la proiezione a quoziente, allora per ogni $a \in R$ si ha $a^2 - a = 0$ e quindi $0 = \pi(0) = \pi(a^2 - a) = \pi(a)^2 - \pi(a)$, ossia per ogni $A \in R/_M$ si ha $A^2 - A = 0$ ossia $A(A-1) = 0$. Ma ora, dato che M è massimale, $R/_M$ è un campo (proposizione 22.6), in particolare è un dominio di integrità (corollario 14.11) e pertanto da $A(A-1) = 0$ si deduce che $A = 0$ oppure $A = 1$. $R/_M$ ha solo i due elementi $0 + M$ e $1 + M$, è quindi isomorfo a $\mathbb{Z}/_{2\mathbb{Z}}$, e quindi per ogni $A, A' \in R/_M$ si ha:

$$\begin{aligned} A + A' = 1 &\iff A = 1 \text{ e } A' = 0 \text{ oppure } A = 0 \text{ e } A' = 1 \\ AA' = 1 &\iff A = 1 \text{ e } A' = 1 \end{aligned}$$

che possono essere riscritte

$$\begin{aligned} A + A' \neq 0 &\iff A \neq 0 \text{ e } A' = 0 \text{ oppure } A = 0 \text{ e } A' \neq 0 \\ AB \neq 0 &\iff A \neq 0 \text{ e } A' \neq 0 \end{aligned}$$

Ma allora la tesi si ottiene prendendo $A = r + M$ e $A' = r' + M$ e ricordando che per ogni $r \in R$ si ha $r + M = 0 + M$ se e solo se $r \in M$. ❑

Indichiamo con $\operatorname{Max} R$ l'insieme degli ideali massimali di R e consideriamo l'applicazione $\varepsilon : R \to \mathcal{P}(\operatorname{Max} R)$ definita da:

$$\varepsilon(r) = \{M \in \operatorname{Max} R \mid r \notin M\} \tag{28}$$

Teorema 22.9 (di rappresentazione) *Sia R un anello booleano. Allora l'applicazione $\varepsilon : (R, +, \cdot) \to (\mathcal{P}(\operatorname{Max} R), \triangle, \cap)$ definita sopra è un morfismo iniettivo di anelli con identità.*

Se R è finito, ε è anche surgettiva, e quindi un isomorfismo.

Lezione 23 (5 maggio 1999 h. 9.30-10.30)

Dimostrazione del teorema di rappresentazione (22.9)

Dim. Per definizione di ε, dati $r \in R$ e $m \in \operatorname{Max} R$, si ha che $M \in \varepsilon(r)$ se e solo se $r \notin M$. Ma allora le due relazioni date dal lemma precedente (22.8) possono essere riscritte

$$\begin{aligned} M \in \varepsilon(r + r') &\iff M \in \varepsilon(r) \text{ e } M \notin \varepsilon(r') \text{ oppure } M \notin \varepsilon(r) \text{ e } M \in \varepsilon(r') \\ M \in \varepsilon(rr') &\iff M \in \varepsilon(r) \text{ e } M \in \varepsilon(r') \end{aligned}$$

ossia

$$\begin{aligned} M \in \varepsilon(r + r') &\iff M \in \varepsilon(r) \triangle \varepsilon(r') \\ M \in \varepsilon(rr') &\iff M \in \varepsilon(r) \cap \varepsilon(r') \end{aligned}$$

ovvero

$$\begin{aligned} \varepsilon(r+r') &= \varepsilon(r) \bigtriangleup \varepsilon(r') \\ \varepsilon(rr') &= \varepsilon(r) \cap \varepsilon(r') \end{aligned}$$

quindi ε è un morfismo di anelli.

Proviamo ora che ε porta l'identità di R nell'identità di $\mathcal{P}(\operatorname{Max} R)$, ossia che $\varepsilon(1) = \operatorname{Max} R$. Infatti se $M \in \operatorname{Max} R$ allora $M \neq R$ (definizione 22.5) quindi $1 \notin R$ (esercizio 15.6), ossia $M \in \varepsilon(1)$.

ε è iniettivo. Supponiamo che $\varepsilon(r) = \varnothing$, allora, dato che ε è un morfismo di anelli con identità, $\varepsilon(1+r) = \varepsilon(1) \bigtriangleup \varepsilon(r) = \max R \bigtriangleup \varnothing = \operatorname{Max} R$. Allora $1+r$ è invertibile, altrimenti esisterebbe un ideale massimale che lo contiene (teorema 22.7). Ma allora per l'esercizio 22.3 $1 + r = 1$ e quindi $r = 0$.

Proviamo l'ultima parte dell teorema. Dato che R è finito, anche $\operatorname{Max} R$ lo è e quindi anche tutti i suoi sottoinsiemi lo sono. Sia allora $X \subseteq \operatorname{Max} R$ e proviamo per induzione sul numero di elementi di X che allora esiste $r \in R$ tale che $\varepsilon(r) = X$. Se X ha 0 elementi, allora $X = \varnothing$ e $\varepsilon(0) = \varnothing$. Supponiamo che X abbia un solo elemento, ossia $X = \{M\}$. Dato che R è finito $R \setminus M$ è finito (e non vuoto perché $M \neq R$), sia $R \setminus M = \{x_1, \dots, x_s\}$. Consideriamo $r = x_1 \dots x_s$ il prodotto di tali x_i. Usando il lemma 22.8, si ha

$$\left.\begin{array}{r}\left.\begin{array}{r}\left.\begin{array}{r}\left.\begin{array}{l}x_1\notin M\\ x_2\notin M\end{array}\right\}\Rightarrow x_1x_2\notin M\\ x_3\notin M\end{array}\right\}\Rightarrow \\ \ddots \end{array}\right\}\Rightarrow x_1\cdots x_{s-1}\notin M \\ x_s\notin M\end{array}\right\}\Rightarrow x_1\cdots x_s\notin M$$

quindi $M \in \varepsilon(r)$. D'altra parte se $N \in \operatorname{Max} R$ e $N \neq M$ allora $N \not\subseteq M$ (altrimenti non sarebbe massimale) e quindi esiste i tale che $x_i \in N$. Dato che N è un ideale, $r = x_1 \cdots x_i \cdots x_s \in N$ e quindi $N \notin \varepsilon(r)$. Pertanto $\varepsilon(r) = \{M\} = X$.

Supponiamo ora che X abbia $n+1$ elementi, allora possiamo scrivere $X = Y \cup Z$ con $X \cap Y = \varnothing$ e Z costituito da un solo elemento. Allora Y ha n elementi, per ipotesi di induzione esiste r tale che $\varepsilon(r) = Y$ e per il caso $n = 1$ esiste r' tale che $\varepsilon(r') = Z$. Ma allora

$$\varepsilon(r+r') = \varepsilon(r) \bigtriangleup \varepsilon(r') = Y \bigtriangleup Z = Y \cup Z \setminus y \cap Z = X \cup \varnothing = X.$$

Questo conclude la dimostrazione. ❏

Definizione di insieme parzialmente ordinato

Definizione 23.1 *Sia X un insieme, una relazione $\leq$ su X si dirà un* ordinamento parziale *se*

1. è riflessiva*: $x \leq x$ per ogni $x \in X$;*

2. *è* antisimmetrica*:* $x \leq y$ *e* $y \leq x \Rightarrow x = y$*;*

3. *è* transitiva*:* $x, ley, y \leq z \Rightarrow x \leq z$*.*

Un ordinamento parziale si dirà un ordinamento totale *se in più*

4. per ogni $x, y \in X$ *si ha che o* $x \leq y$ *o* $y \leq x$*.*

Una coppia $(X, \leq)$*, dove* $\leq$ *è un ordinamento parziale, si dirà un* insieme parzialmente ordinato*, se* $\leq$ *è un ordinamento totale sidirà un insieme totalmente ordinato o anche una* catena*.*

Esempio 23.2 Gli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ dotati dell'ordinamento naturale, sono degli insiemi totalmente ordinati.

Sia X un insieme, allora la relazione di inclusione $\subseteq$ è un ordinamento sull'insieme delle sue parti $\mathcal{P}(X)$.

La relazione $\big|$ è un ordinamento parziale (si veda la proposizione 3.3) sull'insieme $\mathbb{N}$ dei numeri naturali.

Esercizio 23.1 Se $Y \subset X$ e $\leq$ è un ordinamento su X, la relazione su Y $\leq_Y = \leq \cap Y \times Y$ è ancora un ordinamento che viene chiamato l'*ordinamento indotto* da $\leq$ su Y.

Esercizio 23.2 Se $\leq$ è un ordinamento parziale su X allora la relazione $\geq$ definita da $x \geq y \iff y \leq x$ è un ordinamento su X, che viene chiamato l'*ordinamento inverso*

Definizione 23.3 *Sia* X *un insieme parzialmente ordinato e sia* $a \in X$ *e* $Y \subseteq X$ *si dirà che:*

a è massimo *di* X *se:*	$x \leq a$ *per ogni* $x \in X$
a è minimo *di* X *se:*	$a \leq x$ *per ogni* $x \in X$
a è maggiorante *di* Y *se:*	$y \leq a$ *per ogni* $y \in Y$
a è minorante *di* Y *se:*	$a \leq y$ *per ogni* $y \in Y$
a è estremo superiore *di* Y *se:*	a *è minimo dei maggioranti di* Y
	(i.e. $y \leq x$ *per ogni* $y \in Y \Rightarrow a \leq y$*)*
a è estremo inferiore *di* Y *se:*	a *è massimo dei minoranti di* Y
	(i.e. $x \leq y$ *per ogni* $y \in Y \Rightarrow y \leq a$*)*
a è massimale*:*	$a \leq x \Rightarrow x = a$
a è minimale*:*	$x \leq a \Rightarrow x = a$

Esercizio 23.3 Si provi che in $(\mathbb{N}, |)$ gli insiemi del tipo $\{a, b\}$ hanno sempre estremo inferiore ed estremo superiore.

Esercizio 23.4 Sia X un insieme parzialmente ordinato, $Y \subset X$. Si provino le seguenti asserzioni:

1. Il minimo di X se esiste è unico.

2. il massimo di X se esiste è unico.
3. L'estremo inferiore di Y se esiste è unico.
4. L'estremo superiore di Y se esiste è unico.
5. Se a è minimo di X allora a è minimale. È vero il viceversa?
6. Se a è massimo di X allora a è massimale. È vero il viceversa?
7. se a è minimo di Y allora a è anche estremo inferiore. È vero il viceversa?
8. se a è massimo di Y allora a è anche estremo superiore. È vero il viceversa?

Ordinamento degli anelli booleani

Sia R un anello booleano (definizione 22.1) definiamo una rela zione $\leq$ su R ponendo

$$a \leq b \iff a = ab. \tag{29}$$

Proposizione 23.4 *La relazione appena definita è un ordinamento parziale su R.*

Dim. Diamo due dimostrazioni di questo fatto.

Prima dimostrazione. La relazione è riflessiva. Infatti se $a \in R$ allora, poicé R è booleano, $a = aa$ e quindi $a \leq a$.

La relazione è antisimmetrica. Se $a \leq b$ e $b \leq c$ allora, per definizione di $\leq$, $a = ab$ e $b = ba$. Dato che R è commutativo (proposizione 22.4), $ab = ba$ e quindi $a = b$.

La relazione è transitiva. Se $a \leq b$ e $b \leq c$ allora $a = ab$ e $b = bc$. Sostituiendo la seconda nella prima si ha allora che $a = abc$ ed usando di nuovo la prima $abc = ac$ e quindi $a = ac$, ossia $a \leq c$.

