Capitolo 1

Esercizi di teoria dei gruppi e teoria degli anelli

In questa sezione svolgeremo alcuni esercizi di teoria dei gruppi e teoria degli anelli. Gli esercizi segnati con un asterisco sono più difficili degli altri, quindi, devono essere considerati come elementi di approfondimento per apprendere le tecniche standard di dimostrazione su queste strutture.

1.1 Proprietà fondamentali di un gruppo

1.1.1 Verifica che una struttura con operazione binaria è un gruppo

ESERCIZIO 1. *Dimostrare che l'insieme* $\mathbb{R}$*, dotato dell'operazione* $\cdot$ *definita da:*

$$x \cdot y = \sqrt[3]{x^3 + y^3}$$

è un gruppo.

Dimostrazione. Verifichiamo gli assiomi che definiscono un gruppo:

1. É un'operazione interna. Infatti $x \cdot y \in \mathbb{R}$.
2. L'operazione è associativa. Infatti, dato che $\sqrt[3]{x}$ è una funzione biunivoca:

$$(x \cdot y) \cdot z = (\sqrt[3]{x^3 + y^3}) \cdot z = \sqrt[3]{(\sqrt[3]{x^3 + y^3})^3 + z^3} = \sqrt[3]{x^3 + y^3 + z^3} =$$
$$= \sqrt[3]{(x^3 + \sqrt[3]{+y^3 + z^3})^3} = x \cdot (y \cdot z)$$

3. Esiste l'elemento neutro a destra $e = 0$. Infatti:

$$x \cdot e = \sqrt[3]{x^3 + 0^3} = \sqrt[3]{x^3} = x$$

4. Per ogni elemento x esiste il suo inverso a destra. Sia $x \in (\mathbb{R}, \cdot)$, considero $-x$, allora:

$$x \cdot (-x) = \sqrt[3]{x^3 + (-x)^3} = 0 = e$$

5. L'operazione $\cdot$ è commutatativa:

$$x \cdot y = \sqrt[3]{x^3 + y^3} = \sqrt[3]{y^3 + x^3} = y \cdot x$$

Quindi possiamo concludere che $(\mathbb{R}, \cdot)$ è un gruppo abeliano.

N.B: *Poiché vale la proprietà commutativa basta verificare che esistono elemento neutro ed inverso da una sola parte. Va osservato che in generale gli assiomi che definiscono un gruppo possono essere ridotti, richiedendo solo che l'operazione sia una legge di composizione interna, associativa e che esistano elemento neutro a destra (sinistra) ed inverso a destra (sinistra) di ciascun elemento del gruppo* (vedere dispense). □

ESERCIZIO 2. *Dimostrare che l'insieme T delle matrici 2×2 sull'anello $\mathbb{Z}$ del tipo:*

$$H = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

con $a, b, c \in \mathbb{Z}$ e $a^2 = c^2 = 1$, dotato del prodotto $\cdot$ righe per colonne, è un gruppo.

Dimostrazione. Verifichiamo che sono soddisfatti gli assiomi che definiscono un gruppo:

1. L'operazione $\cdot$ è interna a T. Infatti se considero le due matrici:

$$H_1 = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad H_2 = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$$

   allora il prodotto righe per colonne $H_1 \cdot H_2$ appartiene ancora a T, infatti:

$$H_1 \cdot H_2 = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}$$

   inoltre $(ad)^2 = a^2 d^2 = c^2 f^2 = (cf)^2 = 1$, dato che $a^2 = c^2 = d^2 = f^2 = 1$.

2. Il prodotto è associativo, essendo l'usuale prodotto di matrici.

3. La matrice I appartiene all'insieme Te dunque esiste in T l'elemento neutro.

4. Esiste l'inverso di ogni elemento. Infatti, dato H_1, questo ha determinante diverso da 0, essendo $det(H_1) = ac$. Quindi esiste inversa nell'insieme delle matrici 2×2 data da:

$$H_1^{-1} = \frac{1}{det(H_1)} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix}$$

Per verificare che $(T, \cdot)$ ammette sempre inverso, dobbiamo verificare che $H_1^{-1} \in T$. Per fare questo dobbiamo verificare che $(\frac{c}{det(H_1)})^2 = (\frac{a}{det(H_1)})^2 = 1$. Dato che $a^2 = c^2 = 1$, allora:

$$(\frac{c}{det(H_1)})^2 = \frac{c^2a^2}{(ac)^2} = 1$$

dato che $a^2 = 1$, e:

$$(\frac{a}{det(H_1)})^2 = \frac{a^2c^2}{(ac)^2} = 1$$

dato che $c^2 = 1$.

N.B: *Osserviamo che l'esercizio poteva essere svolto in maniera più veloce ricordando che l'insieme $GL(2, \mathbb{R})$ delle le matrici quadrate di ordine 2, non singolari, a coefficienti reali, è un gruppo rispetto all'usuale prodotto di matrici. Poiché $T \subseteq GL(2, \mathbb{R})$, basta quindi mostrare che T è un sottogruppo usando uno dei criteri per un sottogruppo.*

□

1.1.2 Struttura

E' ben noto che in un gruppo valgono le leggi di semplificazione (o di cancellazione) a sinistra e a destra:

$$x \cdot k = y \cdot k \Rightarrow x = y \tag{1.1}$$

$$k \cdot x = k \cdot y \Rightarrow x = y \tag{1.2}$$

La validità delle leggi di cancellazione è una condizione sufficiente affinché i semigruppi *finiti* siano gruppi.

