

parte stabile generata da un insieme

ESERCIZIO 1 *L'intersezione di una famiglia di parti stabili, se non é vuota, é ancora una parte stabile.*

DEFINIZIONE 2 Sia X un insieme di elementi di una struttura algebrica. L'intersezione di tutte le parti stabili contenenti X prende il nome di *parte stabile generata da X* e si denota con $st(X)$.

ESERCIZIO 3 *Sia X un insieme di elementi di una struttura algebrica di sostegno S . Provare che un sottoinsieme Y di S é la parte stabile generata da X se, e solo se, valgono le seguenti due proprietá:*

- Y é una parte stabile contenente X ;
- Y é contenuto in ogni parte stabile che contenga X .

Ne segue che $st(X)$ é la minima parte stabile, rispetto all'inclusione, di S contenente X .

DEFINIZIONE 4 Sia X un insieme non vuoto di elementi di una struttura algebrica S . Se la parte stabile generata da X coincide con S , si dice che X é un *generatore* di S , o anche che X *genera* S .

ESEMPIO 5 Siano a, b due interi distinti e non nulli. In $(\mathbb{Z}, +)$ risulta:

- $st(a) = \{na : n \in \mathbb{Z}^+\}$
- $st(a, b) = \{na + mb : n, m \in \mathbb{Z}\}$.

ESEMPIO 6 Siano X, Y sottoinsiemi non vuoti e distinti di S . In $(P(S), \cap)$ risulta:

- $st(X, Y) = \{X, Y, X \cap Y\}$.

DEFINIZIONE 7 Una struttura algebrica (S, \circ) , con operazione interna, si chiama *semigruppero* se l'operazione \circ é associativa. Se \circ é anche commutativa, il semigruppero si dice *commutativo* o *abeliano*.

ESEMPI 8 Le strutture che seguono esempi di semigrupperi.

- $(N_0, +), (Z, +), (Q, +), (R, +), (C, +), (Z_n, +)$.
- $(N_0, \cdot), (Z, \cdot), (Q, \cdot), (R, \cdot), (C, \cdot), (Z_n, \cdot), (U(n), \cdot)$.
- $(Z[x], +), (Q[x], +), (R[x], +), (C[x], +)$.
- $(Z[x], \cdot), (Q[x], \cdot), (R[x], \cdot), (C[x], \cdot)$.
- $(P(S), \cap), (P(S), \cup)$.

PROPOSIZIONE 9 Sia (S, \circ) un semigruppero e X un insieme non vuoto di elementi di S . Allora risulta

$$st(X) = \{x_1 \circ x_2 \circ \dots \circ x_n : x_1, x_2, \dots, x_n \in X \text{ e } n \in N\}.$$

PROPOSIZIONE 10 In un semigruppero (S, \circ) con elemento neutro valgono le seguenti proprietá:

- a simmetrizzabile $\Rightarrow a$ ha un unico simmetrico;
- a simmetrizzabile e tale che $a \circ b = b \circ a \Rightarrow a' \circ b = b \circ a'$.

ESERCIZIO 11 Siano a, b elementi simmetrizzabili di un semigruppero unitario (S, \circ) . Provare che $a \circ b$ é simmetrizzabile e

$$(a \circ b)' = b' \circ a'. \tag{1}$$

Provare inoltre che $(a \circ b)' = a' \circ b'$ se, e solo se, risulta $a \circ b = b \circ a$.

ESERCIZIO 12 Sull'insieme $S = R^3$ si consideri l'operazione " \circ " definita da

$$(a, b, c) \circ (a', b', c') = (aa', (a + b + c)b' + ba', (a + b + c)c' + ca').$$

Provare che (S, \circ) é un semigruppero unitario e che un elemento (a, b, c) é invertibile se, e solo se, a e $a + b + c$ sono entrambi diversi da zero.

elementi regolari

DEFINIZIONE 13 Sia (S, \circ) una struttura algebrica con operazione interna. Un elemento a si dice *cancellabile a sinistra* (*a destra*) se:

$$a \circ b = a \circ c \Rightarrow b = c \quad (b \circ a = c \circ a \Rightarrow b = c).$$

L'elemento a si dice *cancellabile* o *regolare* se é cancellabile a sinistra e a destra. Se tutti gli elementi di S sono regolari, si dice che (S, \circ) é *regolare* o anche che in (S, \circ) vale la *legge di cancellazione*.

PROPOSIZIONE 14 Sia (S, \circ) un semigrupp unitario. Allora ogni suo elemento simmetrizzabile é regolare.

