Corso di Laurea in Matematica

Esercizi per il corso di Algebra II
Teoria dei Gruppi

Per gli esercizi contrassegnati da una stella (★), la soluzione, o almeno una risposta, si trova in fondo.

1 Operazioni, semigruppi e monoidi.

Esercizio 1 ★ Sia A un insieme non vuoto, e si consideri il monoide $(P(A), \cup)$. Sia $\emptyset \neq B \subseteq A$ e sia $P_B = \{ X \mid B \subseteq X \subseteq A \}$. Si provi che P_B è un sottoinsieme chiuso di $P(A)$; é P_B un sottomonoide del monoide $(P(A), \cup)$? Si dica se $(P_B, \cup)$ è un monoide.

Esercizio 2 ★ Sia $(M, \cdot)$ un monoide e si fissi un elemento $m \in M$. Su M si consideri l'operazione $\#$ definita ponendo, per ogni $a, b \in M$: $a\#b = a \cdot m \cdot b$. Si provi che $(M, \#)$ é un semigruppo e si dica per quali condizioni su m, $(M, \#)$ è un monoide.

Esercizio 3 ★ Sia $(M, \cdot)$ un monoide e si fissi un elemento $a \in M$. Si dica (motivando adeguatamente le risposte) quali tra i seguenti sottoinsiemi di M sono sottomonoidi:

(i) $C(\mathrm{a}) = \{\mathrm{x} | \mathrm{x} \in M \text{ e } \mathrm{xa} = \mathrm{ax}\}$;

(ii) $D(\mathrm{a}) = \{\mathrm{x} | \mathrm{x} \in M \text{ e } \mathrm{xax} = \mathrm{a}\}$

(iii) $I(\mathrm{a}) = \{\mathrm{x} | \mathrm{x} \in M \text{ e xa è invertibile }\}$.

Esercizio 4 ★ Sia L un alfabeto con almeno due simboli distinti, e sia X l'insieme di tutte le terne ordinate di elementi di L. Su X sia definita l'operazione $\#$ ponendo, per ogni $\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{x}', \mathrm{y}', \mathrm{z}' \in L$:

$$\mathrm{xyz} \# \mathrm{x'y'z'} = \mathrm{xy'z}$$

(a) Si dimostri che $(X, \#)$ è un semigruppo. E' commutativo?

(b) Dati elementi distinti x e y di L, si dica, motivando la risposta, se l'elemento xxy appartiene oppure no al sottosemigruppo generato dagli elementi xyx e yxx.

(c) Si dica se $(X, \#)$ è un monoide, determinandone in caso affermativo l'identità.

Esercizio 5 ★ Sia $(S, \cdot)$ un semigruppo che gode della seguente proprietá: per ogni $x, y \in S$: $xyx = y$. Si dimostri che S è un gruppo commutativo tale che $x^2 = 1$ per ogni $x \in S$.

Esercizio 6 ★ Sia $(S, \cdot)$ un semigruppo e si supponga che esista $b \in S$ tale che $bab = a$ per ogni $a \in S$. Si provi che $ab = ba$ per ogni $a \in S$. Si dimostri quindi che S è un monoide. [Sugg.: si cominci con l'osservare che $b^3 = b$].

Esercizio 7 ★ Sull'insieme $\mathbb{Q}^2 = \{ (x, y) \mid x, y \in \mathbb{Q} \}$ si definisca l'operazione $*$ ponendo, per ogni:

$$(\mathrm{a}, \mathrm{b}), (\mathrm{a}_1, \mathrm{b}_1) \in \mathbb{Q}^2 \ , \ (\mathrm{a}, \mathrm{b}) * (\mathrm{a}_1, \mathrm{b}_1) = (\mathrm{aa}_1, \mathrm{ab}_1 + \mathrm{b}).$$

Si dica se tale operazione è associativa e se esiste un elemento identico in $\mathbb{Q}^2$. Per ogni $b \in \mathbb{Q}$ e ogni $n \in \mathbb{N}$ si determini, procedendo per induzione su n, la potenza $(1, b)^n$.

Esercizio 8 ★ Sull'insieme $\mathbb{Z}$ dei numeri interi si definisca l'operazione $*$ ponendo, per ogni $n, m \in \mathbb{Z}$: $n * m = n + m - nm$. Si dimostri che $(\mathbb{Z}, *)$ è un monoide e si determinino gli elementi invertibili.

Esercizio 9 ★ Si consideri il semigruppo $(\mathbb{Z}, +)$. Motivando le risposte, si dica quali fra le seguenti affermazioni sono vere.

(a) -6 appartiene al sottosemigruppo generato da 3.

(b) L'insieme $T = \{x \in \mathbb{Z} \mid x \geq 0$ e $x = 2a - 3b$ con $a, b \in \mathbb{N} \}$ è un sottosemigruppo di $(\mathbb{Z}, +)$.

(c) Il sottosemigruppo generato da $\{3, -2\}$ è tutto $\mathbb{Z}$.

(d) Siano $\mathrm{a}, \mathrm{b} \in \mathbb{Z}$, e siano [a] e [b] i sottomonoidi generati, rispettivamente, da a e b; allora $[\mathrm{a}] \cap [\mathrm{b}] = \{0\}$ se e solo se $\mathrm{ab} \leq 0$.

Esercizio 10 Sia $(M, \cdot)$ un monoide e sia $\sigma : M \to M$ una applicazione biettiva. Sull'insieme M si definisca quindi una operazione $*$ ponendo, per ogni $a, b \in M$,

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

(a) Si provi che $(M, *)$ è un monoide.

(b) Si provi che σ è un isomorfismo di monoidi $\sigma : (M, *) \to (M, \cdot)$.

(c) Si definisca una operazione $\#$ su $\mathbb{Z}$, tale che $(\mathbb{Z}, \#)$ sia un gruppo con identità -2.

2 Gruppi.

Esercizio 11 Sia G un gruppo. Si dimostri che per ogni coppia di elementi $a, b \in G$ esiste uno e un solo $x \in G$ tale che $ax = b$.

