

.

Capitolo 9

Quozienti e Morfismi di Gruppi e Anelli

9.1 Sottogruppi normali e gruppi quoziente

Siano G un gruppo e H un suo sottogruppo.

PROPOSIZIONE 9.1.1 I laterali sinistri e destri (cfr.def.6.3.4) del sottogruppo H di G verificano le seguenti proprietà:

$$x, y, a \in G, xH = yH \Rightarrow (ax)H = (ay)H; \quad (9.1)$$

$$x, y, a \in G, Hx = Hy \Rightarrow H(xa) = H(ya); \quad (9.2)$$

DIMOSTRAZIONE. Per i laterali sinistri di H abbiamo:

$$\begin{aligned} xH = yH &\Rightarrow x \equiv y(\text{mod } \mathfrak{R}'_H), a \in G \Rightarrow x^{-1}y \in H, a \in G \\ &\Rightarrow x^{-1}y = x^{-1}a^{-1}ay = (ax)^{-1}(ay) \in H \Rightarrow ax \equiv ay(\text{mod } \mathfrak{R}'_H) \Rightarrow (ax)H = (ay)H. \end{aligned}$$

In modo analogo si ragiona per i laterali destri. \diamond

DEFINIZIONE 9.1.2 Si dice che H è un sottogruppo *normale*¹ di G , o che H è *normale* in G , se risulta $\mathfrak{R}'_H = \mathfrak{R}''_H$, cioè se

$$aH = Ha, \quad \text{per ogni } a \in G.$$

Per indicare che H è un sottogruppo normale di G si usa la notazione $H \triangleleft G$. Per un sottogruppo normale H non c'è differenza tra laterali sinistri e destri; per tale motivo, si parla semplicemente di *laterali* e si pone $\mathfrak{R}_H = \mathfrak{R}'_H = \mathfrak{R}''_H$. Nell'ipotesi che H sia normale in G l'insieme quoziente G/\mathfrak{R}_H si denota più semplicemente con G/H . \diamond

OSSERVAZIONE 9.1.3 I sottogruppi banali $\{1\}$ e G sono normali in G . \diamond

¹I sottogruppi normali di un gruppo G sono stati considerati per la prima volta da *Evariste Galois* nel caso $G = S_n$ nell'ambito dello studio delle equazioni algebriche risolubili per radicali.

Figura 9.1: E.Galois (1811-1832)

PROPOSIZIONE 9.1.4 Sia $H \triangleleft G$. Allora valgono le seguenti proprietà:

$$x, y, a, b \in G, \quad xH = aH, \quad yH = bH \Rightarrow (xy)H = (ab)H; \quad (9.3)$$

$$x, y, a, b \in G, \quad xH = aH, \quad yH = bH \Rightarrow H(xy) = H(ab); \quad (9.4)$$

DIMOSTRAZIONE. Segue facilmente dalle (9.1) (9.2) ed è lasciata per esercizio al Lettore. \diamond

DEFINIZIONE 9.1.5 Sia H un sottogruppo normale di G . Nell'insieme G/H dei laterali sinistri di H in G , in forza della (9.3), è ben definita l'operazione

$$(aH)(bH) = (ab)H, \quad \text{per ogni } aH, bH \in G/H$$

e la struttura algebrica $(G/H, \cdot)$ risulta un gruppo, che si chiama *gruppo quoziente* di G rispetto ad H e si denota semplicemente con G/H . \diamond

ESERCIZIO 9.1.6 Provare che in un gruppo quoziente G/H risulta

$$1 = H \quad \text{e} \quad (aH)^{-1} = (a^{-1})H, \quad \text{per ogni } aH \in G/H.$$

OSSERVAZIONI 9.1.7 Valgono le seguenti proprietà:

- $G/\{1\} = G$ e $G/G = \{1\}$ (*quozienti banali*).
- $H \leq Z(G) \Rightarrow H$ è normale in G (in particolare $Z(G)$ è normale in G).
- Se G è abeliano, ogni suo sottogruppo è normale.
- $|G : H| = 2 \Rightarrow H$ è normale in G .
- $H \triangleleft G \Rightarrow H$ permutabile con ogni $K \leq G$.
- $H \triangleleft G, K \leq G \Rightarrow \langle H, K \rangle = HK$. \diamond

ESEMPIO 9.1.8 (quozienti di $(Z_n, +)$) Consideriamo il gruppo additivo $(Z_n, +)$ degli interi modulo n e, detto m un divisore positivo di n , sia $n = mk$. Allora (cfr. 6.1.33 e 6.1.34) $(Z_n, +)$ possiede un unico sottogruppo d'ordine m dato da

$$Z_m = \{0, k, 2k, \dots, (m-1)k\}.$$

Ne segue che il gruppo quoziente $\frac{Z_n}{Z_m}$ é dato da

$$\frac{Z_n}{Z_m} = \{Z_m, 1 + Z_m, 2 + Z_m, \dots, (k-1) + Z_m\}$$

ed é evidentemente isomorfo a $(Z_k, +)$. ◇

ESERCIZIO 9.1.9 Il gruppo alterno A_4 , che ha ordine 12, non possiede sottogruppi d'ordine 6.

SOLUZIONE. Un eventuale sottogruppo H di A_4 d'ordine 6 avrebbe indice 2 in A_4 e, quindi, sarebbe normale. Allora nel gruppo quoziente $G/H = \{H, \sigma H\}$, con $\sigma \in G \setminus H$, avremmo $H^2 = H$ e $(\sigma H)^2 = (\sigma^2)H = H$, cioè

$$\tau \in A_4 \Rightarrow \tau^2 \in H.$$

Questo significa che H dovrebbe contenere i quadrati di tutti gli elementi di A_4 e ciò é assurdo perché H ha ordine 6 e in A_4 ci sono piú di 6 elementi quadrati avendosi:

$$(1, 3, 2)^2 = (1, 2, 3), (1, 2, 3)^2 = (1, 3, 2), (1, 2, 4)^2 = (1, 4, 2), (1, 4, 2)^2 = (1, 2, 4),$$

$$(1, 3, 4)^2 = (1, 4, 3), (1, 4, 3)^2 = (1, 3, 4), (2, 3, 4)^2 = (2, 4, 3), (2, 4, 3)^2 = (2, 3, 4).$$

L'asserto é cosí completamente provato. ◇

DEFINIZIONE 9.1.10 Un gruppo G si dice *semplice* se i due sottogruppi banali $\{1\}$ e G sono i suoi soli sottogruppi normali². ◇

ESERCIZIO 9.1.11 Provare che il gruppo alterno A_n ha indice 2 nel gruppo simmetrico S_n e quindi A_n é normale in S_n . Descrivere il gruppo quoziente S_n/A_n .