DIM. Siano u l'unitá del semigrupp, a un elemento simmetrizzabile e a' il suo simmetrico. Se, per due elementi $b, c \in S$, risulta

$$a \circ b = a \circ c,$$

abbiamo

$$a' \circ (a \circ b) = a' \circ (a \circ c) \Rightarrow (a' \circ a) \circ b = (a' \circ a) \circ c \Rightarrow u \circ b = u \circ c \Rightarrow b = c.$$

Abbiamo cosí che a é cancellabile a sinistra. Allo stesso modo si vede che a é cancellabile a destra e l'asserto é provato.

ESERCIZIO 15 Provare che un elemento $a \in Z_n^*$ che non sia invertibile non é cancellabile.

elementi permutabili

DEFINIZIONE 16 Sia (S, \circ) una struttura algebrica con operazione interna. Due elementi a, b di S si dicono *permutabili* se

$$a \circ b = b \circ a.$$

Un elemento permutabile con tutti gli elementi di S si dice *centrale*. L'insieme di tutti gli elementi centrali si chiama *centro* di (S, \circ) e si denota con $Z(S)$.

OSSERVAZIONI 17 Valgono le seguenti proprietà:

- Ogni elemento é permutabile con se stesso.
- $S = Z(S)$ se, e solo se, l'operazione \circ é commutativa.
- Se (S, \circ) é un semigruppó si ha:
 - (1) a, b permutabili con $c \Rightarrow a \circ b$ permutabile con c ;
 - (2) Se $Z(S)$ é non vuoto, allora: $a, b \in Z(S) \Rightarrow a \circ b \in Z(S)$.

isomorfismi

ESEMPIO 18 Consideriamo le operazioni $\cdot, +, *$ rispettivamente su

$$S_1 = \{1, r_1, r_2, r_3\}, \quad S_2 = \{0, 1, 2, 3\}, \quad S_3 = \{e, a, b, c\},$$

definite dalle seguenti tabelle di Cayley:

\cdot	1	r_1	r_2	r_3
1	1	r_1	r_2	r_3
r_1	r_1	r_2	r_3	1
r_2	r_2	r_3	1	r_1
r_3	r_3	1	r_1	r_2

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

E' evidente che, a meno dei nomi dati alle tre operazioni e agli elementi dei tre insiemi, le strutture considerate sono la stessa struttura; esse sono cioé *algebricamente equivalenti* o, come usualmente si dice, *isomorfe*. Per esempio possiamo identificare la seconda e la terza ponendo:

$$+ = *, \quad 0 = e, \quad 1 = a, \quad 2 = b, \quad 3 = c.$$

Nasce, cosí , l'esigenza di definire rigorosamente le situazioni che permettono di ritenere algebricamente equivalenti due strutture algebriche. Ciò si può fare introducendo il concetto di *isomorfismo*.

isomorfismi

DEFINIZIONE 19 Siano (S, \circ_1) e (S', \circ_2) strutture algebriche con operazioni interne. Una applicazione biunivoca $f: S \rightarrow S'$ si dice *isomorfismo* se

$$f(a \circ_1 b) = f(a) \circ_2 f(b), \quad \text{per ogni } a, b \in S.$$

DEFINIZIONE 20 Siano (S, \circ_1) e (S', \circ_2) strutture algebriche con operazioni esterne aventi lo stesso dominio di operatori A . Un'applicazione biunivoca $f: S \rightarrow S'$ si dice *isomorfismo* se

$$f(\alpha \circ_1 a) = \alpha \circ_2 f(a), \quad \text{per ogni } \alpha \in A \text{ e } a \in S.$$

DEFINIZIONE 21 Un *isomorfismo* fra due strutture algebriche ad n operazioni

$$(S, \star_1, \star_2, \dots, \star_n) \quad \text{e} \quad (S', \circ_1, \circ_2, \dots, \circ_n)$$

é un'applicazione biunivoca $f: S \rightarrow S'$ per cui esiste una permutazione σ degli indici $1, 2, \dots, n$, tale che f é un isomorfismo fra (S, \star_j) e $(S', \circ_{\sigma(j)})$, per ogni $j = 1, 2, \dots, n$.

alcune proprietà

- L'identità é un isomorfismo di ogni struttura algebrica in se stessa.
- f isomorfismo $\Rightarrow f^{-1}$ isomorfismo (*l'inverso di f*).
- $S_1 \xrightarrow{f} S_2 \xrightarrow{g} S_3$, f, g isomorfismi $\Rightarrow S_1 \xrightarrow{fg} S_3$ isomorfismo.
- La relazione di isomorfismo fra strutture algebriche é di equivalenza.