Seconda dimostrazione. Sia ε il morfismo del teorema di rappresentazione (22.9). Allora, dato che ε è iniettivo, si ha:

$$\begin{aligned} a \leq b \quad &\iff \quad ab = a \iff \varepsilon(ab) = \varepsilon(a) \iff \\ &\iff \quad \varepsilon(a) \cap \varepsilon(b) = \varepsilon(a) \iff \varepsilon(a) \subseteq \varepsilon(b) \end{aligned}$$

dato che $\subseteq$ è un ordinamento parziale, anche $\leq$ lo è. ❑

Nel seguito, quando parleremo di *ordinamento di un anello booleano*, ci riferiremo sempre a quello definito dalla precedente proprsizione.

Lezione 24 (10 maggio 1999 h. 9.30-10.30)

Definizione di reticolo

Definizione 24.1 *Sia $(L, \leq)$ un insieme parzialmente ordinato. Diremo che $(L, \leq)$ è un* reticolo *se per ogni $x, y \in L$ l'insieme $\{x, y\}$ ha estremo inferiore ed estremo superiore.*

Per ogni $x, y \in L$ si denota $x \vee y = \sup\{x, y\}$ e $x \wedge y = \inf\{x, y\}$.

Osservazione 24.2 Dalle definizioni (23.3) e dall'unicità (esercizio 23.4) di estremo inferiore ed estremo superiore si ha immediatamente che $x \vee y$ è caratterizzato da:

1. $x \leq x \vee y$ e $y \leq x \vee y$;

2. se $x \leq z$ e $y \leq z$ allora $x \vee y \leq z$.

e $x \wedge y$ è caratterizzato da:

1. $x \wedge y \leq x$ e $x \wedge y \leq y$;

2. se $z \leq x$ e $z \leq y$ allora $z \leq x \wedge y$.

Esempio 24.3 $(\mathcal{P}(X), \subseteq)$ è un reticolo. Infatti se $A, B \in \mathcal{P}(X)$ allora

$$\begin{gathered} A \cap B \subseteq A \text{ e } A \cap B \subseteq B \\ C \subseteq A \text{ e } C \subseteq B \Rightarrow C \subseteq A \cap B \end{gathered}$$

e quindi $A \wedge B = A \cap B$. Analogamente

$$\begin{gathered} A \subseteq A \cup B \text{ e } B \subseteq A \cup B \\ A \subseteq C \text{ e } B \subseteq C \Rightarrow A \cup B \subseteq C \end{gathered}$$

e quindi $A \vee B = A \cup B$.

$(\mathbb{N}, |)$ è un reticolo (esercizio 23.3).

Gli anelli booleani sono reticoli.

Proposizione 24.4 *Sia R un anello booleano e sia $\leq$ il suo ordinamento (proposizione 23.4). Allora $(R, \leq)$ è un reticolo.*

Dim. Siano $a, b \in R$ allora, usando l'associatività del prodotto e la commutatività (proposizione 22.4) degli anelli booleani,

$$\begin{array}{rcccc} (ab)a & = & a^2b = ab & \iff & ab \leq a \\ (ab)b & = & ab^2 = ab & \iff & ab \leq b \end{array}$$

inoltre sia $c \leq a$ e $c \leq b$, ovvero $ca = c$ e $cb = c$ si ha

$$(ab)c = a(bc) = ac = c \iff c \leq ab.$$

Quindi, per quanto osservato sopra (24.2) si ha che $ab = a \wedge b$.

Proviamo ora che $a + b + ab = a \vee b$, infatti, usando nuovamente la commutatività il fatto che $\operatorname{char} R = 2$ (proposizione 22.4), si ha

$$\begin{array}{rcccc} a(a+b+ab) & = & a^2 + ab + a^2b = a + ab + ab = a & \iff & a \leq a+b+ab \\ b(a+b+ab) & = & ba + b^2 + ab^2 = b + ab + ab = b & \iff & b \leq a+b+ab \end{array}$$

inoltre se $a \leq c$ e $b \leq c$ allora

$$(a+b+ab)c = ac+bc+abc = a+b+ab \iff a+b+ab \leq c$$

e quindi la tesi.

Diamo un'altra dimostrazione, Consideriamo il morfismo ε di di rappresentazione (teorema 22.9). Dal fatto che ε è un morfismo di anelli si ha che

$$\begin{aligned} \varepsilon(ab) &= \varepsilon(a) \cap \varepsilon(b) \\ \varepsilon(a+b+ab) &= \varepsilon(a) \bigtriangleup \varepsilon(b) \bigtriangleup (\varepsilon(a) \cap \varepsilon(b)) = \varepsilon(a) \cup \varepsilon(b). \end{aligned}$$

Dato che $\varepsilon(a) \cap \varepsilon(b)$ e $\varepsilon(a) \cup \varepsilon(b)$ sono l'estremo inferiore e superiore rispetto a $\subseteq$ e poiché per ogni $x, y \in R$ si ha che $x \leq y \iff \varepsilon(x) \subseteq \varepsilon(y)$ (si veda la seconda dimostrazione della proposizione 23.4), allora ab e $a+b+ab$ sono l'estremo inferiore e superiore rispetto a $\leq$. ❑

Principio di dualità dei reticoli

Osservazione 24.5 Sia $(L, \leq)$ un reticolo e sia $\geq$ l'ordinamento inverso (esercizio 23.2). Allora $(L, \geq)$ è un reticolo e

$$\begin{aligned} x \vee_{\geq} y &= x \wedge_{\leq} y \\ x \wedge_{\geq} y &= x \vee_{\leq} y \end{aligned}$$

Ciò segue immediatamente dalle caratterrizzazioni di estremo inferiore ed estremo superiore (osservazione 24.2) dalle quali si vede immediatamente che le proprietà che definiscono l'estremo inferiore rispetto a $\leq$ sono quelle che definiscono l'estremo superiore rispetto a $\geq$ e viceversa.

Sia P una proposizione enunciata in termini di $\leq$, $\vee$ e $\wedge$ indichiamo con P^* la *proposizione duale* ossia la proposizione ottenuta da P scambiando $\vee$ con $\wedge$ e $\leq$ con $\geq$.

Teorema 24.6 (principio di dualità) *Sia P una proposizione enunciata in termini di $\leq$, $\vee$ e $\wedge$ e si supponga che in ogni reticolo P sia vera. Allora anche P^* è vera in ogni reticolo.*

Dim. Sia $(L, \leq)$ un reticolo, allora si consideri il reticolo inverso, ossia $(L, \geq)$. Dato che P vale in ogni reticolo, allora vale in $(L, \geq)$. Ma, alla luce di quanto osservato sopra (24.5), la proposizione P "valutata" in $(L, \geq)$ altro non è che la proposizione P^* valutata in $(L, \leq)$. ❑

Prime proprietà dei reticoli

Proposizione 24.7 *Sia $(L, \leq)$ un reticolo, allora per ogni $x, y, z \in L$ si ha:*

1.	$x \vee y = y \vee x$	$x \wedge y = y \wedge x$
2.	$(x \vee y) \vee z = x \vee (y \vee z)$	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
3.	$x \vee (x \wedge y) = x$	$x \wedge (x \vee y) = x$

Le proprietà del punto (3) vengono chiamate proprietà di assorbimento.

Dim. Osserviamo che le asserzioni di ogni riga sono duali una dell'altra, sarà quindi sufficiente, per il principio di dualità, dimostrarne una di ogni riga.

Le (1) sono immediate dalla definizione di estremo superiore e inferiore.

Dimostriamo la prima delle (2). Osserviamo innanzitutto che, dalla prima delle proprietà che caratterizzano $\vee$ (osservazione 24.2) si ha $y \leq x \vee y \leq (x \vee y) \vee z$ e $z \leq (x \vee y) \vee z$. Da queste due relazioni, per la seconda delle proprietà caratterizzanti $\vee$, segue allora che $y \vee z \leq (x \vee y) \vee z$. D'altra parte anche $x \leq x \vee y \leq (x \vee y) \vee z$, quindi $x \vee (y \vee z) \leq (x \vee y) \vee z$. In modo analogo si prova che anche $(x \vee y) \vee z \leq x \vee (y \vee z)$ da cui segue la tesi per la antisimmetria di $\leq$.

Dimostriamo la prima delle (3). $x \leq x$ e $x \wedge y \leq x$, quindi $x \vee (x \wedge y) \leq x$. D,altra parte $x \leq x \vee (x \wedge y)$ e quindi, per la antisimmetria si ha che $x = x \vee (x \wedge y)$, ❑

Esercizio 24.1 Sia $(L, \leq)$ un reticolo, allora per ogni $x, y \in L$

$$x \leq y \iff x = x \wedge y \iff y = x \vee y.$$

Lezione 25 (12 maggio 1999 h. 9.30-10.30)

Reticoli come insiemi con operazioni

Abbiamo visto in precedenza che se $(L, \leq)$ è un reticolo, allora sono definite le due operazioni binarie $\vee, \wedge : L \times L \to L$ che verificano le proprietà commutativa, associativa e di assorbimento (proposizione 24.7). Vediamo come tali proprietà delle due operazioni determinino la struttura del reticolo.

Teorema 25.1 *Sia L un insieme su cui sono definite due operazioni binarie $\vee, \wedge : L \times L \to L$ tali che per ogni $x, y, z \in L$ si abbia:*

1.	$x \vee y = y \vee x$	$x \wedge y = y \wedge x$
2.	$(x \vee y) \vee z = x \vee (y \vee z)$	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
3.	$x \vee (x \wedge y) = x$	$x \wedge (x \vee y) = x$

Allora esiste un ordinamento $\leq$ su L che rende $(L, \leq)$ un reticolo tale che per ogni $x, y \in L$ si ha che $\sup_{\leq}\{x, y\} = x \vee y$ *e* $\inf_{\leq}\{x, y\} = x \vee y$.

Dim. L'esercizio 24.1 ci dice come definire la relazione d'ordine. Definiamo:

$$x \leq y \iff x = x \wedge y.$$

Proviamo che $\leq$ è una relazione d'equivalenza.

$\leq$ è riflessiva. Usando la proprietà di assorbimento si ha che $x = x \vee (x \wedge x)$ e quindi $x \wedge x = x \wedge (x \vee (x \wedge x))$. Ma allora usando ancora la proprietà di assorbimento $x \wedge (x \vee (x \wedge x)) = x$ e quindi $x \wedge x = x$ ossia $x \leq x$.

$\leq$ è antisimmetrica. Siano $x \leq y$ e $y \leq x$, ossia $x \wedge y = x$ e $y \wedge x = x$. Per la commutatività si ha allora che $x \wedge y = y \wedge x$ e quindi $x = y$.

$\leq$ è transitiva. Sia $x \leq y$ e $y \leq z$ ossia $x \wedge y = x$ e $y \wedge z = y$. Allora, usando l'associatività, $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$ e quindi $x \leq z$.

Proviamo ora che $x \wedge y$ è l'estremo inferiore tra x e y. Usando la commutatività, l'associatività ed il già provato fatto che per ogni $x \in L$ si ha $x \wedge x = x$, si ha

$$\begin{array}{lll} (x \wedge y) \wedge x = x \wedge (x \wedge y) = (x \wedge x) \wedge y = x \wedge y & \text{ossia} & x \wedge y \leq x \\ (x \wedge y) \wedge y = x \wedge (y \wedge y) = x \wedge y & \text{ossia} & x \wedge y \leq y \end{array}$$

Sia ora $z \leq x$ e $z \leq y$, ossia $z \wedge x = z$ e $z \wedge y = z$, allora

$$z \wedge (x \wedge y) = (z \wedge x) \wedge y == z \wedge y = z \quad \text{ossia} \quad z \leq x \wedge y.$$

$x \wedge y$ verifica quindi le proprietà caratterizzanti (osservazione24.2) dell'estremo inferiore, e quindi è l'estremo inferiore.