ESERCIZIO 9.1.12 Provare che il gruppo H delle rotazioni di un poligono regolare P_n ha indice 2 nel gruppo diedrale D_n e quindi é normale in S_n . Descrivere il gruppo quoziente D_n/H .

ESERCIZIO 9.1.13 Verificare se il sottogruppo ciclico di D_n generato da una riflessione é normale in D_n .

ESERCIZIO 9.1.14 Determinare tutti i sottogruppi normali del gruppo Q_2 dei quaternioni (cfr. 6.3.20).

²L'aggettivo *semplice* usato per questa classe di gruppi trova la sua motivazione nel fatto che un gruppo privo di sottogruppi normali non banali ha solo quozienti (e quindi, come vedremo, immagini epimorfe) banali. I gruppi semplici furono definiti per la prima volta da *Camille Jordan*.

ESERCIZIO 9.1.15 Siano H un sottogruppo normale di G e K un sottogruppo di G contenente H . Provare che H é normale in K .

OSSERVAZIONE 9.1.16 Se H é un sottogruppo normale di un gruppo G e se K é un sottogruppo normale di H , il sottogruppo K non é in generale normale in G (cfr. esercizio 9.6.4). \diamond

PROPOSIZIONE 9.1.17 Per un sottogruppo H di un gruppo G sono equivalenti le seguenti condizioni:

- (a) H é normale in G ;
- (b) $a^{-1}Ha = H$, per ogni $a \in G$;
- (c) $a^{-1}Ha \subseteq H$, per ogni $a \in G$;
- (d) per ogni $a \in G$ e $h \in H$, esiste $h' \in H$ tale che $ah = h'a$.

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. \diamond

PROPOSIZIONE 9.1.18 Sia H un sottogruppo normale di G . Un sottoinsieme Γ di G/H é un sottogruppo di G/H se, e soltanto se, esiste un sottogruppo K di G contenente H tale che $\Gamma = K/H$.

DIMOSTRAZIONE. Se K é un sottogruppo di G contenente H , é facile verificare che

$$H \triangleleft K \Rightarrow K/H \leq G/H.$$

Se Γ é un sottogruppo di G/H abbiamo

$$H \subseteq K = \bigcup_{aH \in \Gamma} aH \subseteq G$$

e K é un sottogruppo di G perché:

$$a, b \in K \Rightarrow aH, bH \in \Gamma \Rightarrow (a^{-1}b)H \in \Gamma \Rightarrow a^{-1}b \in K.$$

Per costruzione risulta $H \triangleleft K$ e $\Gamma = K/H$. Si ha cosí l'asserto. \diamond

Figura 9.2: M.E.C.Jordan (1838-1922)

PROPOSIZIONE 9.1.19 Sia $\Gamma = K/H$ un sottogruppo di G/H . Allora Γ é normale in G/H se, e soltanto se, K é normale in G .

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore.

PROPOSIZIONE 9.1.20 Sia $K = \bigcap_{H \in \mathcal{F}} H$ l'intersezione di un insieme di sottogruppi normali di G . Allora K é normale in G .

DIMOSTRAZIONE. Fissato $h \in K$, per ogni $H \in \mathcal{F}$, risulta

$$a^{-1}ha \in H, \text{ per ogni } a \in G$$

perché $H \triangleleft G$. Ne segue che

$$a^{-1}ha \in K, \text{ per ogni } a \in G,$$

da cui abbiamo $K \triangleleft G$. ◇

ESERCIZIO 9.1.21 Il sottogruppo generato da un insieme di sottogruppi normali in G é normale in G .

9.2 Morfismi di gruppi

Siano G e G' due gruppi. Ricordiamo che una funzione $f : G \rightarrow G'$ fra due gruppi é un *omomorfismo*, o *morfismo di gruppi*, se risulta

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

Valgono le seguenti proprietá:

$$f(1) = 1, \quad f(a^{-1}) = f(a)^{-1}, \quad f(a^n) = f(a)^n,$$

per ogni $a \in G$.

DEFINIZIONE 9.2.1 Sia $f : G \rightarrow G'$ un omomorfismo. L'insieme

$$\text{Ker } f = \{a \in G : f(a) = 1\}$$

prende il nome di *nucleo* dell'omomorfismo f . ◇

PROPOSIZIONE 9.2.2 Sia $f : G \rightarrow G'$ un omomorfismo. Allora il nucleo $H = \text{Ker } f$ di f é un sottogruppo normale di G .

DIMOSTRAZIONE.

• $a, b \in H \Rightarrow f(a) = f(b) = 1, f(a)^{-1} = 1 = f(a^{-1}) \Rightarrow f(a^{-1}b) = f(a^{-1})f(b) = 1 \Rightarrow a^{-1}b \in H \Rightarrow H \leq G$.