OSSERVAZIONE 22 Dal punto di vista algebrico due strutture isomorfe possono considerarsi equivalenti. Questo fatto si esprime dicendo che *le strutture algebriche si studiano a meno di isomorfismi*.

esempi di isomorfismi

ESEMPIO 23 Si considerino le strutture algebriche (R^+, \cdot) , ove R^+ denota l'insieme dei numeri reali positivi, e $(R, +)$. E' noto che la funzione logaritmo

$$\log : a \in R^+ \rightarrow \log a \in R$$

é biunivoca. Essa é un isomorfismo di (R^+, \cdot) in $(R, +)$ perché risulta

$$\log(ab) = \log(a) + \log(b), \text{ per ogni } a, b \in R^+.$$

L'isomorfismo inverso della funzione logaritmo é la funzione esponenziale.

ESEMPIO 24 Sia $S = \{1, 2, 3, \dots, n\}$ e, per ogni sottoinsieme A di S , si definisca la *funzione caratteristica* f_A di A nel seguente modo:

$$f_A(j) = \begin{cases} 1 & \text{se } j \in A \\ 0 & \text{se } j \notin A \end{cases},$$

per ogni $j \in S$. Denotato con V_n l'insieme delle n -ple ordinate degli elementi di $Z_2 = \{0, 1\}$, si puó definire in V_n un'operazione di addizione nel seguente modo:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n),$$

ove $a_i + b_i$ é l'addizione modulo 2. Allora le strutture algebriche $(P(S), \star)$, ove \star é l'operazione di differenza simmetrica, e $(V_n, +)$ sono isomorfe; un isomorfismo essendo dato dalla funzione $f : P(S) \rightarrow V_n$ definita da

$$f(A) = (f_A(1), f_A(2), \dots, f_A(n)),$$

per ogni sottoinsieme A di S .

morfismi

DEFINIZIONE 25 Siano (S_1, \circ) e $(S_2, *)$ due strutture algebriche con operazioni interne. Un'applicazione $f: S_1 \rightarrow S_2$ si chiama *morfismo* o *omomorfismo* se:

$$f(a \circ b) = f(a) * f(b) \text{ per ogni } a, b \in S_1.$$

DEFINIZIONE 26 Siano (S_1, \circ) e $(S_2, *)$ strutture algebriche con operazioni esterne aventi lo stesso dominio di operatori A . Una applicazione $f: S_1 \rightarrow S_2$ si chiama *morfismo* se:

$$f(\alpha \circ a) = \alpha * f(a), \text{ per ogni } \alpha \in A \text{ e } a \in S_1.$$

DEFINIZIONE 27 Un *morfismo* fra due strutture

$$(S_1, \circ_1, \circ_2, \dots, \circ_n) , (S_2, *_1, *_2, \dots, *_n)$$

ad n operazioni é una applicazione $f: S_1 \rightarrow S_2$ se é un morfismo fra (S_1, \circ_j) e $(S_2, *_j)$, per ogni $j = 1, 2, \dots, n$.

OSSERVAZIONE 28 Un morfismo biiettivo é un isomorfismo. La nozione di morfismo é dunque una generalizzazione di quella di isomorfismo. Essa é molto utile perché due strutture non isomorfe possono essere legate tra loro da un morfismo e, come vedremo, vi sono proprietà delle strutture algebriche che sono conservate dai morfismi.

DEFINIZIONE 29 Un morfismo f si dice *monomorfismo* se é iniettivo, *epimorfismo* se é suriettivo.

morfismi

ESERCIZIO 30 Siano $S_1 = (S_1, \circ)$ e $S_2 = (S_2, *)$ due strutture algebriche con operazioni interne e $f: S_1 \rightarrow S_2$ un monomorfismo. Provare che $f(S_1)$ é una parte stabile di $(S_2, *)$. Provare inoltre che la restrizione $f: S_1 \rightarrow f(S_1)$ é un isomorfismo fra (S_1, \circ) e la struttura algebrica indotta da $(S_2, *)$ su $f(S_1)$.

ESERCIZIO 31 Provare le seguenti implicazioni:

- $S_1 \xrightarrow{f} S_2 \xrightarrow{g} S_3$, f, g morfismi $\Rightarrow S_1 \xrightarrow{fg} S_3$ morfismo.
- $S_1 \xrightarrow{f} S_2$, f morfismo, X parte stabile di $S_1 \Rightarrow f(X)$ parte stabile di S_2 .