Esercizio 12 Per ogni coppia (a, b) di numeri reali con $a \neq 0$ sia $\sigma_{a,b} : \mathbb{R} \to \mathbb{R}$, la applicazione definita da $\sigma_{a,b}(x) = ax+b$ per ogni $x \in \mathbb{R}$. Sia $G = \{\sigma_{a,b} \mid a, b \in \mathbb{R}\ a \neq 0\}$. Si dimostri che G dotato della operazione di composizione di applicazioni è un gruppo e si verifichi che il sottoinsieme $T = \{\ \sigma_{1,b} \mid b \in \mathbb{R}\ \}$ è un suo sottogruppo.

Esercizio 13 Sia G un gruppo abeliano e sia $n \in \mathbb{N}$. Si provi che l'insieme

$$G[n] = \{\ g \in G \mid\ g^n = 1\ \}$$

è un sottogruppo di G. Si mostri con un esempio che tale proprietà è in generale falsa se G non è abeliano.

Esercizio 14 Sia $\sim$ la relazione sull'insieme dei numeri interi $\mathbb{Z}$ definita da, per ogni $x, y \in \mathbb{Z}$:

$$x \sim y \quad \text{se} \quad \frac{x-y}{2} \in \mathbb{Z} \quad \text{e} \quad 3 \text{ divide } \frac{x-y}{2}.$$

(a) Si provi che $\sim$ è una relazione di equivalenza.

(b) ★ Si dica se esiste un sottogruppo H di $\mathbb{Z}$ tale che $\mathbb{Z}/\sim = \mathbb{Z}/H$, e in caso affermativo, si determini H.

Esercizio 15 ★ Un gruppo G si dice *privo di torsione* se vale la proprietà:
- per ogni $x \in G$ e ogni $n \in \mathbb{N} \setminus \{0\}$ se $x^n = 1$ allora $x = 1$.

Si provi che se G è un gruppo privo di torsione, $1 \neq x \in G$ e $n, m \in \mathbb{N}$, allora $x^n = x^m$ se e solo se $n = m$.

Esercizio 16 ★ Sia G un gruppo finito di ordine pari. Si provi che esiste $1 \neq x \in G$ tale che $x = x^{-1}$.

Esercizio 17 Sia $(G, \cdot)$ un gruppo e $g \in G$.

(a) Si provi che se $x \in G$ è tale che $xg = gx$, allora $x^{-1}g = gx^{-1}$.

(b) Sia $C = \{\ x \in G \mid xg = gx\ \}$; si provi che C è un sottogruppo di G.

(c) ★ Sia $D = \{\ x \in G \mid xg = g^{-1}x\ \}$. Si dimostri che $D = \emptyset$ oppure D è una classe laterale modulo C, e che $C \cup D$ è un sottogruppo di G.

Esercizio 18 ★ Siano H e K sottogruppi del gruppo G e $x, y \in G$.

(a) Si provi che se $Hx = Ky$ allora $H = K$.

(b) Sia $G = S_4, H = <(1\ 2\ 3)>$ e $x =(1\ 2)(3\ 4)$. Si determini Hx, quindi si trovi un sottogruppo K di G tale che $K \neq H$ e $Hx = xK$.

Esercizio 19 Nel gruppo $G = Sym(\mathbb{Z})$ delle permutazioni di $\mathbb{Z}$ si considerino gli elementi α, β definiti da, per ogni $x \in \mathbb{Z}$

$$\alpha(x) = -x \ , \qquad \beta(x) = -x + 1 \ .$$

(a) Si provi che $|\alpha| = |\beta| = 2$.

(b) Procedendo per induzione, si provi che per ogni $n \in \mathbb{N}$, si ha $(\alpha\beta)^n(0) = -n$. Dedurre che $|\alpha\beta| = \infty$.

(c) Posto $\gamma = \alpha\beta$, provare che, per ogni $z \in \mathbb{Z}$ si ha $(\gamma^z)^\alpha = \gamma^{-z}$.

(d) Si provi che $\langle\gamma\rangle\langle\alpha\rangle$ è un sottogruppo di G.

Esercizio 20 Sia G un gruppo **commutativo**. Su G si definisca una relazione $\sim$ ponendo, per ogni $x, y \in G$; $x \sim y$ se $(xy^{-1})^2 = 1$.

(a) Si provi che $\sim$ è una equivalenza.

(b) Si provi che $[1_G]_\sim$ è un sottogruppo di G

(c) Assumendo che $[1_G]_\sim = \{1_G\}$, si determini $[x]_\sim$ per ogni $x \in G$.

Esercizio 21 Sull'insieme $G = \mathbb{N}^\mathbb{N} = \{ \ f \mid f : \mathbb{N} \to \mathbb{N}$ applicazione $\}$ definiamo una operazione $+$, ponendo, per ogni $f, g \in G$, ed ogni $n \in \mathbb{N}$,

$$(f + g)(n) = f(n) + g(n) \ .$$

(a) Si provi che $(G, +)$ è un gruppo commutativo.

(b) Si provi che $H = \{f \in G \mid f(n)$ è pari, per ogni $n \in \mathbb{N}\}$ è un sottogruppo di G.

(c) Si provi che H è isomorfo a G. [sugg.: si consideri l'applicazione $\alpha : H \to G$ definita ponendo $\alpha(f)(n) = \frac{f(n)}{2}$, per $f \in H, \ n \in \mathbb{N}$.]

3 Gruppi ciclici.

Esercizio 22 Sia G un gruppo ciclico di ordine 24, e sia g un generatore di G.

(a) Scrivere gli elementi del sottogruppo d'ordine 8 di G come potenze di g.

(b) Si scrivano tutti i sottogruppi di G.

Esercizio 23 ★ Sia G un gruppo di ordine 56 e sia $g \in G$. E' vero che se $g^{15} = 1_G$ allora $g = 1_G$?

Esercizio 24 ★ Si dimostri che se G è un gruppo ciclico e $H \leq G$, il gruppo quoziente G/H è ciclico.

Esercizio 25 Sia $(G, \cdot)$ un gruppo. Per ogni $g \in G$, si denoti con $|g|$ l'ordine di g. Si dimostri che, per ogni $x, y \in G$: $|xy| = |yx|$ [Si osservi che $(xy)^n = x(yx)^{n-1}y = x(yx)^n x^{-1}$ ....]