Proviamo ora che $x \vee y$ è l'estremo superiore tra x e y. Usando le proprietà commutative e di assorbimento, si ha

$$\begin{array}{lll} (x \vee y) \wedge x = x \vee (x \wedge y) = x & \text{ossia} & x \leq x \vee y \\ (x \vee y) \wedge y = y \wedge (y \vee x) = y & \text{ossia} & y \leq x \vee y \end{array}$$

Sia ora $x \leq z$ e $y \leq z$ ossia $x \wedge z = x$ e $y \wedge z = y$. Allora, usando le proprietà di assorbimento e la commutatività, si ha che da $x \wedge z = x$ si ha che $z = (x \wedge z) \vee z = x \vee z$ e, analogamente, $z = y \vee z$, ma allora, usando queste relazioni, l'associatività e la proprietà di assorbimento, si ha

$$\begin{array}{ll} (x \vee y) \wedge z = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge (x \vee (y \vee z)) = & \\ \quad = (x \vee y) \wedge ((x \vee y) \vee z)) = (x \vee y) & \text{ossia} \quad x \vee y \leq z \end{array}$$

Questo, prova che $x \vee y$ è l'estremo superiore tra x e y (osservazione 24.2).

Si poteva anche osservare che dalle tre proprietà si ricava che $x = x \wedge y \iff y = x \vee y$ (si veda l'esercizio seguente), ossia $x \leq y$ se e solo se $y = x \vee y$. L'ultima proprietà poteva più semplicemente essere mostrata nel seguente modo: se $x \leq z$ e $y \leq z$ allora $z = x \vee z$ e $z = y \vee z$, ma allora

$$(x \vee y) \vee z = x \vee (y \vee z) = x \vee z = z \quad \text{ossia} \quad x \vee y \leq z.$$

❏

Osservazione 25.2 La proposizione 24.7 ed il teorema precedente mostrano che è completamente equivalente definire un reticolo in termini di ordinamento (definizione 24.1) oppure definirlo come insieme dotato di due operazioni commutative, associative e che verificano la proprietà di assorbimento. Le due strutture algebrica (data dalle proprietà delle operazioni) e d'ordine sono due facce della stessa medaglia e che possono quindi essere usate indifferentemente a seconda delle necessità.

Esercizio 25.1 Si dimostri usando soltanto le proprietà commutativa, associativa e di assorbimento delle due operazioni, che in un reticolo $x \vee y = y \iff x \wedge y = x$.

Definizione di complemento

Definizione 25.3 *Sia L un reticolo diremo che L è* limitato *se ha massimo e minimo, che saranno denotati rispettivamente con* 0 *e* 1*. Ossia, nel linguaggio dell'ordinamento*

$$\exists 0, 1 \in L : x \leq 1 \text{ e } 0 \leq x \quad \forall x \in L$$

o, equivalentemente, nel linguaggio algebrico

$$\exists 0, 1 \in L : x \wedge 1 = x \text{ e } x \wedge 0 = 0 \quad \forall x \in L$$

che, in virtù di quanto visto nell'esercizio 24.1, equivale a dire

$$\exists 0, 1 \in L : x \vee 1 = 1 \text{ e } x \vee 0 = x \quad \forall x \in L.$$

Se L è un reticolo limitato, diremo che $x' \in L$ è un complemento *di x se:*

$$x \vee x' = 1 \qquad x \wedge x' = 0.$$

Un reticolo limitato in cui ogni elemento ha un complemento di dice complementato

Osservazione 25.4 Rispetto alla struttura algebrica, lo 0 è elemento neutro per $\vee$ mentre 1 è un elemento neutro per $\wedge$.

Definizione di reticolo distributivo

Definizione 25.5 *Diremo che un reticolo L è* distributivo *se valgono le seguenti:*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad \forall x, y \in L$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \forall x, y \in L$$

Esercizio 25.2 Sia L un reticolo. Si provi che le due proposizioni

1. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad \forall x, y \in L$
2. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \forall x, y \in L$

sono equivalenti.

In altri termini, nella definizione che abbiamo dato una delle due richieste è superflua, e quindi per verificare che un reticolo è distributivo è sufficiente mostrarne una delle due.

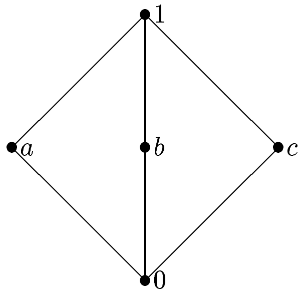
Proposizione 25.6 *Sia L un reticolo distributivo e limitato. Se $x \in L$ ha un complemento, allora tale complemento è unico.*

Dim. Supponiamo che x_1 e x_2 siano due complementi di x, allora

$$x_1 = x_1 \wedge 1 = x_1 \wedge (x \vee x_2) = (x_1 \wedge x) \vee (x_1 \wedge x_2) = 0 \vee (x_1 \wedge x_2) = (x_1 \wedge x_2)$$

scambiando x_1 con x_2 si ottiene anche $x_2 = x_2 \wedge x_1$ e quindi, $x_1 = x_2$. ❑

Osservazione 25.7 La distributività è essenziale per l'unicità del complemento. Si prenda ad esempio il reticolo schemattizzato dal seguente diagramma:



intendendo con questo che $0 \leq x$ e $x \leq 1$ per ogni x e che a, b, c non sono tra loro confrontabili. Allora chiaramente sia b che c sono dei complementi per a ed infatti il reticolo non è distributivo:

$$a \vee (b \wedge c) = a \vee 0 = a$$

mentre

$$(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1.$$

Definizione di algebra di Boole

Definizione 25.8 *Un reticolo distributivo, e complementato viene chiamato un'*algebra di Boole*.*

Esempio 25.9 Se X è un insieme il reticolo $\mathcal{P}(X)$ delle sue parti è un'algebra di Boole. Valgono infatti le relazioni di distributività ed il complemento di un $A \in \mathcal{P}(X)$ non è altro che il suo complementare insiemistico $\complement A = X \setminus A$.

Gli anelli booleani sono algebre di Boole

Teorema 25.10 *Sia R un anello booleano allora R, con la sua struttura di reticolo (proposizione 24.4) è un'algebra di Boole.*

Dim. Dobbiamo dimostrare che R è limitato, complementato e distributivo. Ricordiamo che la struttura di reticolo di R è data dll'ordinamento parziale $a \leq b \iff ab = a$ per la quale si ha $a \vee b = a + b + ab$ e $a \wedge b = ab$.

Osserviamo che $a \wedge 0 = a0 = o0$ per ogni $a \in R$ e quindi lo 0 dell'anello è anche lo 0 del reticolo.

Se $a \in R$ allora $a \wedge 1 = a1 = a$ e quindi l'1 dell'anello è anche l'1 del reticolo.

Se $a \in R$ allora

$$\begin{aligned} a \wedge (1+a) &= a(1+a) = a + a^2 = a + a = 0 \\ a \vee (1+a) &= a + (1+a) + a(1+a) = \\ &= a + 1 + a + a + a^2 = 1 + a + a + a + a = 1. \end{aligned}$$

quindi $(1+a)$ è un complemento di a.

Proviamo che è distributivo.

$$a \vee (b \wedge c) = a \vee (bc) = a + bc + a(bc) = a + bc + abc$$

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= (a+b+ab) \wedge (a+c+ac) = (a+b+ab)(a+c+ac) = \\ &= a^2 + ac + a^2c + ba + bc + bac + aba + abc + abac = \\ &= a^2 + ac + a^2c + ab + bc + abc + a^2b + abc + a^2bc = \\ &= a + ac + ac + ab + bc + abc + ab + abc + abc = \\ &= a + bc + abc \end{aligned}$$

e quindi $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Per quanto detto nell'esercizio 25.2, possiamo allora affermare che il reticolo è distributivo. ❏

Lezione 26 (17 maggio 1999 h. 9.30-11.30)

Prime proprietà delle algebre di Boole

Proposizione 26.1 *Sia L un'algebra di Boole. Allora*

1. $\forall a \in L$ *si ha* $(a')' = a$;
2. $\forall a, b \in L$ *si ha* $(a \wedge b)' = a' \vee b'$;
3. $\forall a, b \in L$ *si ha* $(a \vee b)' = a' \wedge b'$.

Le proprietà (2) e (3) vengono chiamate le leggi di de Morgan.

Dim. (1). a' è il complemento di a, quindi $a \vee a' = 1$ e $a \wedge a' = 0$. Ma allora, a è un complemento di a', dall'unicità del complemento (proposizione 25.6) segue allora la tesi.

(2). Usando le proprietà distributive, commutative di $\wedge$ e $\vee$ e le proprietà dello 0 e dell'1 si ha:

$$\begin{array}{rcll} (a \wedge b) \vee (a' \vee b') & = & (a' \vee b') \vee (a \wedge b) & \text{(commutativa)} \\ & = & ((a' \vee b') \vee a) \wedge ((a' \vee b') \vee b) & \text{(distributiva)} \\ & = & (a \vee (a' \vee b)) \wedge ((a' \vee b') \vee b) & \text{(commutativa)} \\ & = & ((a \vee a') \vee b) \wedge (a' \vee (b' \vee b) & \text{(associativa)} \\ & = & (1 \vee b) \wedge (a' \vee 1) & \text{(complemento)} \\ & = & 1 \wedge 1 = 1 & (1) \end{array}$$

ed analogamente

$$\begin{array}{rcll} (a \wedge b) \wedge (a' \vee b') & = & ((a \wedge b) \wedge a') \vee ((a \wedge b) \wedge b') & \text{(distributiva)} \\ & = & (a' \wedge (a \wedge b)) \vee ((a \wedge b) \wedge b') & \text{(commutativa)} \\ & = & ((a' \wedge a) \wedge b) \vee (a \wedge (b \wedge b')) & \text{(associativa)} \\ & = & (0 \wedge b) \vee (a \wedge 0) & \text{(complemento)} \\ & = & 0 \vee 0 = 0 & (0) \end{array}$$

Quindi $a' \vee b'$ è un complemento di $a \wedge b$. Per l'unicità del complemento (proposizione 25.6) si ha la tesi.