ESEMPI 32

- Le applicazioni $a \in N \rightarrow a \in Z$, $a \in Z \rightarrow a \in Q$, $a \in Q \rightarrow a \in R$, $a \in R \rightarrow a \in C$ sono morfismi rispetto alle operazioni $+$ e \cdot .
- L'applicazione $m \in Z \rightarrow [m] \in Z_n$ é un morfismo rispetto alle operazioni $+$ e \cdot .
- L'applicazione $A \in M_n(K) \rightarrow \det(A) \in K$, $K = Q, R, C$, é un morfismo fra $(M_n(K), \cdot)$ e (K, \cdot) .

ESEMPIO 33 Siano V e W spazi vettoriali su un campo F . Allora ogni applicazione lineare fra V e W é un omomorfismo fra i gruppi additivi di V e W .

DEFINIZIONE 34 Un morfismo di una struttura algebrica S in se stessa si chiama *endomorfismo* di S . Un isomorfismo di una struttura algebrica in se stessa si chiama *automorfismo* di S .

gruppi

DEFINIZIONE 35 Una struttura algebrica (S, \circ) si chiama *gruppo* se é un semigruppó con elemento neutro e con tutti gli elementi simmetrizzabili. In altre parole (S, \circ) é un gruppo se sono verificate le seguenti proprietá:

1. l'operazione \circ é associativa;
2. esiste l'elemento neutro u ;
3. ogni elemento di S é simmetrizzabile.

Se l'operazione \circ é commutativa il gruppo si dice *commutativo* o *abeliano*.

Un gruppo si dice *moltiplicativo* (risp. *additivo*) se per la sua operazione si usa la notazione moltiplicativa (risp. additiva). Richiamiamo esplicitamente l'attenzione del Lettore sul fatto che la scelta della notazione per l'operazione di un gruppo é ininfluente sulle proprietá algebriche del gruppo stesso.

gruppi

ESEMPI 36 Le strutture sottoelencate sono esempi di gruppi.

- $(Z, +), (Q, +), (R, +), (C, +), (Z_n, +)$ (*gruppi additivi di Z, Q, R, C, Z_n*).
- $(nZ, +)$, con $n \in Z$ e $nZ = \{nz : z \in Z\}$.
- $(Q^*, \cdot), (R^*, \cdot), (C^*, \cdot), (U(n), \cdot), (Z_p^*, \cdot)$ *p* primo (*gruppi moltiplicativi di Z, Q, R, C, Z_p*).
- $(Z[x], +), (Q[x], +), (R[x], +), (C[x], +)$ (*gruppi additivi di $Z[x], Q[x], R[x], C[x], Z_n[x]$*).
- $(M_{m,n}(A), +)$, con $A = Z, Q, R, C$ (*gruppo additivo di $M_{m,n}(A)$*).
- $(GL(n, F), \cdot)$, con $F = Q, R, C$ e $GL(n, F) :=$ insieme delle matrici quadrate ad elementi in F con determinante non nullo (*gruppo lineare (generale)*).
- $(SL(n, F), \cdot)$, con $F = Q, R, C$ e $GL(n, F) :=$ insieme delle matrici quadrate ad elementi in F con determinante 1 (*gruppo lineare speciale*).
- $(P(S), \star)$, ove \star é l'operazione di differenza simmetrica nell'insieme delle parti di un insieme non vuoto S .
- (G_n, \cdot) , con $G_n = \{z \in C : z^n = 1\}$ (*il gruppo delle radici n -esime dell'unitá di C*).

ESERCIZIO 37 Provare che un numero complesso α é una radice n -esima dell'unitá di C se, e solo se, é del tipo $\alpha = \cos(2\frac{m}{n}\pi) + i \sin(2\frac{m}{n}\pi)$, con $m \in Z$.

ESEMPIO 38 Sia V uno spazio vettoriale su un campo F , per esempio $F = Q, R, C$. Allora V , rispetto all'addizione fra vettori, é un gruppo abeliano, detto *gruppo additivo di V* .

ESERCIZIO 39 *Provare che l'insieme $Aut(S)$ degli automorfismi di una struttura algebrica S é un gruppo rispetto al prodotto tra funzioni (il gruppo degli automorfismi di S).*

Nel seguito, tranne esplicito avviso, $G = (G, \cdot)$ denoterá sempre un gruppo moltiplicativo.