Esercizio 26 Sia $D = \mathbb{R} \setminus \{0, 1\}$, e siano $f,\ g : D \to D$ le applicazioni definite da, per ogni $x \in D$,

$$f(x) = \frac{1}{x} \quad , \quad g(x) = \frac{x-1}{x}.$$

(a) Si provi che f, g sono biezioni, e si calcoli g^{-1}.

(b) Si determinino gli ordini di f e di g nel gruppo $Sym(D)$ di tutte le permutazioni di D.

Esercizio 27 ★ Sia G un gruppo di ordine p^2 dove p è un numero primo. Provare che G contiene al più $p + 3$ sottogruppi.

Esercizio 28 ★ Si consideri l'applicazione:

$$f \ : \ \mathbb{Z} \times \mathbb{Z} \ \to \ \mathbb{Z} \times \mathbb{Z}$$

$$(a, b) \ \to \ (b, b - a)$$

(a) Si dimostri che f è invertibile.

(b) Si dica qual'è l'ordine di f nel gruppo $Sym(\mathbb{Z}\times\mathbb{Z})$ (con l'operazione di composizione).

(c) Si dica se f è un automorfismo del gruppo additivo $\mathbb{Z} \times \mathbb{Z}$.

Esercizio 29 Sia G un gruppo, $g \in G$ e H un sottogruppo finito di G. Si provi che se $H \cap \langle g \rangle \neq \{1_G\}$, allora g ha ordine finito.

Esercizio 30 Sia $0 \neq \beta \in \mathbb{C}$, $D = \mathbb{C} \cup \infty$. e sia $f_\beta : D \to D$ definita da

$$f_\beta(x) = \frac{2x - \beta}{-\beta x - 2} \quad \text{se } x \neq -\frac{2}{\beta}, \infty$$

$f_\beta(-2/\beta) = \infty$, e $f_\beta(\infty) = 0$. Si dica per quali valori di β l'applicazione f_β ha ordine 3 nel gruppo Sym(D).

4 Sottoruppi normali.

Esercizio 31 ★ Sia G un gruppo e, per ogni $n \in \mathbb{N}$, sia H_n un sottogruppo di G con la proprietà che, per ogni $i, j \in \mathbb{N}$, se $i \leq j$ allora $H_i \leq H_j$. Si provi che $H = \bigcup_{n\in\mathbb{N}} H_n$ è un sottogruppo di G. Si provi quindi che se esiste $k \in \mathbb{N}$ tale che, per $n \geq k$, H_n è normale in G, allora H è normale.

Esercizio 32 Sia H un sottogruppo del gruppo G. Si dimostri che H è normale se e soltanto se per ogni $x, y \in G$ se $xy \in H$ allora $yx \in H$.

Esercizio 33 Sull'insieme $G = \mathbb{Q} \times \mathbb{Q}^*$ (dove $\mathbb{Q}^* = \{ x \mid x \in \mathbb{Q} \text{ e } x \neq 0 \}$) si definisca una operazione ponendo, per ogni $(x, y), (x_1, y_1) \in G$,

$$(x, y)(x_1, y_1) = (x + x_1 y, y y_1).$$

(a) Si dimostri che con tale operazione G è un gruppo.

(b) Si dica se G è commutativo.

(c) Si provi che l'insieme $N = \{ (x, 1) \in G \mid x \in \mathbb{Q} \}$ è un sottogruppo normale di G.

(d) Si provi che $D = \{ (x, x+1) \in G \mid x \in \mathbb{Q}\ x \neq -1 \}$ è un sottogruppo di G.

(e) Si provi che $G = ND$.

Esercizio 34 Sia $G = SL(2, \mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}\ , ad - bc = 1 \right\}$ il gruppo delle matrici quadrate invertibili di ordine 2 sugli interi; e sia

$$N = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid 3 \text{ divide } b \text{ e } c \right\}.$$

(a) Si provi che per ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$, si ha $3|a - d$.

(b) Si dimostri che N è un sottogruppo normale di G.

(c) ★ Sia $g = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix} \in G \setminus N$. Si calcoli l'ordine di g in G e l'ordine di gN in G/N.

Esercizio 35 Sia G un gruppo e sia N un suo sottogruppo normale. Sia $C_G(N) = \{g \in G \mid gx = xg \text{ per ogni } x \in N\}$. Si provi che $C_G(N) \trianglelefteq G$.

Esercizio 36 Sia p un numero primo, e sia N un sottogruppo normale del gruppo finito G, tale che p non divide $[G : N]$. Si provi che per ogni $x \in G$, se $|x| = p$ allora $x \in N$.

Esercizio 37 ★ Sia S un sottoinsieme del gruppo G tale che $g^{-1}sg \in S$ per ogni $s \in S$ ed ogni $g \in G$. Si provi che il sottogruppo $<S>$ generato da S è normale in G.

Esercizio 38 ★ Sia G un gruppo. (a) Siano N e M sottogruppi normali di G tali che G/M e G/N sono abeliani. Si provi che $G/(M \cap N)$ è abeliano.

(b) Siano $H \leq G$, e N normale in G. Si provi che se G/N è abeliano allora $H/(H \cap N)$ è abeliano.

Esercizio 39 Sia G un gruppo. Per ogni $x, y \in G$ scriviamo $[x, y] = x^{-1}y^{-1}xy$, e poniamo $[G] = \{ [x, y] \mid x, y \in G \}$. Si provi che se H è sottogruppo di G e $[G] \subseteq H$, allora Hè normale in G.

5 Omomorfismi e isomorfismi

Esercizio 40 Sia $(G, \cdot)$ un gruppo, e sia $g \in G$ un elemento fissato di G. Sull'insieme G definiamo una nuova operazione $*$ ponendo, per ogni $x, y \in G$,

$$x * y = y \cdot g^{-1} \cdot x \ .$$

(a) Si provi che $(G, *)$ è un gruppo.

(b) Si provi che $(G, *)$ è isomorfo a $(G, \cdot)$.