(3). Applichiamo la (2) a a' e b' si ottiene

$$(a')' \vee (b')' = (a' \wedge b')'$$

e quindi per la (1),

$$a \vee b = (a' \wedge b')'$$

Complementando entrambi i membri ed usando di nuovo la (1) si ha allora

$$(a \vee b)' = ((a' \wedge b')')' = a' \wedge b'$$

che è la tesi. ❑

Le algebre di Boole sono anelli booleani

Sia L un'algebra di Boole, definiamo due operazioni binarie su L ponendo:

$$\begin{array}{rcl} a + b & = & (a \wedge b') \vee (a' \wedge b) \\ ab & = & a \wedge b \end{array}$$

Teorema 26.2 *Sia L un'algebra di Boole, allora L con le operazionei $+$ e $\cdot$ appena definite è un anello booleano.*

Dim. $+$ è commutativa. Segue immediatamente dalla commutatività di $\vee$ e $\wedge$, infatti

$$b + a = (b \wedge a') \vee (b' \wedge a) = (b' \wedge a) \vee (b \wedge a') = (a \wedge b') \vee (a' \wedge b) = a + b$$

$+$ è associativa. Siano $a, b, c \in L$ allora, dalla definizione di $+$ si ha

$$
\begin{aligned}
(a+b)+c &= ((a \wedge b') \vee (a' \wedge b)) + c \\
&= (((a \wedge b') \vee (a' \wedge b)) \wedge c') \vee (((a \wedge b') \vee (a' \wedge b))' \wedge c)
\end{aligned}
$$

Usando la distributività e l'associatività delle operazioni

$$
(((a \wedge b') \vee (a' \wedge b)) \wedge c') \quad = \quad (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')
$$

Usando le formule di de Moivre e le altre proprietà

$$
\begin{aligned}
((a \wedge b') \vee (a' \wedge b))' \wedge c &= (((a \wedge b')' \wedge (a' \wedge b)') \wedge c \\
&= ((a' \vee b'') \wedge (a'' \vee b'))\wedge) \\
&= ((a' \vee b) \wedge (a \vee b')) \wedge c \\
&= ((a' \wedge a) \vee (a' \wedge b') \vee (b \wedge a) \vee (b \wedge b')) \wedge c \\
&= (0 \vee (a' \wedge b') \vee (b \wedge a) \vee 0) \wedge c \\
&= ((a' \wedge b') \vee (b \wedge a)) \wedge c \\
&= (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c)
\end{aligned}
$$

e quindi, in definitiva,

$$
(a+b)+c = (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c)
$$

Ma ora, usando la commutatività di $+$ e la formula appena provata, si ha:

$$
\begin{aligned}
a+(b+c) &= (b+c)+a \\
&= (b \wedge c' \wedge a') \vee (b' \wedge c \wedge a') \vee (b' \wedge c' \wedge a) \vee (b \wedge c \wedge a) \\
&= (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) \\
&= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c) \\
&= (a+b)+c
\end{aligned}
$$

Esistenza dello 0. Lo 0 dell'algebra di boole è anche 0 per l'anello. Infatti:

$$
a+0 = (a \wedge 0') \vee (a' \wedge 0) = (a \wedge 1) \vee (a' \wedge 0) = a \vee 0 = a
$$

Esistenza dell'opposto.

$$
a+a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0.
$$

$\cdot$ è associativa. Segue immediatamente dall'associatività di $\wedge$.
Proprietà distributiva.

$$
\begin{aligned}
a(b+c) &= a \wedge ((b \wedge c') \vee (b' \wedge c)) \\
&= (a \wedge (b \wedge c')) \vee (a \wedge (b' \wedge c)) \\
&= (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)
\end{aligned}
$$

d'altra parte

$$
\begin{aligned}
ab+ac &= (a \wedge b) + (a \wedge c) \\
&= ((a \wedge b) \wedge (a \wedge c)') \vee ((a \wedge b)' \wedge (a \wedge c)) \\
&= ((a \wedge b) \wedge (a' \vee c')) \vee ((a' \vee b') \wedge (a \wedge c)) \\
&= ((a \wedge b) \wedge a') \vee ((a \wedge b) \wedge c') \vee ((a' \vee b') \wedge a) \vee ((a' \vee b') \wedge c) \\
&= (a \wedge b \wedge a') \vee (a \wedge b \wedge c') \vee (a' \vee b' \wedge a) \vee (a' \vee b' \wedge c) \\
&= 0 \vee (a \wedge b \wedge c') \vee 0 \vee (a' \vee b' \wedge c) \\
&= (a \wedge b \wedge c') \vee (a' \vee b' \wedge c)
\end{aligned}
$$

e quindi $a(b+c) = ab + ac$.

Esistenza dell'identità. L'1 dell'algebra è 1 anche per l'anello, dato che $1a = 1 \wedge a = a$ per ogni $a \in L$.

Ogni elemento è idempotente. Infatti

$$a^2 = aa = a \wedge a = a$$

per ogni $a \in L$. ❑

Il teorema appena dimostrato dà un modo di definire una struttura di anello booleano a partire da quella di algebra di Boole, mentre il teorema 25.10 permetteva di fare il percorso inverso, ossia di ottenere una struttura di algebra di Boole a partire da quella di anello booleano. Effettivamente queste due costruzioni sono una l'inversa dell'altra, ossia

Teorema 26.3 *Dato un anello booleano costruiamo l'algebra di boole come nel teorema 25.10 e da questa costruiamo l'anello booleano come nel teorema precedente, ritroviamo esattamente l'anello da cui si è partiti e vicersa, data un'algebra di Boole fattone l'anello booleano e quindi l'algebra di boole, si riottiene l'algebra di Boole di partenza.*

Dim. Sia R un anello booleano, allora la struttura di algebra di Boole è definita da

$$\begin{aligned} a \vee b &= a + b + ab \\ ab &= a \wedge b \\ a' &= 1 + a \end{aligned}$$

A partire da questi si definiscono i due nuovi operatori di somma e prodotto ponendo:

$$\begin{aligned} a \oplus b &= (a \wedge b') \vee (a' \wedge b) \\ a \odot b &= a \wedge b \end{aligned}$$

Evidentemente $\odot = \cdot$. Ma, ricordando che un anello booleano è commutativo e ha caratteristica 2 (proposizione 22.4) si ha anche

$$\begin{aligned} a \oplus b &= (a \wedge b') \vee (a' \wedge b) \\ &= (a \wedge (1+b)) \vee ((1+a) \wedge b) \\ &= (a(1+b)) \vee ((1+a)b) \\ &= (a + ab) \vee (b + ab) \\ &= (a+ab) + (b+ab) + (a+ab)(b+ab) \\ &= a + b + ab + ab + ab + a^2b + ab^2 + a^2b^2 \\ &= a + b + ab + ab + ab + ab + ab + ab = a + b \end{aligned}$$

e quindi anche $\oplus = +$.

Viceversa, sia L un'algebra di Boole. La struttura di anello è definita da:

$$\begin{aligned} a+b &= (a \wedge b') \vee (a' \wedge b) \\ ab &= a \wedge b \end{aligned}$$

a partire dalla quale viene definita una struttura di algebra di boole ponendo

$$\begin{aligned} a \triangledown b &= a+b+ab \\ a \vartriangle b &= ab \end{aligned}$$

Chiaramente $\vartriangle = \wedge$. D'altra parte

$$\begin{aligned} a \triangledown b &= a+b+ab \\ &= ((a \wedge b') \vee (a' \wedge b)) + (a \wedge b) \\ &= (((a \wedge b') \vee (a' \wedge b)) \wedge (a \wedge b)') \vee (((a \wedge b') \vee (a' \wedge b))' \wedge (a \wedge b)) \\ &= (((a \wedge b') \vee (a' \wedge b)) \wedge (a' \vee b')) \vee (((a \wedge b')' \wedge (a' \wedge b)') \wedge (a \wedge b)) \\ &= (((a \wedge b') \vee (a' \wedge b)) \wedge (a' \vee b')) \vee (((a' \vee b) \wedge (a \vee b')) \wedge (a \wedge b)) \\ &= (((a \wedge b') \vee (a' \wedge b)) \wedge (a' \vee b')) \vee (((a' \wedge b') \vee (a \wedge b)) \wedge (a \wedge b)) \\ &= ((a \wedge b') \wedge (a' \vee b')) \vee ((a' \wedge b) \wedge (a' \vee b')) \vee \\ &\quad ((a' \wedge b') \wedge (a \wedge b)) \vee ((a \wedge b) \wedge (a \wedge b)) \\ &= (a \wedge b' \wedge a') \vee (a \wedge b' \wedge b') \vee (a' \wedge b \wedge a') \vee (a' \wedge b \wedge b') \vee \\ &\quad (a' \wedge b' \wedge a \wedge b) \vee (a \wedge b) \\ &= 0 \vee (a \wedge b') \vee (a' \wedge b) \vee 0 \vee 0 \vee (a \wedge b) \\ &= (a \wedge b') \vee (a' \wedge b) \vee (a \wedge b) \\ &= (a \wedge b') \vee (a' \wedge b) \vee (a \wedge b) \vee (a \wedge b) \\ &= (a \wedge (b \vee b')) \vee ((a \vee a') \wedge b) \\ &= (a \wedge 1) \vee (1 \wedge b) = a \vee b \end{aligned}$$

e quindi anche $\triangledown = \vee$. ❑

Osservazione 26.4 Se X è un insieme allora le due strutture su $\mathcal{P}(X)$ di algebra di Boole (esempio 25.9) e di anello booleano (esempio 22.3) definite rispettivamente dalle operazioni $\cup$, $\cap$, $\complement$ e $\vartriangle$, $\cap$ sono in corrispondenza come dal teorema precedente. Questo segue evidentemente dalle formule:

$$\begin{aligned} A \vartriangle B &= (A \cap \complement B) \cup (\complement A \cap B) \\ A \cup B &= A \vartriangle B \vartriangle (A \cap B) \\ \complement A &= X \vartriangle A \end{aligned}$$

la prima delle quali è la definizione di $\vartriangle$ mentre la seconda e la terza sono di immediata verifica.

Definizione di morfismo di algebre di Boole

Definizione 26.5 *Siano B e B' algebre di Boole, diremo che un'applicazione $\varphi : B \to B'$ è un* morfismo di algebre di boole *se per ogni $a, b \in B$ si ha*

$$\begin{aligned} \varphi(a \vee b) &= \varphi(a) \vee \varphi(b) \\ \varphi(a \wedge b) &= \varphi(a) \wedge \varphi(b) \\ \varphi(a') &= (\varphi(a))'. \end{aligned}$$

Si dirà che φ è un isomorfismo *se e solo se è bigettivo.*

Esercizio 26.1 Si provi che se $\varphi : B \to B'$ è un morfismo di algebre di Boole allora $\varphi(0) = 0$ e $\varphi(1) = 1$.

Si dimostra la seguente

Proposizione 26.6 *Siano B e B' due algebre di Boole, allora $\varphi : B \to B'$ è un morfismo di algebre di boole se e solo se è un morfismo di anelli per le rispettive strutture di anello booleano.*

Osservazione 26.7 La proposizione precedente mostra che il teorema 26.3 non solo dà una corrispondenza tra struttura di algebra di Boole e struttura di anello booleano, ma che tale corrispondenza non cambia l'insieme dei morfismi, in altre parole le due teorie da una parte quella degli anelli booleani e dall'altra quella delle algebre di Boole sono due facce della stessa medaglia e si possono usare contemporaneamente e tutti i risultati di una si traducono in risultati dell'altra.

Definizione di sottoreticoli e sottoalgebre di Boole

Definizione 26.8 *Sia L un reticolo diremo che un sottoinsieme non vuoto $S \subseteq L$ è un* sottoreticolo *se e solo se*

1. $a, b \in S \Rightarrow a \vee b \in S$
2. $a, b \in S \Rightarrow a \wedge b \in S$

Se L è un'algebra di Boole, diremo che S è una sottoalgebra di Boole *se in più*

3. $a \in S \Rightarrow a' \in S$

Esercizio 26.2 Si provi che se L è un reticolo e S è un sottoreticolo di L allora S munito dell'ordinamento indotto da quello di L è un reticolo.

Osservazione 26.9 Visto l'esercizio precedente e tenendo conto che i reticoli possono essere definiti anche a partire dall'ordine, verrebbe voglia di prendere quella data nell'esercizio come definizione. In realtà in generale non è detto che S sia un sottoreticolo pur essendo un reticolo con l'ordinamento indotto. Affinché S sia un sottoreticole, è necessario anche che l'estremo inferiore (risp.