• $a \in G, b \in H \Rightarrow f(a^{-1}ba) = f(a^{-1})f(b)f(a) = f(a)^{-1}f(a) = 1 \Rightarrow a^{-1}ba \in H \Rightarrow a^{-1}Ha \subseteq H$. ◇

ESERCIZIO 9.2.3 *Provare che un omomorfismo f fra due gruppi é un monomorfismo se, e solo se, $\text{Ker}f = \{1\}$.*

ESERCIZIO 9.2.4 *Sia K un campo. Provare che $SL(n, K)$ é normale in $GL(n, K)$.*

SOLUZIONE. Se K é un campo, l'applicazione

$$A \in GL(n, K) \rightarrow \det(A) \in K^*$$

é un omomorfismo fra $GL(n, K)$ e il gruppo moltiplicativo di K e il suo nucleo é $SL(n, K)$. Ne segue l'asserto. \diamond

ESERCIZIO 9.2.5 *Provare che $SO(n)$ é normale in $O(n)$.*

ESERCIZIO 9.2.6 *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 9.2.7 *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 9.2.8 *Provare che S_3 e un gruppo ciclico d'ordine 6 non sono isomorfi.*

ESERCIZIO 9.2.9 *Provare che D_4 non é isomorfo a Q_2 .*

9.2.1 Il teorema di omomorfismo

OSSERVAZIONE 9.2.10 Se H é un sottogruppo normale di un gruppo G , allora la proiezione canonica

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

é un epimorfismo, l'*epimorfismo canonico*. \diamond

TEOREMA 9.2.11 (teorema di omomorfismo) *Sia $f : G_1 \rightarrow G_2$ un omomorfismo fra due gruppi. Allora esiste un unico omomorfismo*

$$\varphi : G_1/\text{Ker}f \rightarrow G_2$$

per cui é commutativo il seguente diagramma

$$\begin{array}{ccc}
 G_1 & \xrightarrow{f} & G_2 \\
 \pi \searrow & & \nearrow \varphi \\
 & G_1/Ker f &
 \end{array} \tag{9.5}$$

L'omomorfismo φ é un monomorfismo e i gruppi $G_1/Ker f$ e $f(G_1)$ sono isomorfi.

DIMOSTRAZIONE. Osserviamo che, posto $H = Ker f$, la relazione \mathfrak{R}_H coincide con la relazione \mathfrak{R}_f (cfr.prop.3.4.2), avendosi per ogni $a, b \in G_1$

$$a\mathfrak{R}_H b \Leftrightarrow a^{-1}b \in Ker f \Leftrightarrow f(a^{-1}b) = f(a)^{-1}f(b) = 1 \Leftrightarrow f(a) = f(b) \Leftrightarrow a\mathfrak{R}_f b.$$

Allora, in forza del teorema 3.4.4, esiste un'unica funzione iniettiva $\varphi : G_1/Ker f \rightarrow G_2$ che rende commutativo il diagramma (9.5). D'altra parte, ricordando che

$$\varphi(aH) = f(a), \text{ per ogni } a \in G_1,$$

per ogni $a, b \in G_1$, risulta:

$$\varphi(aH bH) = \varphi((ab)H) = f(ab) = f(a)f(b) = \varphi(aH)\varphi(bH).$$

Ne segue che φ é un morfismo, da cui l'asserto. ◇

OSSERVAZIONE 9.2.12 Con riferimento al teorema precedente, il fatto che i gruppi $G_1/Ker f$ e $f(G_1)$ sono isomorfi é noto anche come *primo teorema di isomorfismo* (dei gruppi). ◇

ESERCIZIO 9.2.13 Sia f un omomorfismo fra i gruppi G e G' . Provare le seguenti proprietá:

- $a \in G$ e $|a| = n \Rightarrow |f(a)|$ divide n .
- H sottogruppo di G con $|H| = n \Rightarrow |f(H)|$ divide n .

ESERCIZIO 9.2.14 Siano G un gruppo, H un suo sottogruppo normale e $a \in G$ un elemento di periodo finito n in G . Provare che aH , come elemento di G/H , ha periodo finito divisore di n .

9.2.2 Teoremi di isomorfismo

Questo paragrafo é dedicato ad alcune prime applicazioni del teorema 9.2.11.

PROPOSIZIONE 9.2.15 Siano H e K due sottogruppi di un gruppo G tali che H é normale in $\langle H, K \rangle$. Allora $H \cap K$ é normale in K .

DIMOSTRAZIONE. Dall'essere H normale in $\langle H, K \rangle$ e dall'esercizio 6.3.10, per ogni $a \in K$, si ha che

$$a(H \cap K) = aH \cap aK = Ha \cap K = Ha \cap Ka = (H \cap K)a.$$

Ne segue che $H \cap K$ é normale in K . ◇

TEOREMA 9.2.16 (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.*

DIMOSTRAZIONE. Cominciamo con l'osservare che, essendo $H \triangleleft \langle H, K \rangle$, H é permutabile con tutti i sottogruppi di $\langle H, K \rangle$ e in particolare con K , per cui risulta

$$\langle H, K \rangle = HK = \{hk : h \in H, k \in K\}.$$

La proposizione precedente assicura che $H \cap K$ é normale in K e quindi possiamo considerare la seguente applicazione tra i gruppi $\frac{K}{H \cap K}$ e $\frac{\langle H, K \rangle}{H}$:

$$f : (H \cap K)k \in \frac{K}{H \cap K} \rightarrow Hk \in \frac{\langle H, K \rangle}{H}.$$

Poiché risulta

$$(H \cap K)k_1 = (H \cap K)k_2 \Leftrightarrow k_1 k_2^{-1} \in H \cap K \Leftrightarrow k_1 k_2^{-1} \in H \Leftrightarrow Hk_1 = Hk_2,$$

l'applicazione f é iniettiva. Inoltre, in forza della prima osservazione, ogni laterale di H in $\langle H, K \rangle$ é del tipo $H(hk)$, con $h \in H$ e $k \in K$, e si ha

$$H(hk) = (Hh)(Hk) = (H)(Hk) = Hk.$$

Ne segue che f é anche suriettiva e, quindi, biunivoca. Infine, f é un isomorfismo perché

$$\begin{aligned} f((H \cap K)k_1 (H \cap K)k_2) &= f((H \cap K)k_1 k_2) = H(k_1 k_2) \\ &= Hk_1 Hk_2 = f((H \cap K)k_1) f((H \cap K)k_2) \end{aligned}$$

e l'asserto é completamente provato. \diamond

TEOREMA 9.2.17 (terzo teorema di isomorfismo) *Siano H e K sottogruppi normali di G , con $H \leq K$. Allora risulta*

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

DIMOSTRAZIONE. 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. \diamond

9.2.3 Gruppi ciclici

Come prima applicazione dei risultati del paragrafo precedente mostreremo la classificazione dei gruppi ciclici.