Esercizio 41 ★ Siano ψ e ζ due omomorfismi del gruppo G nel gruppo G'. Si dimostri che l'insieme $\{\ g \in G \mid \psi(g) = \zeta(g)\ \}$ è un sottogruppo di G. Si provi quindi che se S è un sistema di generatori di G e $\psi(s) = \zeta(s)$ per ogni $s \in S$, allora $\psi = \zeta$.

Esercizio 42 Sia

$$G = \left\{ \begin{pmatrix} x & 0 & y \\ a & x & a \\ 0 & 0 & x-y \end{pmatrix} \mid a, x, y \in \mathbb{R}\ ,\ 0 \neq x \neq y \right\}.$$

(a) Si provi che $G \leq GL_3(\mathbb{R})$.

(b) Si provi che la applicazione $\phi : G \to \mathbb{R}^*$, definita da:

$$\phi \begin{pmatrix} x & 0 & y \\ a & x & a \\ 0 & 0 & x-y \end{pmatrix} = x$$

è un omomorfismo del gruppo G nel gruppo moltiplicativo dei numeri reali non nulli, e si determini il nucleo $Ker(\phi)$.

Esercizio 43 ★ Siano G e H gruppi finiti tali che $(|G|, |H|) = 2$. Si dimostri che se esiste un omomorfismo $\phi : G \to H$ tale che $Ker(\phi) \neq G$ allora G ha un sottogruppo di indice 2.

Esercizio 44 ★ Si dimostri che i seguenti gruppi sono a due a due non isomorfi :

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}\ ; \quad \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}\ ; \quad \frac{\mathbb{Z}}{8\mathbb{Z}}.$$

Esercizio 45 Siano $\mathbb{C}^*$ e $\mathbb{R}^*$ il gruppo moltiplicativo, rispettivamente, dei numeri complessi diversi da zero e quello dei reali diversi da zero. Fissato un intero positivo dispari n, si ponga $D_n = \{\ z \in \mathbb{C}^* \mid z^n \in \mathbb{R}\ \}$.

(a) Si provi che D_n è un sottogruppo di $\mathbb{C}^*$.

(b) Sia $\eta : D_n \to \mathbb{R}^*$ l'applicazione definita da, per ogni $z \in D_n$, $\eta(z) = z^n$. Si dimostri che η è un omomorfismo suriettivo di gruppi e si determini $Ker(\eta) \cap \mathbb{R}^*$ e $|Ker(\eta)|$.

Esercizio 46 ★ Sia $\psi : G \to G$ un endomorfismo del gruppo G tale che $\psi \circ \psi = \psi$. Si provi che:

$$G = \psi(G)\mathrm{Ker}(\psi) \quad \text{e} \quad \psi(G) \cap \mathrm{Ker}(\psi) = \{1\}.$$

Esercizio 47 Sia G un gruppo di ordine 45. Si provi che se esiste un omomorfismo ϕ non nullo (cioè tale che $Ker(\phi) \neq G$), $\phi : G \to \mathbb{Z}/35\mathbb{Z}$ allora G ha un sottogruppo di ordine 9.

Esercizio 48 ★ Sia $G = \{ \frac{m}{n} \in \mathbb{Q} \mid (m,n) = 1 \text{ e } n \text{ divide } 12 \}$

(a) Si dimostri che G è un sottogruppo di $(\mathbb{Q}, +)$.

(b) Si calcoli l'ordine del gruppo quoziente $G/\mathbb{Z}$, e si provi che $G/\mathbb{Z}$ è un gruppo ciclico.

(c) Si calcoli l'ordine del gruppo quoziente $G/3\mathbb{Z}$.

Esercizio 49 ★ Sia $\mathbb{C}^*$ il gruppo moltiplicativo dei numeri complessi non nulli e sia

$$G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R},\ (a,b) \neq (0,0) \right\} .$$

a) Si provi che G è un sottogruppo del gruppo $GL(2,\mathbb{R})$ delle matrici quadrate invertibili di ordine 2 su $\mathbb{R}$.

b) Si provi che l'applicazione $\phi : \mathbb{C}^* \to G$ definita da, per ogni $z = a + bi \in \mathbb{C}^*$:

$$\phi(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

è un isomorfismo di gruppi.

c) Si determinino tutte le matrici $A \in G$ tali che $A^3 = 1$.

d) Dato l'elemento $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2,\mathbb{R})$, si provi che, per ogni $z \in \mathbb{C}^*$ si ha

$$\phi(\overline{z}) = (\phi(z))^C .$$

Esercizio 50 Siano G, H, K gruppi e siano $\alpha : G \longrightarrow H$, $\beta : G \longrightarrow K$ due omomorfismi tali che $Ker(\alpha) \cap Ker(\beta) = \{1_G\}$. Si provi che l'applicazione

$$\begin{array}{rccc} \phi : & G & \longrightarrow & H \times K \\ & x & \mapsto & (\alpha(x), \beta(x)) \end{array}$$

è un omomorfismo iniettivo.

Esercizio 51 Siano G e H gruppi, e siano $f, g : G \longrightarrow H$ due omomorfismi di gruppo. Sia $A = \{ x \in G \mid f(x) = g(x) \}$.

(a) Si provi che A è un sottogruppo di G.

(b) Si provi che se H è commutativo, allora A è un sottogruppo normale di G.

(c) Provare che se $Ker(f)A = G$, allora $f = g$.

(d) Provare che se $|G| = 36$, $|H| = 3$, e 9 divide $|A|$, allora $f = g$.

Esercizio 52 Sia $H = \mathbb{Z}_{15}$ il gruppo (additivo) delle classi di congruenza modulo 15, e sia $G = H \times H$.

(a) Si provi che l'applicazione $f : G \to H$ definita da $f((a, b)) = a+b$, per ogni $(a, b) \in G$, è un omomorfismo di gruppi..

(b) Posto $N = \ker(f)$, si determinino i sottogruppi del gruppo quoziente G/N.

6 Prodotti diretti.

Esercizio 53 ★ Sia $G = H \times K$ il gruppo prodotto diretto (interno) dei gruppi finiti H e K. Sia $S \leq G$ tale che $S \leq H$.

a) Si provi che $[G : S] = |K|[H : S]$.

b) Si provi che se $S \trianglelefteq H$ allora $S \trianglelefteq G$.