ESERCIZIO 3 (*). *Dimostrare che un insieme finito S, dotato di un'operazione interna $*$ associativa, che soddisfa la legge di semplificazione a sinistra e a destra è un gruppo.*

Dimostrazione. Dato che S è finito posso numerare i suoi elementi $S = \{s_1, \ldots, s_n\}$ con $n = |S|$. Sia un elemento $a \in S$, devo dimostrare che a ammette inverso e che esiste l'elemento neutro e. Consideriamo l'insieme:

$$L = \{a * s_i,\ s_i \in S\}$$

Dimostriamo che ha cardinalità n. Infatti $|L| \leq n$, inoltre, gli elementi di L sono tutti distinti; consideriamo due elementi qualunque $a*s_i$ e $a*s_j$ con $i \neq j$. Per ipotesi $*$ soddisfa la legge di cancellazione bilatera, quindi, se fossero uguali $a * s_i = a * s_j$ si dedurrebbe che $s_i = s_j$ che è assurdo dato che $i \neq j$. Quindi $|L| = n$. Similmente per $M = \{s_i * a,\ s_i \in S\}$ ricaviamo che $|M| = n$. Dato che $*$ è un'operazione interne gli elementi $a * s_i$ e $s_i * a$ sono elementi di S e quindi, dato che $|M| = n$ e $|L| = n$ ricaviamo che:

$$L = S \ e \ M = S$$

Da questo fatto ricaviamo che deve esistere un s_h per cui vale:

$$a * s_h = a$$

Dimostriamo che $s_h = e$ è elemento neutro a destra di $(S, *)$. Sia b un elemento qualunque di S, allora deve esistere un s_k per cui vale $s_k * a = b$, in questo modo, sfruttando l'associatività di $*$, otteniamo:

$$b * s_h = (s_k * a) * s_h = s_k * (a * s_h) = s_k * a = b$$

Quindi s_h è un elemento neutro destro. Dimostriamo che b ha inverso destro in S. Ripetendo lo stesso ragionamento di prima, possiamo costruire i due insiemi di cardinalità n, $\{s_i * b,\ s_i \in S\}$ e $\{b * s_i,\ s_i \in S\}$. Dato che coincidono con S, allora esiste un s_t tale che:

$$b * s_t = e$$

Quindi s_t è rispettivamente l'inverso destro di b. Per la riduzione degli assiomi di un gruppo $(S, *)$ è quindi un gruppo. □

N.B: *Osservare che la condizione di finitezza, è indispensabile. Esistono infatti semigruppi infiniti in cui valgono le leggi di cancellazione a destra e a sinistra ma che non sono gruppi. Basta considerare, infatti,* $\mathbb{N}$ *rispetto al prodotto. Valgono le leggi di cancellazione, ma* $(\mathbb{N}, \cdot)$ *non è un gruppo.*

ESERCIZIO 4. *Utilizzando il problema precedente, dimostrare che* $\mathbb{Z}_p \setminus \{0\}$*, con p primo, è un gruppo.*

Dimostrazione. Verifichiamo che valgono tutte le ipotesi del precedente esercizio:

1. L'insieme $\mathbb{Z}_p$ è finito.

2. Sappiamo che il prodotto di classi di resti è ben definito ed associativo, dobbiamo però provare che, togliendo la classe $[0]_p$, la legge di composizione rimane una legge di composizione interna. Supponiamo che $[x_1]_p \cdot [x_2]_p = [0]_p$,e proviamo che se $[x_1]_p \neq [0]_p$ segue $[x_2]_p = [0]_p$. La prima equazione, infatti, può essere tradotta in $p|(x_1 \cdot x_2)$, quindi, p essendo primo, deve dividere uno almeno dei due fattori e, poiché da $[x_1]_p \neq [0]_p$ segue che non divide x_1, allora x_2 e cioè $[x_2]_p = [0]_p$.

3. Verifichiamo che vale la legge di cancellazione bilatera. Dimostriamo che vale la legge di cancellazione destra, sia:

   $$[x_1]_p \cdot [h]_p = [x_2]_p \cdot [h]_p$$

   con $[x_1]_p, [x_2]_p, [h]_p$ diversi dallo zero di $\mathbb{Z}_p$. Questa equazione è equivalente a:

   $$[(x_1 - x_2)h]_p = 0$$

   e questo, a sua volta, equivale a dire che i rappresentanti x_1, x_2, h soddisfano:

   $$p|(x_1 - x_2)h$$

Dato che p è primo, allora deve dividere h o $(x_1 - x_2)$; poichè $[h]_p \neq 0$, allora necessariamente $p|(x_1 - x_2)$, cioè:

$$[x_1]_p = [x_2]_p$$

La stessa cosa avviene per la legge di semplificazione sinistra:

$$[h]_p \cdot [x_1]_p = [h]_p \cdot [x_2]_p \Rightarrow [x_1]_p = [x_2]_p$$

e, quindi, vale la legge di semplificazione bilatera.