TEOREMA 9.2.18 (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 $(\mathbb{Z}_m, +)$.*

DIMOSTRAZIONE. Consideriamo la seguente funzione suriettiva

$$f : n \in \mathbb{Z} \rightarrow a^n \in G. \quad (9.6)$$

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 $|G| = m \Rightarrow |\mathbb{Z}/\text{Ker } f| = m \Rightarrow \mathbb{Z}/\text{Ker } f = \mathbb{Z}_m$. ◇

Il teorema di classificazione 9.2.18 assicura che lo studio dei gruppi ciclici é equivalente a quello del gruppo additivo di \mathbb{Z} e del gruppo additivo di \mathbb{Z}_m , al variare di m negli interi maggiori di 1. Allora, tenuto conto dei risultati del paragrafo 6.1.2, della 9.1.8 e dell'epimorfismo (9.6), rimane stabilita la seguente proposizione.

PROPOSIZIONE 9.2.19 *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 $m = hk$, $G / \langle a^h \rangle$ é isomorfo a $(\mathbb{Z}_h, +)$.*

OSSERVAZIONE 9.2.20 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'unit  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   ciclico; infatti ogni suo elemento diverso da 1, essendo una radice p^n -esima dell'unit , 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'unit , altrimenti sarebbe $H = G$. Allora H   contenuto in G_{p^m} che   ciclico e, quindi, H stesso   ciclico. Resta cos  provato che tutti i sottogruppi propri di G sono ciclici. \diamond

ESERCIZIO 9.2.21 Sia G il sottogruppo additivo del campo complesso. Provare che G non   ciclico.

9.3 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.   semplice provare che 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 $(A/H, +, \cdot)$, come subito si verifica, risulta un anello.

DEFINIZIONE 9.3.1 L'anello $(A/H, +, \cdot)$, che denoteremo semplicemente con A/H , si chiama *anello quoziente di A rispetto all'ideale H* .

PROPOSIZIONE 9.3.2 Valgono le seguenti propriet :

- A commutativo $\Rightarrow A/H$ commutativo.
- A unitario con unit  1 $\Rightarrow A/H$ unitario con unit  $1 + H$.
- 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   un ideale sinistro (destro, bilatero) di A contenente H .

DIMOSTRAZIONE. É lasciata al Lettore per esercizio. \diamond

ESERCIZIO 9.3.3 *I quozienti non banali dell'anello degli interi relativi sono tutti e soli gli anelli Z_m , $m > 1$.*

PROPOSIZIONE 9.3.4 *Sia A un anello commutativo unitario e sia $H \leq A$. L'ideale H é massimale se, e solo se, A/H é un campo.*

DIMOSTRAZIONE. Segue facilmente dalla proposizione 7.1.11 e dall'ultima parte della prop. 9.3.2. \diamond

COROLLARIO 9.3.5 *Siano A un campo e $f \in A[x]$ irriducibile su A . Allora $A[x]/(f)$ é un campo.*

PROPOSIZIONE 9.3.6 *Siano A un anello commutativo e H un suo ideale proprio. Allora H é un ideale primo se, e soltanto se, A/H é un dominio d'integritá.*

DIMOSTRAZIONE.

• H primo e $(a + H)(b + H) = H \Rightarrow ab + H = H \Rightarrow ab \in H \Rightarrow a \in H$ oppure $b \in H \Rightarrow a + H = H$ oppure $b + H = H \Rightarrow A/H$ dominio d'integritá.

• A/H dominio d'integritá e $ab \in H \Rightarrow ab + H = (a + H)(b + H) = H \Rightarrow a + H = H$ oppure $b + H = H \Rightarrow a \in H$ oppure $b \in H \Rightarrow H$ primo. \diamond

COROLLARIO 9.3.7 *Sia A un anello commutativo unitario. Allora ogni ideale massimale di A é primo.*

DIMOSTRAZIONE. H massimale $\Rightarrow A/H$ campo $\Rightarrow A/H$ dominio d'integritá $\Rightarrow H$ primo. \diamond

OSSERVAZIONE 9.3.8 Osserviamo che esistono anelli commutativi unitari contenenti ideali primi che non sono massimali. Per esempio, nell'anello $Z[x]$, l'ideale (x) é primo e non massimale (cfr. prop. 8.4.5, 8.4.6).

9.4 Morfismi di anelli e teorema di omomorfismo

Ricordiamo che una funzione $f : A_1 \rightarrow A_2$ fra due anelli é un *omomorfismo*, o *morfismo di anelli*, se risulta

$$f(a + b) = f(a) + f(b), f(ab) = f(a)f(b), \forall a, b \in A_1.$$

OSSERVAZIONI 9.4.1 Se $f : A_1 \rightarrow A_2$ é un omomorfismo, valgono le seguenti proprietá:

- $f(0) = 0$; $f(na) = nf(a)$, $n \in Z$ e $a \in A_1$.
- L'insieme

$$\text{Ker } f = \{a \in A_1 : f(a) = 0\},$$

che si chiama *nucleo* di f , é un ideale bilatero di A_1 .

- f monomorfismo $\Leftrightarrow \text{Ker } f = (0)$.

- Sia H un ideale bilatero di A . Allora, l'applicazione canonica

$$\pi : a \in A \rightarrow a + H \in A/H$$

é un epimorfismo e risulta $\text{Ker}\pi = H$.

- X sottoanello di $A_1 \Rightarrow f(X)$ sottoanello di A_2 .