Esercizio 54 ★ Sia G un gruppo finito e siano H e K sottogruppi di G tali che $[G : H]$ e $[G : K]$ sono coprimi. Si provi che $HK = KH = G$. (Si ricordi la formula: $|HK| = \frac{|H||K|}{|H \cap K|}$).

Esercizio 55 ★ Dato un gruppo G, sia $W = G \times G$ e $D = \{ (g, g) \in W \mid g \in G \}$.

(a) Si provi che D è un sottogruppo di W isomorfo a G.

(b) Si dimostri che D è normale in W se e solo se G è abeliano.

Esercizio 56 (a) Sia $f : G \to G'$ un omomorfismo suriettivo di gruppi e sia N sottogruppo normale di G. Si dimostri che $f(N)$ è un sottogruppo normale di G'.

(b) Siano A, B gruppi e sia $A \times B$ il gruppo prodotto diretto.
Si consideri la applicazione $\pi : A \times B \to A$ definita da, per ogni $(a, b) \in A \times B$, $\pi(a, b) = a$. Sia N un sottogruppo normale di $A \times B$, si provi che $\pi(N)$ è un sottogruppo normale di A.

7 Permutazioni.

Esercizio 57 ★ Si consideri la permutazione di $\{1, 2, ..., 7\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

(a) Si scriva σ come prodotto di cicli disgiunti e si dica quale è la sua classe.

(b) Si provi che non esiste alcuna trasposizione τ di $\{1, 2, ..., 7\}$ tale che $\sigma\tau = \tau\sigma$.

Esercizio 58 ★ Si consideri la permutazione su $\{1, 2, ..., 8\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 4 & 3 & 1 & 6 & 2 & 7 \end{pmatrix}.$$

(a) si scriva σ come prodotto di cicli disgiunti e si determini la classe di σ.

(b) Si determini il periodo di σ e l'ordine del suo centralizzante in S_8.

Esercizio 59 Nel gruppo simmetrico S_7 si consideri l'elemento

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 5 & 2 & 4 & 1 \end{pmatrix}$$

(a) Scrivere σ come prodotto di cilci disgiunti e dire se $\sigma \in A_7$.

(b) Si trovi una trasposizione $(i\, j)$ tale che $A_7\sigma = A_7(i\, j)$.

(c) Posto $H = \langle\sigma\rangle$, dire se esiste un omomorfismo non banale $H \longrightarrow \mathbb{Z}_7$.

Esercizio 60 ★ Si consideri la permutazione di $\{1, 2, ..., 8\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 6 & 5 & 3 & 8 & 2 \end{pmatrix}.$$

(a) si scriva σ come prodotto di cicli disgiunti e si determini la sua classe.

(b) Nel gruppo S_8 di tutte le permutazioni dell'insieme $\{1, 2, ..., 8\}$ si trovi una permutazione τ tale che

$$\tau^2(16)\sigma = \sigma\tau.$$

Esercizio 61 Si consideri la permutazione di $\{1, 2, \ldots, 6\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix}.$$

(a) ★ si scriva σ come prodotto di cicli disgiunti.

(b) ★ si dica quanti elementi contiene il sottogruppo $< \sigma >$ di S_6.

Sia quindi $\tau \in S_6$ tale che $\tau\sigma = \sigma\tau$.

(c) si provi che $\tau(5) = 5$ e $\tau(\{1,4\}) = \{1,4\}$.

(d) si provi che $\tau = \sigma^i$ per qualche intero positivo i.

Esercizio 62 ★ Si considerino le seguenti permutazioni sull'insieme $\{1,2,\ldots,6\}$, $\alpha = (1234)$, $\beta = (1524)$.

(a) Si determini l'ordine della permutazione $\alpha\beta$.

(b) Sia $H =< \alpha, \beta >$ il sottogruppo generato da α e β nel gruppo S_6 ; si determinino le orbite di H nella sua azione su $\{1,2,3,4,5,6\}$.

(c) Si dica, giustificando la risposta, per quali fra i seguenti interi n esistono due cicli ρ, σ di lunghezza 4 in S_6 tali che il prodotto $\rho\sigma$ ha ordine $n = 1,\ 2,\ 3,\ 5,\ 7$.

Esercizio 63 Sia $G = S_4$ il gruppo simmetrico su $\{1,2,3,4\}$.

(a) Si provi che non esiste alcun omomorfismo suriettivo di G in $\mathbb{Z}/3\mathbb{Z}$.

(b) Si definisca un omomorfismo suriettivo di G in $\mathbb{Z}/2\mathbb{Z}$.

Esercizio 64 ★ Si determini un sottogruppo normale proprio e non banale del gruppo alterno A_4.

Esercizio 65 ★ Si provi che il gruppo alterno A_4 non ha sottogruppi di ordine 6.

Esercizio 66 ★ Individuare il più piccolo n tale che $\mathbb{Z}_2 \times \mathbb{Z}_2$ si immerge in S_n.

Esercizio 67 Sia $I = \{1,2,3,4,5,6,7,8\}$, e sia $G = S_8 = Sym(I)$ il gruppo simmetrico su I.

(a) Sia $\emptyset \neq Y \subseteq I$; si provi che $G_Y = \{\sigma \in G \mid \sigma(Y) \subseteq Y\}$ è un sottogruppo di G.

(b) Posto $A = \{1,2,3,4,5\}$, e $B = \{6,7,8\}$, si provi che $G_A = G_B$. Per ogni $\sigma \in G_A$ siano quindi $\sigma_{|A}$ la restrizione di σ a A, e $\sigma_{|B}$ la restrizione di σ a B. Si provi che l'applicazione $\Phi_A : G_A \longrightarrow Sym(A)$, definita da, per ogni $\sigma \in G_A$,

$$\Phi_A(\sigma) = \sigma_{|A} \ ,$$

è omomorfismo suriettivo di gruppi. Similmente si definisca $\Phi_B : G_A \longrightarrow Sym(B)$, ponendo $\Phi_B(\sigma) = \sigma_{|B}$.

