

morfismi di gruppi

ESERCIZIO 1 Sia f un omomorfismo di G in G' . Provare le seguenti proprietà:

- $H \leq G \Rightarrow f(H) \leq G'$.
- $H = \langle a \rangle$ sottogruppo ciclico di $G \Rightarrow f(H)$ sottogruppo ciclico di G' generato da $f(a)$.
- H sottogruppo abeliano di $G \Rightarrow f(H)$ sottogruppo abeliano di G' .
- H sottogruppo normale di $G \Rightarrow f(H)$ sottogruppo normale di $f(G')$.
- K sottogruppo di $G' \Rightarrow f^{-1}(K)$ sottogruppo di G .
- K sottogruppo normale di $G' \Rightarrow f^{-1}(K)$ sottogruppo normale di G .

ESERCIZIO 2 Sia f un isomorfismo fra i gruppi G e G' . Provare le seguenti proprietà:

- H sottogruppo normale di $G \Leftrightarrow f(H)$ sottogruppo normale di G' .
- $a \in G$ e $|a| = n \Leftrightarrow |f(a)| = n$.
- H sottogruppo di G con $|H| = n \Leftrightarrow |f(H)| = n$.

ESERCIZIO 3 Provare che S_3 e un gruppo ciclico d'ordine 6 non sono isomorfi.

ESERCIZIO 4 Provare che D_4 non é isomorfo a Q_2 .

teoremi di isomorfismo

TEOREMA 5 (secondo teorema di isomorfismo) Siano H, K sottogruppi di un gruppo G tali che H é normale in $\langle H, K \rangle$. Allora i gruppi $\frac{\langle H, K \rangle}{H}$ e $\frac{K}{H \cap K}$ sono isomorfi.

TEOREMA 6 (terzo teorema di isomorfismo) Siano H e K sottogruppi normali di G , con $H \leq K$. Allora risulta

$$\frac{G/H}{K/H} \sim G/K.$$

DIM. Poniamo

$$\pi : a \in G \rightarrow aH \in G/H,$$

$$\pi_1 : aH \in G/H \rightarrow (aH)(K/H) \in \frac{G/H}{K/H}.$$

La funzione

$$\pi_2 = \pi \pi_1 : a \in G \rightarrow (aH)(K/H) \in \frac{G/H}{K/H}$$

é un epimorfismo, perché prodotto di epimorfismi. Inoltre abbiamo:

$$a \in G, a \in \text{Ker} \pi_2 \Leftrightarrow \pi_2(a) = (aH)(K/H) = K/H \Leftrightarrow aH \in K/H \Leftrightarrow a \in K,$$

da cui segue che $\text{Ker} \pi_2 = K$. Allora dal teorema di omomorfismo abbiamo

$$G/\text{Ker} \pi_2 = G/K \sim \pi_2(G) = \frac{G/H}{K/H},$$

cioé l'asserto.

classificazione dei gruppi ciclici

TEOREMA 7 (teorema di classificazione) Sia $G = \langle a \rangle$ un gruppo ciclico. Allora,

(i) se G é infinito, G é isomorfo a $(\mathbb{Z}, +)$,

(ii) se G é finito d'ordine m , allora G é isomorfo a $(\mathbb{Z}_m, +)$.

DIM. Consideriamo la seguente funzione suriettiva

$$f : n \in \mathbb{Z} \rightarrow a^n \in G. \quad (1)$$

Poiché risulta

$$f(b + c) = a^{b+c} = a^b a^c = f(b)f(c),$$

abbiamo che f é un epimorfismo e quindi $\mathbb{Z}/\text{Ker}f \sim G$. Ne segue che

- G infinito $\Rightarrow \mathbb{Z}/\text{Ker}f$ infinito $\Rightarrow \text{Ker}f = \{0\} \Rightarrow \mathbb{Z}/\text{Ker}f = \mathbb{Z}$.
- G finito con $|G| = m \Rightarrow |\mathbb{Z}/\text{Ker}f| = m \Rightarrow \mathbb{Z}/\text{Ker}f = \mathbb{Z}_m$.

proprietá gruppi ciclici

PROPOSIZIONE 8 Se $G = \langle a \rangle$ é un gruppo ciclico, valgono le seguenti proprietá:

1. G é abeliano.
2. Se G é infinito, allora $a^h = a^k$ se, e soltanto se, $h = k$.
3. Se G é infinito, allora $G = \langle a^m \rangle$ se, e soltanto se, $m = \pm 1$.
4. G é finito d'ordine m se, e soltanto se, $|a| = m$ e $G = \{a^0, a, a^2, \dots, a^{m-1}\}$.
5. Se G é finito d'ordine m , allora $a^h = a^k$ se, e soltanto se, $h \equiv k \pmod{m}$.
6. Se G é finito d'ordine m , allora $G = \langle a^h \rangle$ se, e soltanto se, $\text{MCD}(h, m) = 1$.
7. Ogni sottogruppo di G é ciclico.
8. Se G é finito d'ordine m e se d é un divisore positivo di m con $m = dk$, allora G possiede un unico sottogruppo C_d d'ordine d , dato da $C_d = \langle a^k \rangle$.
9. Ogni quoziente di G é ciclico. Se G é infinito ed m un intero positivo, $G / \langle a^m \rangle$ é isomorfo a $(\mathbb{Z}_m, +)$. Se G é finito d'ordine m ed é $m = hk$, $G / \langle a^h \rangle$ é isomorfo a $(\mathbb{Z}_h, +)$.

gruppi ciclici

OSSERVAZIONE 9 Il fatto che tutti i sottogruppi propri di un gruppo ciclico siano ciclici non é una proprietá caratteristica di tali gruppi. Daremo ora un esempio di gruppo non ciclico con la proprietá che tutti i suoi sottogruppi propri sono ciclici. A tale scopo, fissiamo un primo positivo p e, per ogni intero positivo n , denotiamo con G_{p^n} il gruppo delle radici p^n -esime dell'unitá del campo complesso. E' facile verificare che, rispetto al prodotto fra numeri complessi,

$$G = \bigcup_{n \geq 1} G_{p^n}$$

costituisce un gruppo infinito. Tale gruppo non é ciclico; infatti ogni suo elemento diverso da 1, essendo una radice p^n -esima dell'unitá, per un opportuno n , genera un sottogruppo finito. Inoltre i gruppi G_{p^n} formano in G una catena infinita di sottogruppi con minimo $\{1\}$ e massimo G :

$$\{1\} \leq G_p \leq G_{p^2} \leq \cdots \leq G_{p^n} \leq \cdots \leq G.$$

Ora, detto H un sottogruppo proprio di G , deve esistere un intero positivo m tale che, per ogni $n > m$, H non contiene radici p^n -esime dell'unitá, altrimenti sarebbe $H = G$. Allora H é contenuto in G_{p^m} che é ciclico e, quindi, H stesso é ciclico. Resta cosí provato che tutti i sottogruppi propri di G sono ciclici.

ESERCIZIO 10 Sia G il sottogruppo additivo del campo complesso. Provare che G non é ciclico.

anelli quoziente

Sia H un ideale bilatero di un anello A e, considerato H come sottogruppo del gruppo additivo di A , denotiamo con A/H l'insieme quoziente di A rispetto alla relazione \mathfrak{R}_H . Sappiamo che in A/H l'operazione di addizione

$$(a + H) + (b + H) = (a + b) + H, \quad a, b \in A$$

definisce un gruppo abeliano.

In A/H risulta ben definita anche la seguente operazione di moltiplicazione:

$$(a + H)(b + H) = (ab) + H, \quad a, b \in A.$$

La struttura algebrica $(A/H, +, \cdot)$ risulta un anello.

DEFINIZIONE 11 L'anello $(A/H, +, \cdot)$, che denoteremo con A/H , si chiama *anello quoziente di A rispetto all'ideale H* .

PROPOSIZIONE 12 Valgono le seguenti proprietà:

- A commutativo $\Rightarrow A/H$ commutativo.
- A unitario con unità $1 \Rightarrow A/H$ unitario con unità $1 + H$.
- A unitario, $a \in A$ invertibile $\Rightarrow a + H$ invertibile e $(a + H)^{-1} = a^{-1} + H$.
- Gli ideali sinistri (destri, bilateri) di A/H sono tutti e soli quelli del tipo K/H ove K è un ideale sinistro (destro, bilatero) di A contenente H .

ESERCIZIO 13 I quozienti non banali dell'anello degli interi relativi sono tutti e soli gli anelli Z_m , $m > 1$.