ESEMPIO 9.4.2 Siano A_1 e A_2 anelli. L'applicazione

$$a \in A_1 \rightarrow 0 \in A_2$$

é un morfismo di anelli, che si chiama *morfismo nullo*. ◇

OSSERVAZIONE 9.4.3 Un omomorfismo fra due anelli unitari non conserva necessariamente l'unitá. Ad esempio, se H é un sottoanello unitario di un anello unitario A con unitá 1_H diversa dall'unitá 1 di A (cfr.(7.1.3)), l'applicazione (*immersione*)

$$a \in H \rightarrow a \in A$$

é un omomorfismo di anelli che non trasforma l'unitá di H nell'unitá di A . ◇

PROPOSIZIONE 9.4.4 Sia $f : A_1 \rightarrow A_2$ un omomorfismo non nullo tra due anelli unitari A_1 e A_2 . Allora, se f é un epimorfismo o se A_2 é un dominio d'integritá, risulta $f(1) = 1$.

DIMOSTRAZIONE. Nell'ipotesi che f sia un epimorfismo, per ogni $a' \in A_2$, esiste $a \in A_1$ tale che $f(a) = a'$ e si ha:

$$a' = f(a) = f(1a) = f(1)f(a) = f(1)a';$$

$$a' = f(a) = f(a1) = f(a)f(1) = a'f(1).$$

Ne segue che deve essere $f(1) = 1$.

Se, ora, supponiamo che A_2 sia un dominio d'integritá, scelto $a \in A_1$ con $f(a) \neq 0$, in forza della legge di cancellazione abbiamo

$$f(a) = f(1a) = f(1)f(a) \Rightarrow 1 = f(1)$$

e l'asserto é completamente provato. ◇

DEFINIZIONE 9.4.5 Un omomorfismo fra due anelli unitari che conservi l'unitá si chiama *omomorfismo*, o *morfismo, di anelli unitari*. ◇

TEOREMA 9.4.6 (teorema di omomorfismo) Sia $f : A_1 \rightarrow A_2$ un omomorfismo fra due anelli. Allora esiste un unico monomorfismo

$$\varphi : A_1/\text{Ker}f \rightarrow A_2$$

per cui é commutativo il seguente diagramma

$$\begin{array}{ccc}
 A_1 & \xrightarrow{f} & A_2 \\
 \pi \searrow & & \nearrow \varphi \\
 & A_1/\text{Ker } f &
 \end{array}$$

Inoltre, gli anelli $A_1/\text{Ker } f$ e $f(A_1)$ sono isomorfi.

DIMOSTRAZIONE. É del tutto simile alla dimostrazione del teorema d'omomorfismo per i gruppi ed é lasciata, per esercizio, al Lettore. \diamond

ESERCIZIO 9.4.7 Siano A_1 un corpo, A_2 un anello e f un omomorfismo non nullo di A_1 in A_2 . Provare che f é un monomorfismo e dedurre da ciò che $f(A_1)$ é un sottocorpo di A_2 isomorfo ad A_1 .

ESERCIZIO 9.4.8 Siano A un anello e $H(X, A)$ l'anello delle funzioni di un insieme non vuoto X in A . Provare che, se si denota con \underline{a} la funzione costante determinata dall'elemento $a \in A$, cioè

$$\underline{a} : x \in X \rightarrow a \in A,$$

allora l'applicazione

$$i : a \in A \rightarrow \underline{a} \in A^S$$

é un monomorfismo e A e $i(A)$ sono isomorfi.

9.4.1 Endomorfismi di un gruppo ciclico

Siano $G = \langle a \rangle$ un gruppo ciclico additivo e $\text{End}(G)$ l'anello dei suoi endomorfismi. E' facile verificare che, per ogni intero n , l'applicazione

$$f_n : a \in G \rightarrow na \in G$$

é un endomorfismo di G .

PROPOSIZIONE 9.4.9 Sia φ un endomorfismo di G . Allora esiste un intero n tale che $\varphi = f_n$.

DIMOSTRAZIONE. Detto n un intero tale che $\varphi(a) = na$, risulta

$$\varphi(ma) = m\varphi(a) = m(na) = n(ma) = f_n(ma)$$

e da ciò segue che $\varphi = f_n$. \diamond

PROPOSIZIONE 9.4.10 La funzione suriettiva

$$g : n \in Z \rightarrow f_n \in \text{End}(G)$$

é un epimorfismo fra gli anelli Z e $\text{End}(G)$.

DIMOSTRAZIONE. Abbiamo che

$$f_{n+m}(x) = (n+m)x = nx + mx = f_n(x) + f_m(x) = (f_n + f_m)(x),$$

da cui segue

$$g(n+m) = f_{n+m} = f_n + f_m = g(n) + g(m).$$

Inoltre

$$f_{nm}(x) = (nm)x = n(mx) = nf_m(x) = f_n(f_m(x)) = (f_n f_m)(x)$$

e quindi

$$g(nm) = f_{nm} = f_n f_m = g(n)g(m),$$

come volevamo dimostrare. \diamond

TEOREMA 9.4.11 *Sia $G = \langle a \rangle$ un gruppo ciclico infinito. Allora $\text{End}(G)$ é isomorfo a Z .*

DIMOSTRAZIONE. Osserviamo che risulta

$$f_n = f_m \Leftrightarrow n = m,$$

da cui segue che g é biunivoca, cioè un isomorfismo. \diamond

TEOREMA 9.4.12 *Sia $G = \langle a \rangle$ un gruppo ciclico finito d'ordine m . Allora $\text{End}(G)$ é isomorfo a Z_m .*

DIMOSTRAZIONE. Osserviamo che risulta

$$f_h = f_k \Leftrightarrow h \equiv k \pmod{m},$$

da cui segue che $\text{Ker } g = mZ$. Allora l'anello quoziente $Z/\text{Ker } g = Z_m$ é isomorfo a $g(Z) = \text{End}(G)$. \diamond

TEOREMA 9.4.13 *Siano $G = \langle a \rangle$ un gruppo ciclico infinito e $\text{Aut}(G)$ il gruppo dei suoi automorfismi. Allora risulta*

$$\text{Aut}(G) = \{f_1, f_{-1}\} \sim (\{1, -1\}, \cdot).$$

DIMOSTRAZIONE. Sappiamo che un endomorfismo di G é del tipo

$$f_n : a \in G \rightarrow na \in G.$$

Se f_n é un automorfismo, allora $f_n(a) = na$ é un generatore di G e quindi $n = \pm 1$. D'altra parte f_1 e f_{-1} sono automorfismi e quindi $\text{Aut}(G) = \{f_1, f_{-1}\}$, come volevamo provare. \diamond