(c) Si provi che $G_A = \ker(\Phi_A) \times \ker(\Phi_B)$. Quindi si determnini $|G_A|$ e $[G : G_A]$.

(d) Posto $C = \{4,5,6,7,8\}$, è vero che G_A e G_C sono coniugati in G?

Esercizio 68 ★ Sia $G = S_n$ il gruppo simmetrico su $\{1, ..., n\}$ e si considerino i sottoinsiemi

$$H = \{\ \sigma \in G \mid \{\sigma(1), \sigma(2)\} = \{1, 2\}\ \} \qquad K = \{\ \sigma \in H \mid \sigma(1) = 1\ \}$$

Si dimostri che $H \leq G$ e che K è un sottogruppo normale di H.

Esercizio 69 ★ Sia $n \geq 1$ e sia S_n il gruppo simmetrico su $\{1, ..., n\}$. Sia T un sottoinsieme non vuoto di $\{1, ..., n\}$. Si provi che l'insieme H di tutte le permutazioni $\sigma \in S_n$ tali che $\sigma(T) = T$, é unsottogruppo di S_n. Sia quindi $K = \{\ \sigma \in S_n \mid \sigma(x) = x$ per ogni $x \in T\ \}$; si dimostri che K è un sottogruppo normale di H e che H/K è isomorfo a S_k, dove $k = |T|$.

Esercizio 70 Per ogni permutazione $f \in Sym(\mathbb{Z})$ poniamo $C_f = \{\ a \in \mathbb{Z} \mid f(a) = a\ \}$. Sia F l'insieme di tutte le permutazioni f di $\mathbb{N}$ tali che $\mathbb{Z} \setminus C_f$ è finito (eventualmente vuoto). Si provi che F è un sottogruppo normale di $Sym(\mathbb{Z})$.

Esercizio 71 Siano $X = \{1, 2, 3, 4, 5, 6\}$, $Y = \{1, 2, 3\}$, e $G = Sym(X)$.

(a) Si dica, motivando le risposte, quali fra i seguenti sottoinsiemi sono sottogruppi di G:

(i) $A = \{\sigma \in G \mid \sigma(Y) = Y\}$.

(ii) $B = \{\sigma \in G \mid \sigma(1) \in Y\}$.

(iii) $C = \{\sigma \in G \mid \sigma = \iota_X$ oppure $\sigma(Y) \cap Y = \emptyset\}$.

(b) Sia H un sottogruppo di G tale che $H \subseteq C$ (definito al punto (iii) di sopra). Si provi che H contiene al più due elementi.

8 Azioni e coniugio.

Esercizio 72 ★ Sia G un gruppo di ordine 2006, e sia data una azione di G su un insieme S con $|S| = 20$; si provi che G ha almeno 3 orbite su S. Si dica qual è il numero di orbite nel caso in cui G non abbia punti fissi.

Esercizio 73 Sia G un gruppo di ordine 15 che opera fedelmente su un insieme Ω, con $|\Omega| = 15$. Si provi che G è transitivo su Ω, oppure ha almeno un punto fisso.

Esercizio 74 Sia A un gruppo abeliano, e sia data un'azione fedele di A su un insieme Ω. Si provi che se tale azione è transitiva allora $A_x = \{1_G\}$ per ogni $x \in \Omega$; si concluda che (se Ω è finito) $|A| = |\Omega|$.

Esercizio 75 Sia data un'azione fedele del gruppo G sull'insieme Ω e sia A un sottogruppo abeliano di G. Si supponga inoltre che la restrizione ad A dell'azione di G su Ω sia transitiva. Si provi che, per ogni $x \in \Omega$, $G = AG_x$ e $A \cap G_x = \{1\}$.

Esercizio 76 Sia dta un'azione *transitiva* del gruppo G sull'insieme Ω e sia $N \trianglelefteq G$. Per ogni $x \in \Omega$ denotiamo con xN l'orbita di x mediante N, e indichiamo con Γ l'insieme di tutte le N-orbite su Ω.

(a) Si provi che ponendo, per ogni $xN \in \Gamma$ ed ogni $g \in G$,

$$(xN) \cdot g = (x \cdot g)N$$

si definisce un'azione di G su Γ.

(b) Si provi che l'azione di G su Γ definita al punto (a) è transitiva.

(c) Si provi che tutte le orbite di N su Ω hanno la stessa cardinalità.

Esercizio 77 Sia G un gruppo e sia $A = Aut(G)$ il gruppo dei suoi automorfismi. Allora, esiste un'azione naturale di A su $G^{\#} = G \setminus \{1\}$, data da, per ogni $1 \neq g \in G$ e ogni $\phi \in A$, $g \cdot \phi = \phi^{-1}(g)$.

(a) Sia G finito, e si supponga che l'azione di A su $G^{\#}$ definita sopra sia transitiva. Si provi che esiste un primo p tale che $|g| = p$ per ogni $1 \neq g \in G$. Si provi quindi che G è abeliano

[Sugg.: sia $|G| = n$, e si ponga $N = Inn(G)$; allora $N \trianglelefteq A$ e $|N|$ dividet n - si veda la fine del capitolo 3. Quindi se d è la lunghezza di un'orbita di N su $G^{\#}$ allora $d \mid n$. D'altra parte, per il punto (c) dell'esercizio 76, d divide $|G^{\#}| = n - 1$. Segue $d = 1$, e dunque ...]

(c) Sia p un primo. Si provi che, posto $G = C_p \times C_p$, allora $Aut(G)$ opera transitivamente su $G^{\#}$.

Esercizio 78 Un'azione di un gruppo G su un insieme Ω si dice *2-transitiva* se, per ogni $x_1,\ x_2,\ y_1,\ y_2 \in \Omega$ con $x_1 \neq x_2$, $y_1 \neq y_2$, esiste $g \in G$ tale che

$$\begin{cases} x_1 \cdot g = y_1 \\ x_2 \cdot g = y_2. \end{cases}$$

(a) Sia $n \geq 2$. Si provi che l'azione naturale di S_n su $\{1, \ldots, n\}$ è 2-transitiva.