□

Il precedente gruppo fa parte di una classe più ampia di gruppi:

ESERCIZIO 5. *Dimostrare che nell'insieme $\mathbb{Z}_n \setminus \{0\}$ dotato del prodotto $\cdot$ definito da:*

$$[a]_n \cdot [b]_n := [ab]_n$$

l'insieme degli elementi minore e primi con n, con l'operazione $\cdot$ è un gruppo, detto gruppo di Eulero $(\Phi(n), \cdot)$.

Dimostrazione. Come nella precedente dimostrazione, possiamo verificare che $\cdot$ è un'operazione associativa, in un insieme finito $\Phi(n)$. Verifichiamo la legge di cancellazione destra (la sinistra è analoga). Per fare questo consideriamo tre elementi $x_1, x_2, h \in \Phi(n)$:

$$[x_1]_n \cdot [h]_n = [x_2]_n \cdot [h]_n$$

La precedente equazione è equivalente a dire che:

$$n|(x_1 - x_2)h$$

dato che $MCD(n, h) = 1$, allora necessariamente:

$$n|(x_1 - x_2)$$

cioè $[x_1]_n = [x_2]_n$. □

1.1.3 Potenze di elementi in un gruppo

ESERCIZIO 6. *Dimostrare che un gruppo $(G, \cdot)$ in cui vale:*

$$(a \cdot b)^2 = a^2 \cdot b^2 \ \forall\, a,\ b \in G$$

è un gruppo abeliano.

Dimostrazione. Dato che $(a \cdot b)^2 = (a \cdot b)(a \cdot b) = a \cdot (b \cdot a) \cdot b$, mentre $a^2 \cdot b^2 = a \cdot (a \cdot b) \cdot b$, otteniamo l'uguaglianza:

$$a \cdot (b \cdot a) \cdot b = a \cdot (a \cdot b) \cdot b$$

da cui moltiplicando a destra per b^{-1} e a sinistra per a^{-1}, otteniamo $b \cdot a = a \cdot b$. □

ESERCIZIO 7. *Dimostrare che $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. Usare questa relazione per risolvere l'esercizio precedente.*

Dimostrazione. Dato che $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = e$ e $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = e$, per l'unicità dell'inverso in un gruppo otteniamo:

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Da $(a \cdot b)^2 = a^2 \cdot b^2$ otteniamo $a^{-1} \cdot (a \cdot b) = a \cdot b^2 \cdot (a \cdot b)^{-1} = a \cdot b^2 \cdot (b^{-1} \cdot a^{-1}) = (a \cdot b) \cdot a^{-1}$, quindi moltiplicando a destra per a, otteniamo $a \cdot b = b \cdot a$. □

Nel successivo esercizio omettiamo il simbolo $\cdot$ e scriviamo $a \cdot b = ab$.

ESERCIZIO 8. *Sia G un gruppo per cui esiste un $r \in \mathbb{Z}$ tale che:*

$$ab = ba^r$$

dimostrare:

1. $a^n b = ba^{rn}$, $\forall n \in \mathbb{N}$.
2. $ab^n = b^n a^{r^n}$, $\forall n \in \mathbb{N}$.

Dimostrazione.

1. Per induzione su n. Osserviamo che la base dell'induzione è vera, infatti per ipotesi: $ab^1 = ba^{1r}$. Supponiamo vero l'assunto per $n-1$, allora moltiplicando a sinistra per a la relazione: $a^{(n-1)}b = ba^{r(n-1)}$, otteniamo $a^n b = a(a^{(n-1)}b) = a(ba^{r(n-1)}) = (ab)a^{r(n-1)}$ e, dato che per ipotesi $ab = ba^r$, otteniamo $a^n b = a(a^{(n-1)}b) = a(ba^{r(n-1)}) = (ab)a^{r(n-1)} = (ba^r)a^{r(n-1)} = ba^r$.

2. Sempre per induzione su n. La base è vera, infatti per ipotesi: $ab = ba^{r^1}$. Supponiamo vera la 2 per $n-1$: $ab^{(n-1)} = b^{(n-1)}a^{r^{(n-1)}}$. Moltiplicando a destra per b questa relazione otteniamo:

$$ab^n = (ab^{(n-1)})b = (b^{(n-1)}a^{r^{(n-1)}})b = b^{(n-1)}(a^{r^{(n-1)}}b)$$

per il primo punto $a^{r^{(n-1)}}b = ba^{r(r^{(n-1)})} = ba^{r^n}$. Quindi otteniamo $ab^n = b^{(n-1)}(ba^{r^n}) = b^n a^{r^n}$.

□

ESERCIZIO 9. *Dimostrare che se in un gruppo G ogni elemento coincide con il proprio inverso, allora G è abeliano.*

Dimostrazione. Osserviamo che in un gruppo di questo tipo tutti gli elementi hanno periodo 2, infatti:

$$e = aa^{-1} = aa = a^2$$

In particolare, considerando il quadrato di ab, si ha:

$$(ab)^2 = e$$

e allora:

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

da cui :

$$ba = ab$$

per il primo esercizio di questo paragrafo, quindi G è abeliano. Potevamo anche dire direttamente che:

$$(ab) = (ab)^{-1} = b^{-1}a^{-1} = (ba)$$

□

1.1.4 Sottogruppi

ESERCIZIO 10. *Dimostrare che il centro di un gruppo G, definito da:*

$$Z(G) = \{x \in G : \ xa = ax \ \forall a \in G\}$$

è un sottogruppo di G.