TEOREMA 9.4.14 *Siano $G = \langle a \rangle$ un gruppo ciclico finito d'ordine m e $\text{Aut}(G)$ il gruppo dei suoi automorfismi. Allora risulta*

$$\text{Aut}(G) = \{f_n : n \in U(m)\} \sim U(m).$$

DIMOSTRAZIONE. Sappiamo che un endomorfismo di $(Z_m, +)$ é del tipo

$$f_n : a \in Z_m \rightarrow na \in Z_m.$$

Se f_n é un automorfismo, allora $f_n(a) = na$ é un generatore di G e quindi $MCD(n, m) = 1$, cioè $n \in U(m)$. Se ora supponiamo $n \in U(m)$, cioè $MCD(n, m) = 1$, abbiamo:

- $f_n(a) = f_n(b) \Rightarrow na = nb$ e n é cancellabile $\Rightarrow a = b \Rightarrow f_n$ é iniettiva.
- $a \in Z_m \Rightarrow f_n(an^{-1}) = a \Rightarrow f_n$ é suriettiva.

Ne segue che f_n é un automorfismo. ◇

OSSERVAZIONE 9.4.15 Osserviamo esplicitamente che dai teoremi precedenti si ha che

$$\begin{aligned} \text{End}((Z, +)) &\sim (Z, +, \cdot), & \text{End}((Z_m, +)) &\sim (Z_m, +, \cdot), \\ \text{Aut}((Z, +)) &\sim \{f_1, f_{-1}\}, & \text{End}((Z_m, +)) &\sim U(m). \end{aligned}$$

ESERCIZIO 9.4.16 *Provare che gli endomorfismi dell'anello degli interi sono solo l'endomorfismo nullo e quello identico.*

SOLUZIONE. Un endomorfismo f dell'anello Z é anche un endomorfismo del gruppo additivo di Z . Allora esiste un intero n tale che $f = f_n$ e si ha

$$n = f_n(1) = f_n(1 \cdot 1) = f_n(1)f_n(1) = n^2 \Rightarrow n = 0, 1,$$

come volevamo dimostrare. ◇

ESERCIZIO 9.4.17 *Provare che l'unico automorfismo dell'anello degli interi é l'identità.*

ESERCIZIO 9.4.18 *Provare che gli endomorfismi del campo razionale Q sono solo l'endomorfismo nullo e quello identico.*

SOLUZIONE. Se f é un endomorfismo non nullo di Q , essendo f iniettivo, é $f(1) \neq 0$. Allora abbiamo

$$1f(1) = f(1 \cdot 1) = f(1)f(1) \Rightarrow f(1) = 1$$

e

$$\begin{aligned} n \neq 0 \Rightarrow m = m \cdot 1 = mf(1) = f(m \cdot 1) = f(m) = \\ f\left(\frac{m}{n}n\right) = f\left(\frac{m}{n}\right)n \Rightarrow \frac{m}{n} = f\left(\frac{m}{n}\right), \end{aligned}$$

come volevamo dimostrare. ◇

ESERCIZIO 9.4.19 *Provare che l'unico automorfismo del campo razionale é l'identità.*

9.5 Sottoanello fondamentale di un anello unitario

Sia A un anello unitario. Denotati con u l'unità di A e con 1 l'unità di Z , l'applicazione

$$f : n \in Z \rightarrow nu \in A \quad (9.7)$$

è un morfismo di anelli unitari; infatti, per ogni $n, m \in Z$, si ha

1. $f(n + m) = (n + m)u = nu + mu = f(n) + f(m)$,
2. $f(nm) = (nm)u = n(mu) = (nu)(mu) = f(n)f(m)$,
3. $f(1) = 1u = u$.

DEFINIZIONE 9.5.1 L'immagine dell'omomorfismo (9.7),

$$Im f = \{nu : n \in Z\} \sim Z/Ker f, \quad (9.8)$$

che è un sottoanello di A , si chiama *sottoanello fondamentale* di A e si denota con $E(A)$. \diamond

TEOREMA 9.5.2 Il sottoanello fondamentale $E(A)$ di un anello unitario A è isomorfo a Z o a Z_c , a seconda che A abbia caratteristica rispettivamente 0 o c .

DIMOSTRAZIONE. Dalle (9.7) e (9.8) segue che $E(A) (\sim Z/ker f)$ è isomorfo ad un quoziente di Z e da ciò segue l'asserto. \diamond

PROPOSIZIONE 9.5.3 Sia A un anello unitario integro di caratteristica $c \neq 0$. Allora c è un numero primo ed $E(A)$ è un campo finito d'ordine c .

DIMOSTRAZIONE. Se $c \neq 0$ e A è integro, anche $E(A) \sim Z_c$ è integro. Ne segue che $E(A)$ è un campo d'ordine finito c e c è primo. \diamond

DEFINIZIONE 9.5.4 Sia K un corpo. Allora il sottoanello fondamentale $E(K)$ è un dominio d'integrità e la caratteristica c di K è zero o un numero primo. Inoltre il campo dei quozienti $Q(E(K))$ di $E(K)$ è isomorfo al sottocampo di K

$$\overline{E}(K) = \{ab^{-1} : a \in E(K), b \in E(K)^*\}.$$

Il sottocampo $\overline{E}(K)$ si chiama *sottocampo fondamentale* di K . \diamond

PROPOSIZIONE 9.5.5 Sia K un corpo di caratteristica c . Allora si ha

- $c = 0 \Rightarrow \overline{E}(K) \sim Q$;
- $c \neq 0 \Rightarrow c$ è un primo e $\overline{E}(K) \sim Z_c$;
- $\overline{E}(K)$ è l'intersezione di tutti i sottocorpi di K .