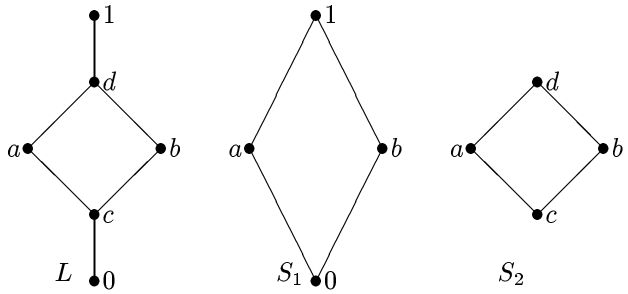


Figura 1: S_2 è un sottoreticolo di L ma non S_1

superiore) fatto in S coincida con quello fatto in L.Si consideri ad esempio il reticolo L rappresentato nel diagramma di figura 1. Allora S_1, pur essendo un reticolo con l'ordinamento indotto, non è un sottoreticolo: l'estremo inferiore tra a e b fatto in S_1 è), mentre fatto in L è c. S_2 è invece un sottoreticolo.

Proposizione 26.10 *Sia B un'algebra di Boole, allora S è una sottoalgebra se e solo se è un sottoanello per la struttura di anello booleano.*

Osservazione 26.11 La proposizione precedente mostra come anche la nozione di sottostruttura sia conservata dalla corrispondenza data dal teorema 26.3.

Esercizio 26.3 Si provi che se S è una sottoalgebra dell'algebra di Boole B, allora $0, 1 \in S$.

Teorema di rappresentazione per le algebre di Boole

Teorema 26.12 *Sia L un'algebra di Boole. Allora esiste un insieme X tale che L è isomorfa ad una sottoalgebra di $\mathcal{P}(X)$. Se L è finita allora esiste X tale che L è isomorfa a $\mathcal{P}(X)$.*

Dim. È conseguenza immediata del teorema di rappresentazione per anelli booleani (teorema 22.9) di quanto visto nelle proposizioni 26.6 e 26.10 e di quanto osservato in 26.4. Infatti per ilteorema di rappresentazione degli anelli booleani esiste un morfismo iniettivo di anelli booleani $\varepsilon : L \to \mathcal{P}(X)$ per un opportuno insieme X, che è anche surgettivo quando L è finito. Allora ε è un morfismo di algebre di Boole quando si considerino le strutture corrispondenti, e quindi la tesi. ❑

Corollario 26.13 *Se L è un'algebra di Boole finita, allora esiste n tale che $|L| = 2^n$.*

Esempio 26.14 Si consideri il reticolo L rappresentato nel diagramma di figurafig:S¡L. Ci chiediamo: è un 'algebra di Boole? Per il corollario precedente, la risposta è chiaramente no, in quanto questo reticolo ha 6 elementi e 6 non è una potenza di 2.

Lezione 27 (20 maggio 1999 h. 10.30-11.30)

Definizione di Ω-algebra

Definizione 27.1 *Sia A un insieme e $n \in \mathbb{N}$, una* operazione n-aria *su A non è altro che un'applicazione $A^n \to A$. Quindi l'insieme delle applicazioni n-arie su A altri non è che A^{A^n}.*

Osservazione 27.2 Operazioni binarie (i.e. 2-arie) se ne sono incontrate a non finire (le operazioni di un gruppo, di un anello, di un reticolo), anche di operazioni 1-arie, ossia di funzioni, ad esempio il complemento in un'algebra di Boole, l'inverso in un gruppo sono operazioni 1-arie.

Cerchiamo di capire cosa sono le operazioni 0-arie. Si pone, per definizione, $A^0 = \{\varnothing\}$, ossia l'insieme che ha come unico elemento l'insieme vuoto, allora una operazione 0-aria su A non è altro che un'applicazione $\{\varnothing\} \to A$ ossia è fissare un elemento di A. Ma allora anche di operazioni 0-arie se ne sono già incontrate tante: l'unità di un monoide è un'operazione 0-aria (si fissa un particolare elemento del monoide), lo 0 e l'1 di un anello con identità o di un'algebra di Boole sono operazioni 0-arie.

Definizione 27.3 *Sia Ω un insieme e sia $a : \Omega \to \mathbb{N}$ un'applicazione. Chiameremo (Ω, a) un* dominio di operatori *e dato $\omega \in \Omega$ diremo che $a(\omega)$ è la* arietà *di ω. Indichereamo con Ω_n l'insieme degli omega che hanno arietà pari a n, ossia $\Omega_n = \{\omega \in \Omega \mid a(\omega) = n\}$.*

Definizione 27.4 *Sia A un insieme una struttura di Ω-algebra su A è il dato per ogni $n \in \mathbb{N}$ di un'applicazione $\Omega_n \to A^{A^n}$.*

In pratica si interpreta ogni elemento di Ω_n come una operazione n-aria su A. Se $a_1, \dots, a_n \in A$ e $\omega \in \Omega_n$ si indica con $a_1 a_2 \dots a_n \omega$ il risultato dell'operazione rappresentata da ω sulla n-pla $(a_1, \dots, a_n)$. Questo tipo di notazione è conosciuta come *notazione polacca inversa* ed è comoda in quanto non necessita dell'utilizzo delle parentesi: ogni volta che si trova scritto un operatore n-ario, lo si fa agire sugli n elementi di A che lo precedono.

Esempio 27.5 I semigruppi. Sia $\Omega = \{\mu\}$ costituito da un solo elemento, $a(\mu) = 2$. Allora un semigruppo è una Ω-algebra tale che

$$a_1 a_2 \mu a_3 \mu = a_1 a_2 a_3 \mu \mu \quad \forall a_1, a_2, a_3$$

Si osservi che questa è la traduzione in notazione polacca inversa della relazione che definisce la associativa proprietà (definizione 8.1).

I monoidi. Sia $\Omega = \{\mu, 1\}$ con $a(\mu) = 2$ e $a(1) = 0$. Un monoide è una Ω-algebra in cui oltre alla proprietà associativa si ha

$$1a\mu = a1\mu = a \quad \forall a$$

L'operatore 0-ario 1 è l'identità del monoide e la formula appena scritta è la traduzione delle proprietà dell'identità (definizione 8.2).

I gruppi. Sia $\Omega = \{\mu, \theta, 1\}$ con $a(\mu) = 2$, $a(\theta) = 1$ e $a(1) = 0$. Un gruppo è una Ω-algebra in cui valgono le due precedenti e

$$aa\theta\mu = a\theta a\mu = 1 \quad \forall a.$$

Questa è la traduzione delle proprietà dell'inverso, ossia θ è interpretato come l'operazione 1-aria che ad ogni elemento associa il suo inverso.

In modo analogo si vede che tutte le strutture algebr2iche che abbiamo preso in considerazione (anelli, reticoli, algebre di boole) rientrano in questo quadro generale.

Definizione di morfismo di Ω-algebre

Definizione 27.6 *Siano A e B due Ω-algebre un'applicazione $f : A \to B$ è detta un* morfismo *se:*

$$\forall n \in \mathbb{N}, \forall \omega \in \Omega_n, \forall a_1, \ldots, a_n \in A \quad a_1 f a_2 f \ldots a_n f \omega = a_1 a_2 \ldots a_n \omega f$$

Dove si è usata la notazione polacca anche per f, ossia af significa l'immagine di a tramite f ossia quello che abbiamo sempre denotato con $f(a)$.

Ossia applicare f a ogni elemento e quindi applicare l'operazione su B rappresentata da ω è lo stesso che prima applicare l'operazione su A rappresentata da ω ad ogni elemento e quindi applicare f al risultato. Chiaramente la definizione di morfismo che abbiamo appena dato congloba tutte le definizioni di morfismo che abbiamo dato per ogni struttura.

Definizione di sotto Ω-algebra

Definizione 27.7 *Sia A una ω-algebra. Diremo che $B \subseteq A$ è una* sotto Ω-algebra *se*

$$\forall n \in \mathbb{N}, \forall \omega \in \Omega_n, \forall b_1, \ldots, b_n \in B \quad b_1 \ldots b_n \omega \in B$$

Detto in altri termini B è chiuso rispetto a tutte le operazioni di A. Anche questa definizione chiaramente ingloba tutte le definizioni di sottostruttura che abbiamo dato.

Definizione di quoziente

Definizione 27.8 *Sia A una Ω-algebra, diremo che una relazione d'equivalenza $\mathcal{R}$ su A è una* Ω-congruenza *(brevemente una congruenza) se per ogni $n \in \mathbb{N}$, per ogni $\omega \in \Omega_n$ e per ogni $a_1, \ldots, a_n$, $b_1, \ldots, b_n \in A$*

$$a_i \mathcal{R} b_i \forall i \Rightarrow a_1 \ldots a_n \omega \mathcal{R} b_1 \ldots b_n \omega.$$

Si osservi che questa che abbiamo dato come definizione è esattamente la proprietà che ci è servita nel caso dei gruppi ((16) di pag. 24) e degli anelli ((20) di pag 32) per definire una struttura di gruppo e di anello sul quoziente in modo che la proiezione a quoziente sia un morfismo. Usando esattamente la stessa dimostrazione fatta in questi due casi, si prova allora il seguente teorema:

Teorema 27.9 *Sia A una Ω-algebra e sia $\mathcal{R}$ una Ω-congruenza su A, allora esiste una unica struttura di Ω-algebra su $A/_{\mathcal{R}}$ che rende la proiezione a quoziente un morfismo.*

Tale struttura è definita ponendo per ogni $n \in \mathbb{N}$, $\omega \in \Omega_n$ e $a_1, \ldots, a_n \in A$:

$$[a_1]_{\mathcal{R}} \ldots [a_n]_{\mathcal{R}}\, \omega = [a_1 \ldots a_n \omega]_{\mathcal{R}}\,.$$

Esercizio 27.1 Descrivere in termini di Ω-algebre le strutture di anello, reticolo, algebra di Boole.

Esercizio 27.2 Siano A e B due Ω algebre e sia $\varphi : A \to B$ un morfismo. Si consideri la relazione d'equivalenza $\overset{\varphi}{\sim}$ indotta su A da f. Si provi che $\overset{\varphi}{\sim}$ è una congruenza.

Si provi inoltre che esiste un unico morfismo di Ω-algebre $\widetilde{\varphi} : A/_{\overset{\varphi}{\sim}} \to B$ tale che $\varphi = \widetilde{\varphi} \circ \pi$.

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\pi"'] & B \\
A/_{\overset{\varphi}{\sim}} \arrow[ur, "\widetilde{\varphi}"'] &
\end{tikzcd}$$

Si ha inoltre che:

1. $\widetilde{\varphi}$ è iniettiva;

2. $\widetilde{\varphi}$ è surgettiva se e solo se φ è surgettiva.

Soluzione degli esercizi proposti

Soluzione dell'esercizio 4.1 Procediamo per induzione su k. Se $k = 1$ non c'è nulla da dimostrare. Supponiamo che la tesi sia vera per k e supponiamo che $p \big| n_1 n_2 \dots n_{k+1}$, ossia $p \big| (n_1 n_2 \dots n_k) n_{k+1}$. Per il corollario 4.3, si ha che $p \big| n_1 n_2 \dots n_k$ oppure $p \big| n_{k+1}$. Se si verifica la seconda eventualità abbiamo finito, altrimenti, per ipotesi di induzione esiste $i \in \{1, \dots, k\}$ tale che $p \big| n_i$, e quindi si conclude. ❑

Soluzione dell'esercizio 7.1 Per quanto visto nell'osservazione 7.7, possiamo definire l'applicazione $\Phi : R \to P$ data da $\Phi(\mathcal{R}) = X\big/_{\mathcal{R}}$.