Dimostrazione. Condizione necessaria e sufficiente affinchè un sottoinsieme H di un gruppo sia un sottogruppo, è che $ab \in H \ a^{-1} \in H \ \forall a, b \in H$. Osserviamo per prima cosa che se $a \in Z(G)$ allora $a^{-1} \in Z(G)$, infatti da $ca = ac \, \forall c \in G$, ricaviamo, moltiplicando a destra e a sinistra per a^{-1}, $a^{-1}caa^{-1} = a^{-1}aca^{-1} \, \forall c \in G$, quindi $a^{-1}c = ca^{-1} \, \forall c \in G$. Inoltre se $a, b \in Z(G)$ e c è un qualunque elemento di G:

$$(ab)c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab)$$

Quindi $ab \in Z(G)$. □

ESERCIZIO 11. *Dimostrare che, dato un elemento $a \in G$ di un gruppo G, il sottoinsieme di G:*

$$< a >:= \{a^m, \ m \in \mathbb{Z}\}$$

è un sottogruppo di G (detto sottogruppo generato da a). Osserviamo che per definizione $a^0 = e$.

Dimostrazione. Basta dimostrare che $cb^{-1} \in < a >$ per tutti i c, b di $< a >$. Prendo due elementi qualunque $c = a^{m_1}$ e $b = a^{m_2}$ in $< a >$, allora $b^{-1} = a^{-m_2}$, quindi $cb^{-1} = a^{m_1}a^{-m_2} = a^{m_1-m_2} \in < a >$, dato che $m_1 - m_2 \in \mathbb{Z}$. Inoltre $< a >$ è abeliano dato che:

$$cb = a^{m_1}a^{m_2} = a^{m_1+m_2} = a^{m_2+m_1} = a^{m_2}a^{m_1} = bc$$

□

ESERCIZIO 12. *Dimostrare che un sottoinsieme H finito di un gruppo $(G, \cdot)$ è un sottogruppo se e solo se $\cdot$ è un'operazione chiusa in H (cioè se e solo se $a \cdot b \in H, \forall a, b \in H$).*

Dimostrazione. La parte solo se è banale. Dimostriamo la parte se

Consideriamo un generico $a \in H$. Dato che l'operazione $\cdot$ è chiusa in H, allora tutte le potenze positive di a:

$$a, a^2, a^3, \ldots, a^n \ldots$$

sono in H. Poichè l'insieme H è finito, nell'insieme $\{a^n,\ n \in \mathbb{N}\}$ ci devono essere delle ripetizioni. Quindi, esistono un m e un t, con $m > t \geq 0$, per cui vale:

$$a^m = a^t$$

Dato che G è un gruppo, la precedente uguaglianza implica:

$$a^{m-t} = e$$

con $m - t > 0$, quindi $e \in \{a^n,\ n \in \mathbb{N}\} \subseteq H$, cioè $e \in H$. Inoltre, se $a \neq e$, si ha $m - t \geq 1$, quindi:

$$e = a \cdot a^{m-t-1} = a^{m-t-1} \cdot a$$

ove $a^{m-t-1} \in H$, essendo $m - t - 1 \geq 0$. Quindi per ogni $a \in H$ esiste inverso in H dato da $a^{-1} = a^{m-t-1}$. In questo modo in H esiste elemento neutro e inverso per ogni a. □

ESERCIZIO 13. *Sia G un gruppo. Sia $g \in G$ tale che $g^n = e$ per qualche intero positivo n. Allora posto $t = min\{n > 0\ g^n = e\}$ provare che*

- *(i) $g, g^2, ..., g^t$ sono tutte e sole le potenze distinte di g*
- *(ii) $g^n = e$ se e solo se $t|n$*

Dimostrazione. (i) Consideriamo tutte le potenze positive di g, poiché per ipotesi t è il minimo intero positivo per cui $g^t = e$ abbiamo che $0 < r < s < t$ implica $g^r \neq g^s$; infatti da $g^r = g^s$ seguirebbe $g^{s-r} = e$ con $0 < s - r < t$, assurdo. Inoltre per ogni $0 < r < t$ si ha $g^r \neq e$. Quindi le potenze $g, g^2, ..., g^t$ sono tutte distinte. Infine per ogni $n \in Z$ esistono q ed r con $0 \leq r < t$ tali che $n = qt + r$ da cui $g^n = g^{qt+r} = (g^t)^q g^r = g^r$ e dunque ogni potenza di g coincide con una delle potenze $g, g^2, ..., g^t$ (tenendo conto che $g^0 = g^t$). (ii) Se $t|n$, cioè $n = th$ si ha subito che $g^n = g^{th} = (g^t)^h = e^h = e$. Se $g^n = e$ esistono q ed r con $0 \leq r < t$ tali che $n = qt + r$ da cui $e = g^n = g^{qt+r} = (g^t)^q g^r = g^r$ e quindi , per le ipotesi fatte su t, si ha $r = 0$. □

Un gruppo G è detto ciclico quando esiste un elemento $g \in G$ per cui $< g >= G$.