DIMOSTRAZIONE. E' lasciata per esercizio al Lettore. \diamond

9.6 Esercizi

9.6.1 Siano G un gruppo d'ordine 6 e a, b due suoi elementi distinti di periodo 2. Provare che ab non ha periodo due.

9.6.2 Sia m un intero positivo e G un gruppo contenente un unico sottogruppo H d'ordine m . Provare che H é normale in G .

9.6.3 Siano G un gruppo, H, K due suoi sottogruppi e, per $a \in G$, si ponga

$$HaK = \{hak : h \in H, k \in K\};$$

tale insieme si chiama laterale doppio di H e K rispetto ad a . Provare che, per ogni $a, b \in G$, risulta:

- $bK \subseteq HaK$ oppure $HaK \cap bK = \emptyset$; $bK \subseteq HaK$;
- $HaK = HbK$ oppure $HaK \cap HbK = \emptyset$.

Dedurre che i laterali doppi di H e K formano una partizione degli elementi di G .

9.6.4 Siano

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in R^* \right\}, \quad K = \left\{ \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} : a, b \in R^* \right\},$$

$$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in R^* \right\}.$$

Provare che $A = H \cup K$ é un sottogruppo di $GL(2, R)$, che H é un sottogruppo normale di A e che T é un sottogruppo normale di H . Provare inoltre che, posto

$$x = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

risulta

$$y^{-1}xy \notin T$$

e dedurre che T , come sottogruppo, non é normale in A .

9.6.5 Siano

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in Z \right\}, \quad K = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in Z \right\},$$

$$T = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in Z \right\}.$$

Provare che H é un sottogruppo di $GL(2, R)$ e che K é un sottogruppo normale di H . Provare inoltre che T é un sottogruppo di H e che, posto

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

risulta

$$xT \neq Tx.$$

Dedurre che T non è normale in H .

9.6.6 Siano G il gruppo additivo del campo complesso e H il sottogruppo dei numeri reali. Determinare la relazione \mathfrak{K}_H e provare che G/H è isomorfo ad H .

9.6.7 Sia G un gruppo e si supponga che esista un intero positivo n tale che $(ab)^n = a^n b^n$, per ogni $a, b \in G$. Provare che la funzione

$$a \in G \rightarrow a^n \in G$$

è un endomorfismo di G . Dedurre che i sottoinsiemi

$$G^n = \{a^n : a \in G\}, \quad G_n = \{a \in G : a^n = 1\}$$

sono sottogruppi normali di G e che risulta $G_n \sim G/G_n$.

9.6.8 Si considerino i gruppi $(Z_4, +)$ e $(Z_6, +)$ e si costruisca la loro somma diretta $G = Z_4 \oplus Z_6$. Detto H il sottogruppo ciclico di G generato dall'elemento $(0, 1)$, calcolare il gruppo quoziente G/H e provare che questo è isomorfo a $(Z_4, +)$.

9.6.9 Sia U l'insieme dei numeri complessi di norma 1. Provare che U è un sottogruppo del gruppo moltiplicativo dei complessi C^* e che l'applicazione

$$f : a + ib \in C^* \rightarrow \frac{a}{\sqrt{a^2 + b^2}} + i \frac{b}{\sqrt{a^2 + b^2}} \in U$$

è un epimorfismo di gruppi. Provare che il nucleo di f è il sottogruppo R^+ dei numeri reali positivi e dedurre che il gruppo quoziente C^*/R^+ è isomorfo ad U .

9.6.10 Sia R^+ il sottogruppo del gruppo moltiplicativo del campo complesso C^* costituito dai numeri reali positivi. Provare che l'applicazione

$$f : a + ib \in C^* \rightarrow \sqrt{a^2 + b^2} \in R^+$$

è un epimorfismo di gruppi e calcolarne il nucleo. Con riferimento alle notazioni dell'esercizio precedente e posto $C_2 = (\{1, -1\})$, provare che i gruppi C^*/U e R^*/C_2 sono isomorfi.

9.6.11 Sia H un sottogruppo di S_n contenente una permutazione dispari. Provare che esattamente la metà delle permutazioni in H sono dispari e, quindi, l'ordine di H è pari.

9.6.12 Provare che nel gruppo additivo dei razionali risulta

$$\left\langle \frac{n}{m}, \frac{h}{k} \right\rangle = \left\langle \frac{1}{mk} \right\rangle,$$

per ogni $\frac{n}{m}, \frac{h}{k} \in Q^*$. Dedurre che un sottogruppo additivo di Q generato da un numero finito di elementi è ciclico. Provare inoltre che ogni generatore di $(Q, +)$ è infinito.

9.6.13 Sia H il sottogruppo di S_3 generato dal ciclo $(1, 2, 3)$. Provare che H é normale in S_3 e che S_3/H é ciclico. Dedurne che, se un gruppo quoziente G/H é ciclico, non necessariamente G deve essere ciclico.

9.6.14 Descrivere il reticolo dei sottogruppi del gruppo delle radici n -esime dell'unitá nel campo complesso.

9.6.15 Scrivere tutti i generatori e tutti i sottogruppi del gruppo ciclico delle radici 12-esime dell'unitá nel campo complesso.

9.6.16 Sia G un gruppo ciclico d'ordine minimo contenente un sottogruppo H d'ordine 12 e uno K d'ordine 15. Calcolare l'ordine di G e descrivere il sottogruppo intersezione di H e K .

9.6.17 Sia G un gruppo ciclico finito contenente un sottogruppo H d'ordine 12 e uno K d'ordine 15. Calcolare l'intersezione di H e K .

9.6.18 Sia φ l'epimorfismo canonico dell'anello Z degli interi sull'anello Z_n degli interi modulo n . Provare che la funzione

$$\tilde{\varphi} : \sum a_i x^i \in Z[x] \rightarrow \sum \varphi(a_i) x^i \in Z_n[x]$$

é un epimorfismo fra $Z[x]$ e $Z_n[x]$, il cui nucleo é formato da tutti e soli i polinomi con coefficienti in nZ .