(b) ★ Sia data un'azione transitiva di G su Ω, e sia $x \in \Omega$. Si provi che tale azione è 2-transitiva se e solo se l'azione di G_x su $\Omega \setminus \{x\}$ è transitiva.

(c) Si deduca dal punto (b) che se il gruppo G ammette un'azione 2-transitiva su un insieme Ω con $|\Omega| = n$, allora $n(n-1) \mid |G|$.

Esercizio 79 Si Ω l'insieme di tutte le rette del piano $\mathbb{R} \times \mathbb{R}$ passanti per l'origine, e sia $G = GL(2, \mathbb{R})$ il gruppo di tutte le applicazioni lineari invertibili di $\mathbb{R} \times \mathbb{R}$. Per ogni $r \in \Omega$ ed ogni $g \in G$ si ponga $r \cdot g = g^{-1}(r)$. Si provi che in questo modo si definisce un'azione di G su Ω e che tale azione è 2-transitiva. Si dica se è fedele.

Esercizio 80 Sia G il gruppo delle matrici quadrate invertibili di ordine 2 a coefficienti reali (con l'usuale prodotto righe per colonne). Sia

$$H = \left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \ | a, c \in \mathbb{R}\ , c \neq 0 \right\}$$

(a) Si provi che H è un sottogruppo di G, e si stabilisca se è normale.

(b) Si dimostri che H è il centralizzante in G dell'elemento $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Esercizio 81 Sia $\mathbb{C}^*$ il gruppo moltiplicativo dei numeri complessi diversi da zero, e per ogni numero naturale $n \geq 1$, sia $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ l'insieme delle radici n-esime dell'unità.

(a) Si provi che per ogni n, U_n è un sottogruppo di $\mathbb{C}^*$.

(b) ★ Si dimostri che, per ogni $n,\ m:\ U_n \leq U_m$ se e solo se $n|m$; in tal caso si determini l'indice $[U_m\ :\ U_n]$.

(c) ★ Si dimostri che per ogni n, il gruppo quoziente $\mathbb{C}^*/U_n$ è isomorfo a $\mathbb{C}^*$.
(sugg.: si consideri la applicazione $f(x) = x^n$, di $\mathbb{C}^*$ in sé.

(d) ★ Posto

$$U = \{\ z \in \mathbb{C} \mid z^n = 1 \ \text{ per qualche } \ 0 \neq n \in \mathbb{N}\ \} = \bigcup_{n \in \mathbb{N}} U_n,$$

il sottogruppo di tutte le radici dell'unità, si dimostri che $\mathbb{C}^*/U$ non è isomorfo a $\mathbb{C}^*$.

Esercizio 82 ★ In un gruppo (infinito) G sia F l'insieme degli elementi che hanno un numero finito di coniugati distinti. Si dimostri che F è un sottogruppo normale di G.

Esercizio 83 ★ Sia G un gruppo finito, H un sottogruppo normale di G tale che $(|H|, |G : H|) = 1$. Si provi che se $K \leq G$ e $|K| = |H|$ allora $K = H$.

Esercizio 84 Si consideri il seguente insieme di matrici quadrate di ordine 3 a coefficienti interi:

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}.$$

(a) Si dimostri che, rispetto alla usuale moltiplicazione di matrici, G è un gruppo.

(b) Si determini il centro $Z(G)$ di G.

(c) Si provi che $G/Z(G)$ è abeliano.

Esercizio 85 Sia G un gruppo commutativo finito. Si provi che per ogni divisore d dell'ordine di G, G ha almeno un sottogruppo di ordine d.

Esercizio 86 ★ Sia G un p-gruppo finito (cioè $|G| = p^n$, con p un primo e $n \geq 0$). Si provi che per ogni $1 \leq k \leq n$ esiste un sottogruppo <u>normale</u> di G di ordine p^k.

Esercizio 87 ★ Si provi che il numero di classi di coniugio di un gruppo finito G è

$$\frac{1}{|G|}\sum_{x\in G}|C_G(x)|$$

Esercizio 88 Sia G un gruppo con $|G| = 30$, e si assuma che G ammetta un'azione fedele e transitiva su un insieme Ω, con $|\Omega| = 6$.

(a) Si provi che una tale azione è necessariamente 2-transitiva.

(b) Sia X l'insieme degli elementi di G che non fissano alcun punto di Ω; si provi che $|X| = 5$.

Esercizio 89 Sia $\mathbb{Z}_7$ il campo $\mathbb{Z}/7\mathbb{Z}$.

(1) Si provi che in $\mathbb{Z}_7$ l'elemento -1 non è un quadrato.

(2) Siano $a, b \in \mathbb{Z}_7$; si provi che $a^2 + b^2 = 0$ se e solo se $a = 0 = b$.

(3) Sia $G = \left\{ A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_7,\ DetA \neq 0 \right\}$.

Si provi che G è un gruppo e si determini il suo ordine.

(4) Sia $V = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbb{Z}_7 \right\}$, e si consideri l'azione di G su V data da

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ -bx + ay \end{pmatrix};$$

si provi che le orbite di tale azione sono

$$\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \qquad \text{e} \qquad V \setminus \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}.$$

9 Esercizi vari.

Esercizio 90 Sull'insieme $G = \mathbb{Q} \times \mathbb{Z}$ definiamo l'operazione

$$(x, z)(x', z') = (2^z x + x, z + z')$$

(per ogni $(x, z), (x', z') \in G$). Si provi che con tale operazione G è un gruppo.

(b) Sia $H = \{ (h, 0) \mid h \in \mathbb{Z} \}$, e sia $g = (0, 1)$.

Si provi che H è un sottogruppo di G, che $H^g \leq H$, ma che $H^g \neq H$ (si rammenta che $H^g = \{g^{-1}xg \mid x \in H\}$).

Esercizio 91 Ricordiamo che se G è un gruppo, il **centro** di G è il sottogruppo $Z(G) = \{g \in G \mid xg = gx \text{ per ogni } x \in G\}$. Sia ora G un gruppo fissato, $N \trianglelefteq G$ e definiamo

$$T(N) = \{\ g \in G \mid x^{-1}gxN = Ng \text{ per ogni } x \in G\ \}.$$

(a) Si provi che $T(N)$ è un sottogruppo normale di G che contiene N.