ESERCIZIO 14 (*). *Dimostrare che il sottogruppo H di un gruppo ciclico G è ciclico.*

Dimostrazione. Dobbiamo dimostrare che esiste un elemento $h \in G$ per cui $H =< h >$. Supponiamo H non sia ridotto al solo elemento neutro e, in tal caso, infatti, si avrebbe banalmente $H =< e >$. Dato che G è ciclico, allora $G =< g >$. Osserviamo che esiste almeno un $m > 0$ tale che $g^m \in H$, infatti esiste un $s \neq 0$ tale che $g^s \in H$ ma allora $g^{-s} \in H$ e, quindi, è $s > 0$ o $-s > 0$. Consideriamo:

$$t = \min\{n > 0 : \ g^n \in H\}$$

Dimostriamo che $h = g^t$ è il generatore di H. Sia $b \in H$, allora esiste un m tale che $b = g^m$. Per l'algoritmo della divisione di due interi, esistono un q e r interi per cui vale:

$$m = qt + r$$

con $0 \leq r < t$. Quindi:

$$b = g^m = g^{qt+r} = (g^t)^q \cdot g^r = h^q \cdot g^r$$

Dato che $b \in H$ e $(g^t)^q \in H$ (poichè $h = g^t \in H$ e, quindi, anche tutte le sue potenze intere $h^r \in H$), allora:

$$g^r = h^{-q} b \in H$$

da cui per le ipotesi fatte su t , essendo $0 \leq r < t$, si deduce $r = 0$ e, quindi, $b = h^q$. □

ESERCIZIO 15. *Dimostrare che, dati due sottogruppi propri A, B di G. Se $A \cup B$ è un sottogruppo allora $A \cup B = A$, oppure $A \cup B = B$.*

Dimostrazione. Se $A = B$, allora il teorema è vero, supponiamo, allora, che $A \neq B$. In particolare supponiamo che non valgano entrambe le inclusioni delle ipotesi. In questo caso posso prendere $a \in A \setminus B$ e $b \in B \setminus A$. Considero il prodotto $t = ab$. Questo appartiene sicuramente ad $A \cup B$ (essendo un sottogruppo di G), in particolare può appartenere ad A o B. Se $t \in A$, allora ricaverei $ab \in A$ e, quindi: $b \in A$ che è assurdo. Se $t \in B$, allora ricaverei $ab \in B$ e, quindi: $a \in A$ che è assurdo. Quindi dobbiamo concludere che deve valere almeno una delle relazioni $A \cup B = A$, $A \cup B = B$. □

Osserviamo che nell'ultimo esercizio abbiamo dimostrato che un gruppo non può essere unione di due sottogruppi propri.

ESERCIZIO 16 (*). *Dimostrare che in un gruppo in cui esiste un n tale che $(ab)^n = a^n b^n$ per ogni $a, b \in G$, allora:*

1. *$G^n = \{x^n : \ x \in G\}$ è un sottogruppo normale.*
2. *$G^{n-1} = \{x^{n-1} : \ x \in G\}$ è un sottogruppo normale.*

Dimostrazione. Verifichiamo prima che sono sottogruppi e, successivamente, proviamo la normalità:

1. Dimostriamo prima che G^n è un sottogruppo di G. Per ogni $a, b \in G^n$, allora $a = x^n$ e $b = y^n$ e, per ipotesi, $ab = x^n y^n = (xy)^n$ che appartiene a G^n. Inoltre dato $a = x^n$, allora $a^{-1} = x^{-n} = (x^{-1})^n \in G^n$. Per dimostrare che è normale è sufficiente dimostrare $gG^n g^{-1} \subset G^n$ per ogni $g \in G^n$. Ma, preso un elemento di $a \in G^n$ abbiamo:

$$gag^{-1} = gx^n g^{-1} = g\underbrace{xx\ldots x}_{n} g^{-1} = gx\underbrace{g^{-1}gxg^{-1}gx\ldots g^{-1}gx}_{n-1} g^{-1} = (gxg^{-1})^n \in G^n$$

2. Anche in questo caso proviamo il fatto che G^{n-1} è un sottogruppo. Per ogni $a, b \in G^{n-1}$, allora $a = x^{n-1}$ e $b = y^{n-1}$e il loro prodotto $ab = x^{n-1}y^{n-1}$. Osserviamo che per le ipotesi:

$$xaby = x^n y^n = (xy)^n = \underbrace{xyxy\ldots xy}_{n}$$

quindi:

$$ab = \underbrace{yxy\ldots x}_{n-1} = (yx)^{n-1} \in G^{n-1}$$

Dimostriamo la normalità:

$$gG^{n-1}g^{-1} \subseteq G^{n-1}$$

Prendiamo un $g \in G$ allora:

$$gag^{-1} = gx^{n-1}g^{-1} = (gxg^{-1})^{n-1} \in G^{n-1}$$

per ogni $a \in G^{n-1}$.