Data invece una partizione $\mathcal{P} \in P$ definiamo la relazione $\overset{\mathcal{P}}{\sim}$ ponendo

$$x_1 \overset{\mathcal{P}}{\sim} x_2 \iff \exists A \in \mathcal{P} : x_1, x_2 \in A.$$

Proviamo che $\overset{\mathcal{P}}{\sim}$ è una relazione d'equivalenza.

$\overset{\mathcal{P}}{\sim}$ è riflessiva (1 di definizione 7.1). Se $x \in X$ allora, dato che $\mathcal{P}$ ricopre X (1 di definizione 7.6), esiste $A \in \mathcal{P}$ tale che $x \in A$ e quindi $x \overset{\mathcal{P}}{\sim} x$.

$\overset{\mathcal{P}}{\sim}$ è simmetrica (2 di definizione 7.1). Ovvio.

$\overset{\mathcal{P}}{\sim}$ è transitiva (3 di definizione 7.1). Siano $x_1 \overset{\mathcal{P}}{\sim} x_2$ e $x_2 \overset{\mathcal{P}}{\sim} x_3$, allora esistono $A, B \in \mathcal{P}$ tali che $x_1, x_2 \in A$ e $x_2, x_3 \in B$. Ma, allora $x_2 \in A \cap B$ ossia $A \cap B \neq \varnothing$ e quindi coincidono (2 di definizione 7.6), ossia $A = B$ e quindi $x_1, x_3 \in A$ ovvero $x_1 \overset{\mathcal{P}}{\sim} x_3$.

Definiamo allora $\Psi : P \to R$ ponendo $\Psi(\mathcal{P}) = \overset{\mathcal{P}}{\sim}$, e proviamo che $\Phi \circ \Psi = \mathrm{id}$ e $\Psi \circ \Phi = \mathrm{id}$. Ciò concluderà la dimostrazione.

Sia $\mathcal{R} \in R$, allora, per la 2 della proposizione 7.3, si ha che $x_1 \mathcal{R} x_2$ se e solo se $[x_1]_{\mathcal{R}} = [x_2]_{\mathcal{R}}$ ossia se e solo se esiste $A \in X\big/_{\mathcal{R}}$ tale che $x_1, x_2 \in A$ ossia se e solo se esiste $A \in \Phi(\mathcal{R})$ tale che $x_1, x_2 \in A$ ossia se e solo se $x_1 \overset{\Phi(\mathcal{R})}{\sim} x_2$ e quindi $\mathcal{R} = \Psi(\Phi(\mathcal{R}))$.

Sia invece $\mathcal{P} \in P$, allora, dato $A \in P$ sia $x \in A$, è chiaro che $[x]_{\overset{\mathcal{P}}{\sim}} = A$, ciò unito al fatto che $\mathcal{P}$ ricopre X (1 di definizione 7.6) permette di concludere che $X\big/_{\overset{\mathcal{P}}{\sim}} = \mathcal{P}$ ovvero che $\Phi(\Psi(\mathcal{P})) = \mathcal{P}$. ❑

Soluzione dell'esercizio 7.2 $\overset{f}{\sim}$ è riflessiva (1 di definizione 7.1). Se $x \in X$ allora, $f(x) = f(x)$ e quindi $x \overset{f}{\sim} x$.

$\overset{f}{\sim}$ è simmetrica (2 di definizione 7.1). Ovvio.

$\overset{f}{\sim}$ è transitiva (3 di definizione 7.1). Siano $x_1 \overset{f}{\sim} x_2$ e $x_2 \overset{f}{\sim} x_3$, allora $f(x_1) = f(x_2)$ e $f(x_2) = f(x_3)$ da cui segue immediatamente che $f(x_1) = f(x_3)$ e quuindi $x_1 \overset{f}{\sim} x_3$. ❑

Soluzione dell'esercizio 8.1 (1). Siano $f, g, h \in Y^X$ e sia $x \in X$, allora, usando l'associatività di $*$ si ha:

$$\begin{aligned}(f \bullet (g \bullet h))(x) &= f(x) * (g \bullet h)(x) = f(x) * (g(x) * h(x)) = \\ &= (f(x) * g(x)) * h(x) = (f \bullet g(x)) * h(x) = ((f \bullet g) \bullet h)(x)\end{aligned}$$

e quindi, per l'arbitrarietà di $x \in X$, $f \bullet (g \bullet h) = (f \bullet g) \bullet h$.

(2). Sia $1 \in Y^X$ la funzione $1(x) = 1_Y$ per ogni $x \in X$, essendo 1_Y l'unità di Y.. Allora per ogni $f \in Y^X$ e per ogni $x \in X$ si ha:

$$\begin{aligned}(f \bullet 1)(x) &= f(x) * 1(x) = f(x) * 1_Y = f(x) \\ (1 \bullet f)(x) &= 1(x) * f(x) = 1_Y * f(x) = f(x)\end{aligned}$$

e quindi $f \bullet 1 = 1 \bullet f = f$.

(3). Dato ch eogni elemento di Y ha un inverso, data $f \in Y^X$ possiamo definire la funzione f^{-1} pomnendo $f^{-1}(x) = (f(x))^{-1}$ per ogni $x \in X$. Allora per ogni $x \in X$ si ha

$$\begin{aligned}(f \bullet f^{-1})(x) = f(x) * f^{-1}(x) = f(x) * (f(x))^{-1} = 1_y = 1(x) \\ (f^{-1} \bullet f)(x) = f^{-1}(x) * f(x) = (f(x))^{-1} * f(x) = 1_y = 1(x)\end{aligned}$$

e quindi $f \bullet f^{-1} = f^{-1} \bullet f = 1$.

(4). Siano $f, g \in Y^X$, per la commutatività di $*$ si ha che per ogni $x \in X$

$$f \bullet g(x) = f(x) * g(x) = g(x) * f(x) = g \bullet f(x)$$

e quindi $f \bullet g = g \bullet f$. ❑

Soluzione dell'esercizio 8.2 Dal fatto che $gg^{-1} = 1 = g^{-1}g$ ne segue che g è un inverso destro e sinistro di g^{-1} e quindi per l'unicità dell'inverso (proposizione 8.6) $g = (g^{-1})^{-1}$. ❑

Soluzione dell'esercizio 8.3 Si ha:

$$(g_1g_2)(g_2^{-1}g_1^{-1}) = g_1(g_2g_2^{-1})g_1^{-1} = g_1 1 g_1^{-1} = g_1g_1^{-1} = 1$$

ed analogamente si prova che anche $(g_2^{-1}g_1^{-1})(g_1g_2) = 1$.

Se il gruppo è commutativo, allora $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = g_1^{-1}g_2^{-1}$. Viceversa, supponiamo che $(g_1g_2)^{-1} = g_1^{-1}g_2^{-1}$ per ogni $g_1, g_2 \in G$. Allora

$$g_2g_1 = (g_2^{-1})^{-1}(g_1^{-1})^{-1} = (g_1^{-1}g_2^{-1})^{-1} = ((g_1g_2)^{-1})^{-1} = g_1g_2$$

dove la prima e l'ultima uguaglianza sono ottenuta usando il risultato dell'esercizio precedente, la seconda uguaglianza è data dal primo fatto dimostrato in questo esercizio, e la terza dall'ipotesi. ❑

Soluzione dell'esercizio 8.4 G è chiuso per l'operazione, infatti se $g_1, g_2 \in G$ siano $g_1^{-1}, g_2^{-1} \in M$ gli inversi, allora

$$g_1g_2(g_2^{-1}g_1^{-1}) = g_1(g_2g_2^{-1})g_1^{-1} = g_1 1 g_1^{-1} = g_1g_1^{-1} = 1$$

ed in modo analogo anche $(g_2^{-1}g_1^{-1})g_1g_2 = 1$, e quindi $g_1g_2 \in G$.

Chiaramente 1 è invertibile e se g è invertibile anche g^{-1} lo è. ❏

Soluzione dell'esercizio 8.5 Verifichiamo che per ogni n si ha che $n\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$. $0 \in n\mathbb{Z}$ dato che $n|0$. Inoltre se $n|a$ e $n|b$ allora $n|a-b$ e quindi si conclude per il criterio del sottogruppo.

Proviamo ora che tutti i sottogruppi di $\mathbb{Z}$ sono di questo tipo. Sia G un sottogruppo di $\mathbb{Z}$. Se $G = \{0\}$ allora $G = 0\mathbb{Z}$. Supponiamo che $G \neq \{0\}$, allora l'insieme $S = \{k \in G \mid k > 0\}$ è non vuoto, in quanto se $x \neq 0$ è un elemento di G allora uno tra x e $-x$ sta in S. Sia $n = \min S$ che esiste per l'assioma di buon ordinamento (1.1). Proviamo che allora $G = n\mathbb{Z}$. Dato che $n \in G$ allora anche $hn \in G$ per ogni $h \in \mathbb{Z}$ e quindi $n\mathbb{Z} \subseteq G$. Viceversa sia $g \in G$, allora esistono (teorema 2.1) $q, r \in \mathbb{Z}$ tali che $g = nq + r$ con $0 \leq r < n$. Ora, $r = g - nq \in G$ e quindi se fosse positivo contraddirebbe la minimalità di n, quindi $r = 0$, ossia $g = nq$, che vuol dire $g \in n\mathbb{Z}$. ❏

Soluzione dell'esercizio 8.6 Dimostriamo la prima. Se $n = 0$ è ovvia. Se $n > O$ è immediato dalla definizione delle potenze con esponente negativo. Se invece $n < 0$ allora per definizione, si ha $(x^{-1})^n = ((x^{-1})^{-1})^{-n}$, e quindi per l'esercizio 8.2, $(x^{-1})^n = x^{-n}$.

Dimostriamo la seconda per $n \geq 0$. Procediamo per induzione su n. Se $n = 0$ allora

$$x^{0+m} = x^m = 1x^m = x^0x^m$$

Supponiamo che $x^{n+m} = x^nx^m$ allora

$$x^{n+1+m} = xx^{n+m} = xx^nx^m = x^{n+1}x^m$$

Se ora $n < 0$ allora $-n > 0$ e quindi, usando la definizione, la prima formula e quanto abbiamo appena provato

$$x^{n+m} = (x^{-1})^{-(n+m)} = (x^{-1})^{-n-m} = (x^{-1})^{-n}(x^{-1})^{-m} = x^nx^m.$$

La terza segue osservando che usando la seconda si ha:

$$x^{-n}x^n = x^0 = 1 \text{ e } x^nx^{-n} = x^0 = 1$$

quindi x^{-n} è l'inverso di x^n.