ESERCIZIO 40 *Siano a, b elementi di un gruppo G . Provare che ciascuna delle equazioni $ax = b$ e $xa = b$ ammette un'unica soluzione in G .*

DEFINIZIONE 41 Si chiama potenza n -esima di un elemento $a \in G$, e si denota con a^n , l'elemento di G definito per ricorrenza da

- per $n \geq 0$:

$$a^0 = 1, \quad a^n = a^{n-1}a,$$

- per $n < 0$:

$$a^n = (a^{-1})^{-n}.$$

OSSERVAZIONE 42 Sono verificate le seguenti proprietá, per ogni $a, b \in G$.

- $a^m a^n = a^{m+n} = a^n a^m$.
- $ab = ba \Rightarrow (ab)^n = a^n b^n$.

ESERCIZIO 43 *Trovare quattro matrici quadrate A, B, C, D in $GL(2, Q)$ tali che $(AB)^2 \neq A^2 B^2$ e $(CD)^2 = C^2 D^2$.*

gruppi

DEFINIZIONE 44 Sia a un elemento di G . Se esiste un intero $m \neq 0$ tale che $a^m = 1$ si dice che a é *periodico* o che ha *ordine finito*. In questo caso, il piú piccolo intero positivo n tale che $a^n = 1$ si chiama *ordine* o *periodo* di a e si denota con $|a|$ o con $o(a)$. Se per ogni intero positivo m risulta $a^m \neq 1$ si dice che a é *aperiodico* o che ha *ordine infinito*.

ESERCIZIO 45 *Provare che un gruppo finito G d'ordine pari contiene almeno un elemento di periodo due.*

PROPOSIZIONE 46 *Siano a un elemento di un gruppo G di periodo n ed m un intero positivo. Allora risulta $a^m = 1$ se, e solo se, m é un multiplo di n .*

DIM. Se é $m = hn$, risulta

$$a^m = a^{hn} = (a^n)^h = 1^h = 1,$$

cióé la prima parte dell'asserto. Se é $a^m = 1$, detti q ed r il quoziente ed il resto della divisione tra m ed n , risulta

$$1 = a^m = a^{nq+r} = (a^n)^q a^r = a^r.$$

Allora, essendo r un intero non negativo minore di n , deve essere $r = 0$ e l'asserto é provato.

OSSERVAZIONE 47 L'unitá é l'unico elemento di un gruppo di periodo 1.

ESERCIZIO 48 *L'analogo additivo del concetto di potenza n -sima di un elemento a si chiama multiplo di a secondo l'intero n e si denota con na . Definire i multipli in un gruppo additivo e studiarne le prime proprietá. Definire l'ordine di un elemento di un gruppo additivo.*

ESERCIZIO 49 Siano $n > 1$ ed $h \not\equiv 0 \pmod{n}$ due interi. Allora il periodo di h nel gruppo additivo $(\mathbb{Z}_n, +)$ degli interi modulo n é uguale a $\frac{n}{MCD(n,h)}$. In particolare, h ha ordine n se, e solo se, n ed h sono coprimi.

SOLUZIONE Poniamo $k = \frac{n}{MCD(n,h)}$.

Se n ed h sono coprimi, cioè $k = n$, h ha periodo n in $(\mathbb{Z}_n, +)$ perché nessuno degli interi

$$h, 2h, 3h, \dots, (n-1)h$$

é divisibile per n ; altrimenti h avrebbe un fattore non banale in comune con n .

Se n ed h non sono coprimi, non é restrittivo supporre che h sia minore di n perché ogni intero é congruo modulo n al proprio resto della divisione per n . In queste ipotesi risulta $n = kh$ e gli interi

$$h, 2h, 3h, \dots, (k-1)h,$$

essendo positivi e minori di n , non sono divisibili per n . Ne segue che k é il periodo di h e l'asserto é provato.

ESEMPI 50

- In $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ ogni elemento diverso da zero ha ordine infinito.
- In (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) ogni elemento diverso da 1 e -1 ha ordine infinito e risulta $o(-1) = 2$.
- In (\mathbb{C}^*, \cdot) un elemento diverso da 1 ha periodo finito se, e solo se, é una radice n -esima dell'unitá, per qualche intero $n > 1$. Ne segue che gli elementi di periodo finito sono tutti e soli quelli del tipo

$$\cos\left(2\frac{m}{n}\pi\right) + i \operatorname{sen}\left(2\frac{m}{n}\pi\right), \text{ con } m, n \text{ interi e } n > 0.$$

Ogni radice n -esima dell'unitá ha ordine minore o uguale ad n . Quelle che hanno ordine n si chiamano *primitive* e sono quelle in corrispondenza di m ed n coprimi.