□

1.1.5 Il teorema di Lagrange (∗)

In questa sezione arriviamo a dimostrare l'importante teorema dovuto a Lagrange alla base di molti sistemi crittografici a chiave pubblica e di molti risultati che riguardano le strutture algebriche.

ESERCIZIO 17. *Sia $H \subseteq G$ un sottogruppo del gruppo G. Dimostrare che la relazione di congruenza definita da:*

$$a \sim_H b \iff ab^{-1} \in H$$

è di equivalenza.

Dimostrazione. Verifichiamo che $\sim_H$ soddisfa le proprietà di una relazione di equivalenza:

1. É riflessiva, dato che $a \sim_H a$, essendo H un sottogruppo e, quindi, $aa^{-1} = e \in H$.
2. É simmetrica. Infatti se $ab^{-1} \in H$, allora (sempre per il fatto che H è un gruppo) anche $(ab^{-1})^{-1} \in H$, cioè $ba^{-1} \in H \iff b \sim_H a$.

3. É transitiva. Dato che se $ab^{-1} \in H$ e $bc^{-1} \in H$, allora $(ab^{-1})(bc^{-1}) \in H$, cioè $a \sim_H c$.

□

Il laterale destro Ha di un sottogruppo H è definito come l'insieme:

$$Ha := \{ha : \ h \in H\}$$

In modo analogo si definisce il laterale sinistro aH. Il motivo dell'introduzione di questa definizione risiede nel prossimo esercizio:

ESERCIZIO 18. *Dimostrare che le classi di equivalenza della relazione di equivalenza $\sim_H$ sono i laterali destri Ha. In pratica $[a]_{\sim_H} = Ha$.*

Dimostrazione. Dimostriamo le due inclusioni:

1. $Ha \subseteq [a]_{\sim_H}$. Sia $b = ha \in Ha$, allora $ba^{-1} = h \in H$, quindi $b \sim_H a$ e, dunque, $b \in [a]_{\sim_H}$
2. $[a]_{\sim_H} \subseteq Ha$. Sia $b \in [a]_{\sim_H}$, allora per definizione $ba^{-1} \in H$, quindi, esiste un $h \in H$ tale che $b = ha$ da cui $b \in Ha$.

□

Nel caso di gruppi finiti, la cardinalità (ordine) dei suoi sottogruppi è vincolata dal seguente Teorema di Lagrange:

ESERCIZIO 19. *Dati un gruppo G finito e un suo sottogruppo H, dimostrare che l'ordine $|H|$ di H divide l'ordine $|G|$ di G.*

Dimostrazione. Dal problema precedente ricaviamo che Ha sono le classi di equivalenza della relazione $\sim_H$. Da questo fatto ricaviamo che:

$$G = \bigcup_a Ha$$

dove Ha sono le classi di equivalenza disgiunte e a corre sui rappresentanti della classe. Ma quanti elementi ha la classe Ha? Osserviamo che il laterale destro è composto dagli elementi $h_i a$ con $h_i \in H$ e con $i = 1, \ldots, |H|$. Questi sono distinti dato che, per la legge di cancellazione, se $h_i a = h_j a$, allora $h_i = h_j$. Da questo ricaviamo che $|Ha| = |H|$ per ogni elemento a rappresentante della classe. Dato che i laterali Ha sono disgiunti per rappresentanti diversi, allora:

$$|G| = \sum_a |Ha| = i_H |H|$$

dove i_H è un intero positivo, detto l'indice del laterale e rappresenta il numero delle classi di $\sim_H$. Da questo ricaviamo che la cardinalità di H divide quella di G.

□

Possiamo ora dimostrare il piccolo teorema di Lagrange:

ESERCIZIO 20. *Dimostrare che in un gruppo finito G per ogni $g \in G$ vale:*

$$g^{|G|} = e$$

Dimostrazione. Sappiamo, per la finitezza di G, che esiste un intero positivo n tale che $g^n = e$ e dunque dall'esercizio 13 si ha $g^{|<g>|} = e$. Essendo $< g >$ un sottogruppo, per il teorema precedente, la sua cardinalità divide quella di G:

$$|G| = i_{<g>}| < g > |$$

Quindi:

$$g^{|G|} = (g^{|<g>|})^{i_{<g>}} = e^{i_{<g>}} = e$$

□

ESERCIZIO 21. *Sia G un gruppo abeliano finito. Sia n un intero: $MCD(n, |G|) = 1$. Dimostrare che per ogni $g \in G$ esiste uno e un solo $x \in G$ tale che $x^n = g$.*

Dimostrazione. Consideriamo la funzione $\Phi : G \to G$ definita da $\Phi(x) = x^n$. Se dimostro che Φ è suriettiva, allora per ogni $g \in G$ esiste un $x \in G$ per cui vale $\Phi(x) = g$, cioè $x^n = g$. Sfrutto la finitezza di G, infatti, una funzione $f : G \to G$ su un insieme finito $|G|$ è suriettiva se e solo se è iniettiva. Dimostriamo, dunque, che Φ è iniettiva:

$$\Phi(x_1) = \Phi(x_2) \iff x_1^n = x_2^n$$

e, dato che siamo in gruppo abeliano:

$$x_1^n = x_2^n \iff e = x_1^n x_2^{-n} = (x_1 x_2^{-1})^n$$

Per 13, detto d il minimo intero positivo tale che $(x_1 x_2^{-1})^d = e$, si ha che $d|n$. Dato che vale anche $(x_1 x_2^{-1})^{|G|} = e$, allora d divide anche $|G|$. Dato che $MCD(n, |G|) = 1$, allora necessariamente $d = 1$ da cui:

$$x_1 x_2^{-1} = e$$

cioè: $x_1 = x_2$. Da questo concludiamo che Φ è iniettiva e, dunque, suriettiva e perciò per ogni $g \in G$ esiste uno e un solo $x \in G$ tale che $x^n = g$.