9.6.19 Sia A un anello ed I un suo ideale bilatero. Provare che l'anello quoziente A/I é commutativo se, e solo se, risulta $ab - ba \in I$, per ogni $a, b \in A$.

9.6.20 Sia A un anello commutativo. Provare che l'insieme $\mathcal{N}(A)$ degli elementi nilpotenti di A costituisce un ideale di A e che l'anello quoziente $A/\mathcal{N}(A)$ non contiene elementi nilpotenti non nulli.

9.6.21 Verificare quali tra i seguenti anelli quoziente risultano campi: $Z[x]/(x)$, $Q[x]/(x)$, $R[x]/(x^2 - 1)$, $R[x]/(x^2 + 1)$, $Z_2[x]/(x^2 + x + 1)$, $Z_2[x]/(x^3 + x^2 + x + 1)$, $Z_3[x]/(x^2 + x + 1)$.

9.6.22 Siano $p \in Z$ un primo e $I = \{(pn, m) : n, m \in Z\}$. Provare che I é un ideale di $Z \oplus Z$ e che l'anello quoziente $(Z \oplus Z)/I$ é un campo.

.

Indice

Prefazione	1
1 Preliminari e Richiami	3
1.1 Alcune notazioni standard	3
1.2 Richiami sulle funzioni	4
1.3 Proprietá fondamentali degli interi relativi	7
1.4 Varianti del principio di induzione	9
1.5 Equipotenza di Insiemi e Cardinalitá	11
1.6 Coefficienti binomiali	14
1.7 Numeri di Stirling di seconda specie e numeri di Bell	16
1.8 Numeri di Fibonacci e rapporto aureo	18
1.9 Esercizi	20
2 Aritmetica in Z	23
2.1 La divisione euclidea	23
2.2 Sistemi di numerazione	25
2.3 Massimo comune divisore e algoritmo di Euclide	27
2.4 Il teorema fondamentale dell'aritmetica	30
2.5 Alcune proprietá dei primi	32
2.6 Esercizi	36
2.7 Appendice	38
2.7.1 Tabella di distribuzione di primi	38
2.7.2 Primi di Mersenne e numeri perfetti	38
2.7.3 Tabelle di numeri di Fermat	40
3 Relazioni d'ordine e d'equivalenza	43
3.1 Insiemi ordinati e reticoli	43
3.2 Il lemma di Zorn ed una sua applicazione	47
3.3 Relazioni d'equivalenza e insiemi quoziente	48
3.4 Alcune osservazioni sulle funzioni	50
3.5 Esercizi	52

4	Aritmetica Modulare	53
4.1	Gli interi modulo n	53
4.2	Funzione di Eulero e piccolo teorema di Fermat	57
4.3	Congruenze lineari	60
4.4	Esercizi	61
5	Generalit� sulle Strutture Algebriche	63
5.1	Operazioni su un insieme	63
5.2	Semigrupperi	68
5.3	Una tabella riassuntiva	69
5.4	Isomorfismi	70
5.5	Morfismi	72
5.6	Gruppi e primi esempi	73
5.7	Anelli, corpi, campi e primi esempi	77
5.8	Esercizi	79
6	Prime Propriet� dei Gruppi	83
6.1	Sottogruppi di un gruppo	83
6.1.1	Sottogruppi permutabili	86
6.1.2	Sottogruppi di $(Z, +)$ e di $(Z_n, +)$	88
6.2	Esempi notevoli di gruppi	89
6.2.1	Il gruppo simmetrico S_n	89
6.2.2	Il gruppo alterno A_n	93
6.2.3	Gruppi di Permutazioni e Teorema di Cayley	95
6.2.4	Il gruppo diedrale di grado n	95
6.2.5	Il gruppo diedrale infinito	97
6.2.6	Prodotto diretto esterno di gruppi	98
6.2.7	Il 4–gruppo di Klein	99
6.2.8	Il gruppo dei quaternioni	99
6.2.9	L’automorfo di un gruppo	100
6.2.10	Tabella riassuntiva di gruppi	101
6.3	Laterali di un sottogruppo e teorema di Lagrange	101
6.4	Esercizi	105
7	Prime Propriet� degli Anelli	113
7.1	Sottoanelli e ideali di un anello	113
7.1.1	Ideali massimali e primi	115
7.1.2	Ideali di $(Z, +, \cdot)$ e $(Z_n, +, \cdot)$	117
7.2	Il campo dei quozienti di un dominio d’integrit�	118
7.3	Esempi notevoli di anelli	121
7.3.1	Anelli di polinomi	121
7.3.2	Estensioni quadratiche di Z	128
7.3.3	L’anello degli endomorfismi di un gruppo abeliano	130
7.3.4	Il corpo dei quaternioni	130

7.3.5	Anelli di funzioni	132
7.3.6	Somma diretta di anelli	133
7.3.7	Tabella riassuntiva di anelli	134
7.4	Esercizi	135
7.5	Appendice	138
7.5.1	Polinomi e serie formali	138
8	Polinomi	143
8.1	Divisibilit� in un dominio di integrit� unitario	143
8.2	Divisibilit� in anelli di polinomi	146
8.3	Radici di un polinomio	148
8.4	Polinomi irriducibili e primi	150
8.5	Polinomi irriducibili su Q e Z	154
8.5.1	Irriducibilit� di polinomi ciclotomici	157
8.6	Fattorizzazione unica in $Z[x]$	158
8.7	Radici multiple di un polinomio	159
8.8	Fattorizzazione di polinomi su C ed R	161
8.9	Esercizi	162
9	Quozienti e Morfismi di Gruppi e Anelli	165
9.1	Sottogruppi normali e gruppi quoziente	165
9.2	Morfismi di gruppi	169
9.2.1	Il teorema di omomorfismo	170
9.2.2	Teoremi di isomorfismo	171
9.2.3	Gruppi ciclici	173
9.3	Anelli quoziente	174
9.4	Morfismi di anelli e teorema di omomorfismo	175
9.4.1	Endomorfismi di un gruppo ciclico	177
9.5	Sottoanello fondamentale di un anello unitario	180
9.6	Esercizi	181