Proviamo ora la quarta. Proviamolo per $m \geq 0$, procedendo per induzione su m. Per $m = 0$

$$(x^n)^0 = 1 = x^0 = x^{n0}.$$

Supponiamo che $(x^n)^m = x^{nm}$, allora

$$(x^n)^{m+1} = x^n(x^n)^m = x^n x^{nm} = x^{n+nm} = x^{n(m+1)}$$

Se $m < 0$ allora $-m > 0$ e quindi usando la terza, la definizione e quanto appena visto, si ha:

$$(x^n)^m = ((x^n)^{-1})^{-m} = (x^{-n})^{-m} = x^{(-n)(-m)} = x^{nm}$$

❏

Soluzione dell'esercizio 10.1 Sia $\sigma \in S_n$, e sia $\sigma = \pi_1 \ldots \pi_s$ la decomposizione in cicli disgiunti. Sia $\tau = (a\ b)$ una trasposizione. Si hanno quattro possibilità:

1. né a né b compare in alcun ciclo dei π_i
2. solo a compare in un ciclo, che possiamo supporre essere π_s
3. a e b compaiono in un solo ciclo, che possiamo supporre essere π_s
4. a e b compaiono in due cicli diversi che possiamo supporre essere π_{s-1} e π_s

Caso (1). In questo caso $\pi_1 \ldots \pi_k \tau$ è la decomposizione in cicli disgiunti di $\sigma\tau$ e quindi

$$\begin{aligned} \varepsilon(\sigma\tau) &= (-1)^{\sum_{i=1}^{s}(l(\pi_i)-1)+l(\tau)-1} = (-1)^{\sum_{i=1}^{s}(l(\pi_i)-1)+1} = \\ &= -(-1)^{\sum_{i=1}^{s}(l(\pi_i)-1)} = -\varepsilon(\sigma) = \varepsilon(\sigma)\varepsilon(\tau) \end{aligned}$$

Caso (2). Sia $\pi_s = (a\ a_1 \ldots a_k)$, allora

$$\sigma\tau = \pi_1 \ldots \pi_s \tau = \pi_1 \ldots \pi_{s-1}(a\ a_1 \ldots a_k)(a\ b) = \pi_1 \ldots \pi_{s-1}(a\ b\ a_1 \ldots a_k)$$

è la decomposizione in cicli disgiunti di $\sigma\tau$ e quindi, detto $\pi'_s = (a\ b\ a_1 \ldots a_k)$, si ha $l(\pi'_s) = l(\pi_s + 1$, da cui:

$$\begin{aligned} \varepsilon(\sigma\tau) &= (-1)^{\sum_{i=1}^{s-1}+(l(\pi_i)-1)+l(\pi'_s)-1} = (-1)^{\sum_{i=1}^{s}+(l(\pi_i)-1)+1} = \\ &= -(-1)^{\sum_{i=1}^{s}} = -\varepsilon(\sigma) = \varepsilon(\sigma)\varepsilon(\tau) \end{aligned}$$

Case (3). Sia $\pi_s = (a\ a_1 \ldots a_k\ b\ b_1 \ldots b_h)$ allora

$$\begin{aligned} \sigma\tau &= \pi_1 \ldots \pi_s \tau = \pi_1 \ldots \pi_{s-1}(a\ a_1 \ldots a_k\ b\ b_1 \ldots b_h)(a\ b) \\ &= \pi_1 \ldots \pi_{s-1}(a\ b_1 \ldots b_h)(b\ a_1 \ldots a_k) \end{aligned}$$

è la decomposizione in cicli disgiunti di $\sigma\tau$. Posto $\pi'_s = (a\ b_1 \ldots b_h)$ e $\pi''_s = (b\ a_1 \ldots a_k)$ si ha che $l(\pi'_s) + l(\pi''_s) = l(\pi_s) + 2$ e quindi

$$\begin{aligned} \varepsilon(\sigma\tau) &= (-1)^{\sum_{i=1}^{s-1}+(l(\pi_i)-1)+l(\pi'_s)-1+l(\pi''_s)-1} = (-1)^{\sum_{i=1}^{s-1}+(l(\pi_i)-1)+l(\pi_s)} = \\ &= = (-1)^{\sum_{i=1}^{s}+(l(\pi_i)-1)+1} = -\varepsilon(\sigma) = \varepsilon(\sigma)\varepsilon(\tau) \end{aligned}$$

Caso (4). Siano $\pi_{s-1} = (a\ a_1 \dots a_k)$ e $\pi_s = (b\ b_1 \dots b_h)(a\ b)$. Allora

$$\begin{aligned} \sigma\tau &= \pi_1 \dots \pi_s \tau = \pi_1 \dots \pi_{s-2}\pi_{s-1}(a_1 \dots a_k)(b_1 \dots b_h)(a\ b) = \\ &= \pi_1 \dots \pi_{s-2}(a\ b_1\ \dots b_h\ b\ a_1 \dots a_k) \end{aligned}$$

è la decomposizione in cicli disgiunti di $\sigma\tau$. Posto $\pi = (a\ b_1\ \dots b_h\ b\ a_1 \dots a_k)$ si ha che $l(\pi) = l(\pi_{s-1} + l(\pi_s) + 2$ e quindi:

$$\begin{aligned} \varepsilon(\sigma\tau) &= (-1)^{\sum_{i=1}^{s-2} + (l(\pi_i)-1) + l(\pi) - 1} = (-1)^{\sum_{i=1}^{s-2} + (l(\pi_i)-1) + l(\pi_{s-1}) + l(\pi_s) - 1} = \\ &= = (-1)^{\sum_{i=1}^{s} + (l(\pi_i)-1) + 1} = -\varepsilon(\sigma) = \varepsilon(\sigma)\varepsilon(\tau) \end{aligned}$$

Questo conclude la dimostrazione. ❏

Soluzione dell'esercizio 14.1 Sono tutte verifiche elementari. Mostriamo, a titolo di esempio, che per la somma e il prodotto di classi di resto vale la proprietà distributiva (3 di definizione 14.1)

$$[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$$

Mostriamo inoltre, con un esempio, che l'anello delle matrici non è commutativo se $n \geq 2$. Per $n = 2$ si consideri il seguente esempio:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Nel caso $n > 2$ basta prendere le matrici dell'esempio appena dato ed estenderle con tutti 0 fino a farle diventare $n \times n$. ❏

Soluzione dell'esercizio 14.2 Tutte le asserzioni seguono da quanto visto nell'esercizio 8.1, tranne la distributività. Proviamola. Siano $f, g, h \in R^X$ e sia $x \in X$, allora usando la distributività in R, si ha

$$\begin{aligned} (f(g + h))(x) &= f(x)((g + h)(x)) = f(x)(g(x) + h(x)) = \\ &= f(x)g(x) + f(x)h(x) = fg(x) + fh(x) = (fg + fh)(x). \end{aligned}$$

Dato che ciò vale per ogni $x \in X$ allora $f(g + h) = fg + fh$. ❏

Soluzione dell'esercizio 14.3 Se $[a]$ è una unità, esiste $[x]$ tale che $[a][x] = [1]$ ossia $[ax] = [1]$, che vuol dire $ax \equiv 1 \mod n$, e pertanto esiste y tale che $ax - 1 = ny$ e quindi $1 = ax - ny$ e quindi per quanto osservato in 3.11, $(a, n) = 1$.

Viceversa se $(a, n) = 1$ esistono x, y tali che $1 = ax + ny$ e quindi $ax \equiv 1 \mod n$, ovvero $[a][x] = [1]$. ❏

Soluzione dell'esercizio 14.4 Sia $[a]$ un divisore di zero. Se per assurdo $(a, n) = 1$ allora per l'esercizio precedente (14.3) $[a]$ sarebbe una unità , ma le unità non sono divisori di zero (lemma 14.10).

Viceversa supponiamo che $(a, n) \neq 1$, allora $1 \leq n/(a, n) < n$ quindi $[n/(a, n)] \neq 0$. D'altra parte $an/(n, m) = [n, m]$ è un multiplo di n e pertanto $[a]\,[n/(n, m)] = [an/(n, m)] = [0]$. ❑

Soluzione dell'esercizio 14.5 In effetti il teorema precedente è un caso particolare dell'esercizio 8.4 in quanto le unità di un anello con identità R non sono altro che gli elementi invertibili del monoide moltiplicativo $(R, \cdot)$. ❑

Soluzione dell'esercizio 14.6 Segue immediatamente dagli esercizi 14.3 e 14.4 ❑

Soluzione dell'esercizio 14.7 Il gruppo delle unità di $\mathbb{Z}$ è $\{-1, 1\}$ e l'applicazione $(\mathbb{Z}/_{2\mathbb{Z}}, +) \to (\{-1, 1\}, \cdot)$ definita da $[0] \mapsto 1$ e $[1] \mapsto -1$ è un isomorfismo di gruppi. ❑

Soluzione dell'esercizio 15.1 Se R è commutativo, allora $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$ per ogni $a, b \in R$ e quindi il quoziente è commutativo.

Se $1 \in R$ allora $(1+I)(a+I) = 1a+I = a+I$ per ogni $a \in R$ e, analogamente anche $(a + I)(1 + I) = a + I$ per ogni a, quindi $1 + I$ è l'identità del quoziente. Dato che $\pi(1) = 1 + I$ per definizione, la proiezione a quoziente è un morfismo di anelli unitari. ❑

Soluzione dell'esercizio 15.2 Per l'analogo risultato per i gruppi (proposizione 10.5) si ha che $\bigcap_{\lambda\in\Lambda} I_\lambda$ è un sottogruppo per la somma.

Se $a \in R$ e $s \in \bigcap_{\lambda\in\Lambda} I_\lambda$, allora $s \in I_\lambda$ per ogni λ, dato che I_λ è un ideale, allora $as \in I_\lambda$ e $sa \in I_\lambda$ per ogni λ, quindi $as, sa \in \bigcap_{\lambda\in\Lambda} I_\lambda$. ❑

Soluzione dell'esercizio 15.3 Mimando la definizione di sottogruppo generato (10.7) diremo che l'ideale generato da un sottoinsieme T dall'anello R è il più piccolo ideale che contiene T, ossia se (T) è l'ideale generato, allora

1. $T \subset (T)$
2. se I è un ideale che contiene T allora $I \supseteq (T)$.

Un siffatto ideale, se esiste è chiaramente unico e d'altra parte l'intersezione di tutti gli ideali che contengono T è, per l'esercizio precedente (15.2), un iideale che ha evidentemente le proprietà richieste. ❑

Soluzione dell'esercizio 15.4 Se se $a|b$ allora esiste $c \in R$ tale che $b = ac$. Se I è un ideale tale che $a \in I$ allora)d:di $b = ca \in I$ e quindi $b \in (a)$. D'altra parte, proviamo che $J = \{b \in R \mid a|b\}$ è un ideale. Infatti se $b_1, b_2 \in J$ allora esistono $c_1, c_2 \in R$ tali che $b_1 = ac_1$ e $b_2 = ac_2$ e quindi $b_1 + b_2 = ac_1 + ac_2 = a(c_1 + c_2) \in J$. Se $b \in J$ e $r \in R$ allora esiste $b = ca$ e quindi $rb = r(ca) = (rc)a \in J$. ❑

Soluzione dell'esercizio 15.5 $I + J$ è un ideale. Siano $a, a' \in I + J$ allora esistono $i, i' \in I$ e $j, j' \in J$ tali che $a = i + j$ e $a' = i' + j'$, ma allora $a + a' = (i + j) + (i' + j') = (i + i') + (j + j') \in I + J$ dato che, essendo I e J degli ideali, $i + i' \in I$ e $j + j' \in J$. Sia $a \in I + J$ ossia $a = i + j$ con $i \in I$ e $j \in J$. Sia $r \in R$, allora $ra = r(i + j) = ri + rj \in I + J$ dato che, essendo I e J degli ideali, $ri \in I$ e $rj \in J$.

Osserviamo infine che se $H \subseteq R$ è un ideale che contiene sia I che J, allora $i \in H$ per ogni $i \in I$ ei $j \in J$ per ogn $j \in H$, poiché H è un ideale, $i + j \in H$ per ogni $i \in I$ e $j \in J$, quindi $I + J \subseteq H$, da cui la tesi. ❑

Soluzione dell'esercizio 15.6 Sia $u \in I$ una unità. Allora esiste $u^{-1} \in R$ e quindi, usando la 2 della definizione di ideale (definizione15.3), $1 = uu^{-1} \in I$. Ma allora se $a \in R$, usando nuovamente la 2 della definizione di ideale $a = 1a \in I$. ❑

Soluzione dell'esercizio 15.7 In un corpo tutti gli elementi non nulli sono invertibili, quindi se I è un ideale diverso da (0) allora I contiene un elemento invertibile. Per l'esercizio precedente, $I = R$.