□

ESERCIZIO 22. *Dimostrare che un gruppo G di cardinalità p, con p numero primo, è necessariamente ciclico.*

Dimostrazione. Se $G = (e)$ allora è banalmente ciclico. Altrimenti esiste un $g \in G$ diverso dall'unità e.Considero il sottogruppo $< g >$ generato da g. Per il teorema di Lagrange $| < g > |$ divide p e quindi $| < g > | = p$ da cui $< g >= G$. □

1.1.6 Omomorfismi

ESERCIZIO 23 (*). *Siano G un gruppo e g un elemnto fissato in G. Posto $T_g(x) = g^{-1}xg$ per ogni $x \in G$, dimostrare che T_g è un omomorfismo su G. In particolare dimostrare che T_g è iniettiva e suriettiva, quindi è un automorfismosu G. Considerare la funzione $\psi : G \to \mathcal{A}(G)$ ($\mathcal{A}(G)$ è l'insieme degli automorfismi su G) definita ponendo $\psi(g) = T_g$ per ogni $g \in G$. Dimostrare che ψ è un omomorfismo, con quale nucleo?*

Dimostrazione. 1. T_g è un omomorfismo. Per ogni $a, b \in G$:

$$T_g(ab) = g^{-1}(ab)g = g^{-1}agg^{-1}bg = T_g(a)T_g(b)$$

2. T_g è iniettiva e suriettiva. Infatti siano $a, b \in G$, allora:

$$T_g(a) = T_g(b) \iff g^{-1}ag = g^{-1}bg \iff a = b$$

è suriettiva, dato che per ogni $y \in G$, considerando $x = gyg^{-1}$, si ha $T_g(x) = y$. Quindi T_g è un automorfismo.

3. Dimostriamo che ψ è un omomorfismo: ψ è ovviamente una funzione da G in $\mathcal{A}(G)$, inoltre $\psi(g_1g_2) = T_{g_1g_2}$ e $\psi(g_1) \circ \psi(g_2) = T_{g_1} \circ T_{g_2}$ Consideriamo:

$$T_{g_1g_2}(x) = (g_1g_2)^{-1}x(g_1g_2) = g_2^{-1}(g_1^{-1}xg_1)g_2 = g_2^{-1}(T_{g_1}(x))g_2 = T_{g_2}(T_{g_1}(x)) = (T_{g_1} \circ T_{g_2})(x)$$

Quindi:

$$\psi(g_1g_2) = \psi(g_1) \circ \psi(g_2)$$

4. Dimostriamo che il nucleo è il centro di G $Z(G)$. Sia g tale che $\psi(g) = I$ (I automorfismo identico), allora questo vuol dire che $T_g(x) = x$ per tutti gli x. Quindi $g^{-1}xg = x \ \forall x \in G$ che è la stessa cosa di $g \in Z(G)$. Abbiamo dimostrato così l'inclusione $ker(\psi) \subseteq Z(G)$. Viceversa, supponiamo $g \in Z(G)$, allora, dato che g commuta con tutti gli elementi di G:

$$T_g(x) = g^{-1}xg = g^{-1}gx = x, \ \ \forall x \in G$$

e, quindi, $g \in Ker(\psi)$. Questa inclusione insieme alla precedente dimostra che $Ker(\psi) = Z(G)$

□

Questo esercizio dimostra che l'insieme degli automorfismi del tipo $T_g(x) = gxg^{-1}$, detti automorfismi interni e indicato con $\mathcal{I}(G)$, è isomorfo a $G|_{Z(G)}$.

1.1.7 Anelli

ESERCIZIO 24. *Si consideri l'insieme P delle matrici quadrate di ordine 2 della forma:*

$$\begin{pmatrix} a & 2h \\ 0 & a \end{pmatrix}$$

con $a, h \in \mathbb{Z}$. Dimostrare che P è un anello rispetto alle solite operazioni di somma e prodotto di matrici.

Dimostrazione. Consideriamo due elementi di P:

$$H_1 = \begin{pmatrix} a & 2h_1 \\ 0 & a \end{pmatrix}, \quad H_2 = \begin{pmatrix} b & 2h_2 \\ 0 & b \end{pmatrix}$$

si verifica immediatamente che $H_1 + H_2 \in P$ e che $+$ è un'operazione commutativa, quindi $(P, +)$ è un gruppo abeliano. L'operazione di prodotto è interna all'insieme P, infatti:

$$H_1 H_2 = \begin{pmatrix} ab & 2(ah_2 + bh_1) \\ 0 & ab \end{pmatrix}$$

quindi, $(P, \cdot)$ è un monoide di unità I. Affinchè sia un anello, però, dobbiamo verificare che $\cdot$ sia distributivo ripetto alla somma, ma questo è vero dato che l'usuale operazione di prodotto fra matrice è distributivo rispetto alla somma. □

ESERCIZIO 25. *Dimostrare che un elemento a dell'anello $\mathbb{Z}_n$ non è divisore dello zero se e solo se $MCD(a, n) = 1$. Dimostrare, inoltre, che un elemento $a \in \mathbb{Z}_n$, con $a \neq 0$ è invertibile secondo l'operazione di prodotto $\cdot$ se e solo se $MCD(a, n) = 1$.*

Dimostrazione. Sia $a \in \mathbb{Z}_n$ con $MCD(a, n) = 1$ e $[a]_n \neq [0]_n$. Da:

$$[a]_n \cdot [c]_n = [0]_n$$

si ottiene che $n|ac$; ma dato che $MCD(a, n) = 1$, allora necessariamente $n|c$, cioè:

$$[c]_n = [0]_n$$

Con questo abbiamo dimostrato che se $MCD(a, n) = 1$, allora a non è divisore dello zero. Viceversa dimostriamo che se $MCD(a, n) > 1$, allora a è divisore dello zero. Sia $d = MCD(a, n)$, con $d > 1$, considero $c = \frac{n}{d}$, allora (dato che $d > 1$) $[c]_n \neq [0]_n$ (altrimenti sarebbe $n|c$). Inoltre $n|ac$ dato che $ac = \frac{an}{d}$ e $d|a$. Da questo fatto:

$$[a]_n[c]_n = [ac]_n = [0]_n$$

e quindi a è divisore dello zero.

Osserviamo che tutti gli elementi diversi da zero che ammettono inverso formano un gruppo moltiplicativo in $\mathbb{Z}_n$. Se a è invertibile, allora $[a]_n[a^{-1}]_n = [0]_n$ equivalente ad $aa^{-1} = 1 + kn$, quindi, se $MCD(n, a) = d > 1$, allora, dato che $d|a$ e $d|n$, ricaverei l'assurdo $d|1$. Quindi se a è invertibile, allora $MCD(a, n) = 1$. Viceversa, per l'esercizio 5, gli elementi diversi da zero con $MCD(a, n) = 1$ formano un gruppo e, quindi, sono invertibili.

□

ESERCIZIO 26. *Trovare in $\mathbb{Z}_7$ la soluzione dell'equazione $[3]_7x+[1]_7 = [0]_7$ e dimostrare che è unica. Discutere esistenza ed unicità della soluzione della stessa equazione in $\mathbb{Z}_6$. Dire anche per quali valori di a l'equazione:*

$$[a]_6x + [b]_6 = [0]_6$$

ha in $\mathbb{Z}_6$ una ed una sola soluzione.

Dimostrazione. Sfruttando il fatto che $(\mathbb{Z}_n, +, \cdot)$ è un anello, l'equazione $[3]_7x + [1]_7 = [0]_7$ è equivalente a: $[3]_7x = [-1]_7 = [6]_7$. Dato che $\mathbb{Z}_7$ è un gruppo (7 è primo), allora questo è equivalente a dire che l'equazione $a \cdot x = b$ ammette una ed una sola soluzione, quindi, $[3]_7x = [-1]_7 = [6]_7$ ammette una ed una sola soluzione $x = [3]_7^{-1}[6]_7$. In $\mathbb{Z}_6$ l'equazione $[3]_6x + [1]_6 = [0]_6$ è equivalente a: $[3]_6x = [-1]_6 = [5]_6$. Ma:

$$[3]_6[1]_6 = [3]_6;\ [3]_6[12]_6 = [0]_6;\ [3]_6[3]_6 = [3]_6\ \ [3]_6[4]_6 = [0]_6\ [3]_6[5]_6 = [3]_6$$

e, quindi, non ammette soluzione. Potevamo arrivare alla stessa conclusione notando che la precedente equazione equivale a trovare un intero x per cui valga:

$$(3 + k6)x = (5 + t6)$$

con $k, t \in \mathbb{Z}$. Questo implicherebbe che $3|5$ assurdo. Passiamo al caso generale. Nel caso di $[a]_n = [1]_n, [5]_n$ la soluzione esiste sempre dato che sono invertibili (esercizio precedente). In questo caso la soluzione è data da: $x = [a]_6^{-1}[b]_6$, inoltre è unica, infatti, se esistessero x_1, x_2 che soddisfano a $[a]_6x + [b]_6 = [0]_6$, allora:

$$[a]_6x_1 = [a]_6x_2$$

e, per l'invertibilità di $[a]_6$, questo implica $x_1 = x_2$. Rimangono i casi $a = [0]_6, [2]_6, [3]_6, [4]_6$. Il caso $a = [0]_6$ è compatibile solo con $b = [0]_6$ e la soluzione non è unica (x può essere qualsiasi elemento di $\mathbb{Z}_6$). Per gli altri casi, otteniamo:

		x				
		$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
a	$[2]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
	$[3]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
	$[4]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$

□