Viceversa sia $a \in R - \{0\}$ si consideri (a) l'ideale generato da a , dato che $a \neq 0$ anche $(a) \neq (0)$ e quindi $(a) = R$, ma allora $1 \in (a)$ e per l'esercizio 15.4 esiste $b \in R$ tale che $1 = ab$ e quindi a è invertibile., ❑

Soluzione dell'esercizio 17.1 Dato che id_t è un morfismo, si ha

$$\begin{aligned} f_{P+Q}(t) &= \mathrm{id}_t(P+Q) = \mathrm{id}_t(P) + \mathrm{id}_t(Q) = f_P(t) + f_Q(t) \\ f_{PQ}(t) &= \mathrm{id}_t(PQ) = \mathrm{id}_t(P)\mathrm{id}_t(Q) = f_P(t) f_Q(t) \end{aligned}$$

dato che valgono per ogni $t \in R$ e per come sono definite le operazioni nell'insieme delle funzioni, queste relazioni voglion dire che $f_{P+Q} = f_P + f_Q$ e $f_{PQ} = f_P f_Q$. ❑

Soluzione dell'esercizio 18.1 Sia $f : P \mapsto f_P$ l'applicazione in questione, allora $f_P = 0$ se e solo se $P(t) = 0$ per ogni $t \in K$. Se K è infinito, per il principio di identità dei polinomi (corollario 18.3), questo implica che $P = 0$.

D'altra parte se il campo è finito, allora $K = \{\alpha_1, \ldots, \alpha_n\}$. Consideriamo allora il polinomio, $P = \prod_i (x - \alpha_i)$. Chiaramente per ogni j si ha $P(\alpha_j) = \prod_i (\alpha_j - \alpha_i) = 0$ e quindi $f_P = 0$, ovvero $P \in \ker f$, da cui segue allora che $(P) \subseteq \ker f$.

D'altra parte se $Q \in \ker f$ allora $Q(\alpha_1) = 0$ e quindi, per il teorema di Ruffini (17.5), $Q = (x - \alpha_1)Q_1$. $Q(\alpha_2) = 0$ e quindi $(\alpha_2 - \alpha_1)Q_1(\alpha_2) = 0$ e quindi $Q_1(\alpha_2) = 0$. Per il teorema di Ruffini allora $Q_1 = (x - \alpha_2)Q_2$ e quindi $Q = (x - \alpha_1)(x - \alpha_2)Q_2$. Procedendo per induzione, si prova allora che $Q = \prod_(x - \alpha_i)Q_n = PQ_n$ ossia che $Q \in (P)$, ovvero $\ker f \subseteq (P)$. Mettendo insieme le due inclusioni si ha allora che $\ker f = (P)$. ❑

Soluzione dell'esercizio 18.2 Osserviamo che mostrare la tesi equivale a mostrare che

$$\forall k \qquad (x-\beta)^k \big| Q \iff (x-\beta)^k \big| P.$$

Chiaramente se $(x-\beta)^k \big| Q$ allora $(x-\beta)^k \big| P$. Proviamo ora che $(x-\beta)^k \big| P$ allora $(x-\beta)^k \big| Q$. Procediamo per induzione su k. Sia $k = 1$, allora $(x-\beta)\big| P$ implica che $P(\beta) = 0$ ossia $(\beta-\alpha)^s Q(\beta) = 0$, da cui $Q(\beta) = 0$ e quindi, per il teorema di Ruffini (teorema17.5), $(x-\beta)\big| Q$. Supponiamo la tesi vera per k e supponiamo che $(x-\beta)^{k+1}\big| P$. In particolare $(x-\beta)^k\big| P$, quindi, per ipotesi di induzione si ha che $(x-\beta)^k\big| Q$, ossia $Q = (x - beta)^k R$ e quindi $P = (x-\alpha)^s (x - beta)^k R$. D'altra parte, $P = (x-\beta)^{k+1} S$ e quindi

$$\begin{aligned}(x-\beta)^{k+1} S = (x-\alpha)^s (x-\beta)^k R &\iff (x-\beta)^k ((x-\beta)S - (x-\alpha)^s R) = 0 \\ &\iff (x-\beta)S - (x-\alpha)^s R = 0\end{aligned}$$

e l'ultima uguaglianza valutata in β garantisce che $(\beta-\alpha)^s R(\beta) = 0$ e quindi $R(\beta) = 0$. Per il teorema di Ruffini, $R = (x-\beta)T$ e quindi $Q = (x - beta)^k R = (x-\beta)^{k+1} T$, e quindi la tesi. ❑

Soluzione dell'esercizio 18.3 Sia $n = \operatorname{char} K$ e supponiamo che n non sia primo, esistono quindi $h, k \in \mathbb{N}$ tali che $1 < h, k < n$ e $n = hk$. Ma allora $n1 = (hk)1 = (h1)(k)1$ e, dato che $n = \operatorname{char} K$, $h1 \neq 0$ e $k1 \neq 0$, questo contraddice il fatto che K, essendo un campo, è un dominio di integrità (osservazione14.11). ❑

Soluzione dell'esercizio 18.4 Per la proprietà distributiva si ha $pk = k(p1) = k0 = 0$. ❑

Soluzione dell'esercizio 22.1 Sia $f \in R^X$, allora per ogni $x \in X$ si ha $f^2(x) = (f(x))^2 = f(x)$ e quindi $f^2 = f$. ❑

Soluzione dell'esercizio 22.2 Si consideri l'applicazione $\mathcal{P}(X) \to \mathbb{Z}/_{2\mathbb{Z}})^X$ definita da $A \mapsto \chi_A$ essendo χ_A la funzione indicatrice di A, ossia

$$\chi_A(x) = \left\langle \begin{array}{ll} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{array} \right.$$

e si provi che è un isomorfismo. ❑

Soluzione dell'esercizio 22.3 Se $R \in R$ allora $r(r-1) = 0$, quindi se $r \neq 0$ e $r \neq 1$ si ha che r è un divisore di zero e quindi non è invertibile (lemma 14.10), e quindi la tesi. ❑

Soluzione dell'esercizio 22.4 Basta fare tutte le verifiche. Diamo però un'altra dimostrazione. Osserviamo che

$$\begin{aligned} a \oplus b &= a+b+1 = (a+1)+(b+1)-1 \\ a \odot b &= a+b+ab = a+b+ab+1-1 = (a+1)(b+1)-1. \end{aligned}$$

Quindi detta $\varphi : R \to R$ l'applicazione biunivoca definita da $\varphi(a) = a+1$, si ha che

$$\begin{aligned} a \oplus b &= \varphi^{-1}(\varphi(a)\varphi(b)) \\ a \odot b &= \varphi^{-1}(\varphi(a)+\varphi(b)) \end{aligned}$$

e quindi tutte le proprietà che sono verificate da $+$ e $\cdot$ sono verificate anche da $\oplus$ e $\odot$. Si osservi inoltre che l'applicazione $\varphi : (R, \oplus, \odot) \to (R, +, \cdot)$ è un isomorfismo. ❑

Soluzione dell'esercizio 23.3 Dalle definizioni di massimo comun divisore (3.5) e di minimo comune multiplo (4.4) segue immediatamente che (a, b) e $[a, b]$ sono rispettivamentel'estremo inferiore e l'estremo superiore di $\{a, b\}$. I relativi teoremi di esistenza (3.8 e 4.5) permettono di concludere. ❑

Soluzione dell'esercizio 23.4 (1). Se a e a' sono minimi, allora $a \leq a'$, dato che a è minimo, ma anche $a' \leq a$ dato che a' è minimo. Ma allora per la antisimmetria si ha che $a = a'$.

(2). Analoga alla precedente.

(3). Segue da (2), dato che l'estremo inferiore è il massimo dei minoranti.

(4). Segue da (1).

(5). Se è minimo è ovviamente minimale. In generale non è vero il vicevers. Si consideri $X = \mathbb{N} - \{1\}$ con l'ordinamento parziale indotto da $\big|$, allora ogni primo è minimale, infatti se p è primo e $n \big| p$ allora $n = 1$ o $n = p$, dato che $1 \notin X$ si ha che $n = p$.

(6). L'esempio si ottiene prendendo lo stesso X del punto precedente con l'ordinamento inverso.

(7). Sia $a = \min Y$, e sia x un minorante di Y allora $x \leq a$, dato che $a \in Y$. D'altra parte a è un minorante di Y, quindi è il massimo dei minoranti di Y, ossia $a = \inf Y$. In generale il viceversa non è vero. Si pensi all'esempio dell'esercizio precedente, $\mathbb{N}$ ordinato parzialmente da $\big|$, allora $\inf\{4, 6\} = 2$ ma $\{4, 6\}$ non ha minimo.

(8). Analogo al caso precedente. Come esempio si prenda $\mathbb{N}$ ordinato parzialmente da $\big|$, allora $\sup\{4, 6\} = 12$ ma $\{4, 6\}$ non ha massimo. ❑

Soluzione dell'esercizio 24.1 Se $x \leq y$ evidentemente x verifica le proprietà caratterizzanti dell'estremo inferiore (definizione 24.2):

$$x \leq x, \quad x \leq y$$
$$z \leq x \text{ e } z \leq y \Rightarrow z \leq x.$$

Viceversa se $x = x \wedge y$, dal fatto che $x \wedge y \leq y$ segue allora che $x \leq y$.

La seconda equivalenza segue dal principio di dualità dei reticoli, infatti, la prima equivalenza, applicata al reticolo duale di $(L, \geq)$ dice che

$$x \geq y \iff x = x \vee y$$

e quindi, scambiando x con y si ha $x \leq y \iff y = y \vee x = x \vee y$. ❑

Soluzione dell'esercizio 25.1 Supponiamo che $x \vee y = y$, allora $x \wedge (x \vee y) = x \wedge y$, ma per la proprietà di assorbimento si ha che $x \wedge (x \vee y) = x$ e quindi $x = x \wedge y$.

Viceversa, supponiamo che $x = x \wedge y$, allora, usando le proprietà commutativa e di assorbimento, $x \wedge y = (x \vee y) \wedge y = y \wedge (y \vee x) = y$. ❑

Soluzione dell'esercizio 25.2 Dimostiamo che (1) $\Rightarrow$ (2). Infatti

$$\begin{array}{rcll}
(x \wedge y) \vee (x \wedge z) & = & ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee z) & \text{(ipotesi 1)} \\
& = & (x \vee (x \wedge y)) \wedge (z \vee (x \wedge y)) & \text{(commutativa)} \\
& = & x \wedge (z \vee (x \wedge y)) & \text{(assorbimento)} \\
& = & x \wedge ((z \vee x) \wedge (z \vee y)) & \text{(ipotesi 1)} \\
& = & x \wedge ((x \vee z) \wedge (y \vee z)) & \text{(commutativa)} \\
& = & (x \wedge (x \vee z)) \wedge (y \vee z) & \text{(associativa)} \\
& = & x \wedge (y \vee z) & \text{(assorbimento)}
\end{array}$$

Osserviamo ora che la proposizione (2) $\Rightarrow$ (1) è duale di (1) $\Rightarrow$ (2). Visto che si è provato che in ogni reticolo (1) $\Rightarrow$ (2), allora, per il principio di dualità (teorema 24.6), in ogni reticolo vale anche (2) $\Rightarrow$ (1). ❑

Soluzione dell'esercizio 27.2 Si mimi la dimostrazione dei teoremi di omomorfismo per gruppi (teorema 13.10) e per anelli (teorema 15.10). ❑