(b) Si provi che $T(N)/N = Z(G/N)$.

(c) Si provi che se $[G : N] = p$ con p un numero primo, allora $T(N) = G$.

Esercizio 92 Sia

$$\mathbb{Q}_2 = \left\{\ \frac{m}{2^i} \in \mathbb{Q} \mid m \in \mathbb{Z},\ i \in \mathbb{N}\right\}.$$

(a) Si provi che $\mathbb{Q}_2$ è un sottogruppo del gruppo $(\mathbb{Q}, +)$.

Sia quindi definita $\sigma : \mathbb{Q}_2 \longrightarrow \mathbb{Q}_2$, ponendo, per ogni $x \in \mathbb{Q}_2$, $\sigma(x) = 4x$.

(b) Si provi che σ è un automorfismo del gruppo $\mathbb{Q}_2$.

(c) Si provi che l'applicazione $\overline{\sigma} : \mathbb{Q}_2/\mathbb{Z} \longrightarrow \mathbb{Q}_2/\mathbb{Z}$, definita ponendo, per ogni $x \in \mathbb{Q}_2$, $\overline{\sigma}(x + \mathbb{Z}) = \sigma(x) + \mathbb{Z}$, è ben definita ed è un omomorfismo.

(d) Si dica se $\overline{\sigma}$ è un automorfismo.

Esercizio 93 Siano G un gruppo commutativo, $\mathbb{Z}$ il gruppo additivo degli interi, e

$$W = \mathbb{Z} \times G = \{\ (z, g) \mid z \in \mathbb{Z},\ g \in G\ \}$$

il loro prodotto diretto. Sia h un fissato elemento del centro di G (cioè h è tale che $hg = gh$ per ogni $g \in G$). Si consideri quindi l'applicazione $\phi : W \longrightarrow G$, definita da, per ogni $(z, g) \in W$, $\phi(z, g) = gh^z$.

(a) Si provi che ϕ è un omomorfismo suriettivo di gruppi.

(b) Sia $K = ker(\phi)$. Si provi che $|K| = \infty$.

(c) Si determini $\phi^{-1}(\langle h \rangle)$.

(d) Posto $G_1 = \{(0, g) \mid g \in G\}$, si provi che $W = G_1 \times K$.

Esercizio 94 Sia $G = GL(2, \mathbb{Q})$ il gruppo moltiplicativo delle matrici quadrate invertibili di ordine 2 sui razionali, e siano

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\} \qquad U = \left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \mid z \in \mathbb{Z} \right\}$$

a) Si provi che H è un sottogruppo di G.

b) Si provi che $U \leq H$, e che $U \simeq \mathbb{Z}$ (ovviamente $\mathbb{Z}$ è additivo).

c) Posto $x = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$, si provi che $x^{-1}Ux \leq U$, ma che $x \notin N_H(U)$.

Esercizio 95 Sia $G = GL(2, \mathbb{R})$ il gruppo moltiplicativo delle matrici invertibili di ordine 2 su $\mathbb{R}$. Sia

$$H \left\{ \left(\begin{array}{cc} a & 0 \\ c & a \end{array} \right) \Big| \; a, c \in \mathbb{R},\, a \neq o \right\}.$$

1) Si dimostri che H è un sottogruppo di G. Si dica quindi se H è normale, oppure no.

2) Sia $U = \left(\begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right)$. Si provi che $H = \{A \in G \mid AU = UA\}$.

3) Si determinino gli elementi di H di ordine finito.

Esercizio 96 Sia $G = \mathbb{Z} \times \mathbb{Z}$ il (gruppo) prodotto diretto di due copie del gruppo additivo degli interi, e sia $\phi : G \longrightarrow G$ definita da, per ogni $(a, b) \in G$, $\phi(a, b) = a - 3b$.

a) Si provi che ϕ è un omomorfismo di gruppi.

b) Si dica se ϕ è suriettiva e si determini $N = \ker(\phi)$.

c) Si provi che N e G/N sono entrambi gruppi ciclici.

b) Sia $M = \{(2z, z) \mid z \in \mathbb{Z}\}$. Si provi che $G = N \times M$.

Esercizio 97 Sia p un numero primo fissato, e sia

$$H = \{ \; \frac{z}{p} \mid z \in \mathbb{Z} \; \} \; .$$

(a) Si provi che H è un sottogruppo del gruppo additivo $(\mathbb{Q}, +)$.

(b) Si provi che

$$H/\mathbb{Z} = \left\{ \; \mathbb{Z},\; \frac{1}{p} + \mathbb{Z},\; \frac{2}{p} + \mathbb{Z}, \ldots,\; \frac{p-1}{p} + \mathbb{Z} \; \right\} \; .$$

(c) Si provi che H è isomorfo a $\mathbb{Z}$.

Esercizio 98 Sia $G = Sym(\mathbb{Z})$ il gruppo di tutte le permutazioni dell'insieme $\mathbb{Z}$. Sia $g : \mathbb{Z} \to \mathbb{Z}$, definita da, per ongi $z \in \mathbb{Z}$,

$$g(z) = \begin{cases} z - 1 & \text{se } \; 2 \not| z \\ z + 1 & \text{se } \; 2 | z \end{cases}$$

(a) Si provi che $g \in G$, e si determini il suo ordine come elemento del gruppo G.

(b) Sia $H = \{ \; f \in G \mid f(z) - z \in 2\mathbb{Z} \;$ per ogni $z \in \mathbb{Z} \; \}$. Si provi che H è un sottogruppo di G, e che $g \notin H$.

(c) Si provi che $H^g = H$.

Esercizio 99 Sull'insieme

$$G = \{ \; (a, b) \in \mathbb{Q} \times \mathbb{Q} \mid (a, b) \neq (0, 0) \}$$

definiamo l'operazione $\cdot$ ponendo $(a,b)\cdot(c,d) = (ac+2bd, ad+bc)$. Allora, $(G,\cdot)$ è un gruppo commutativo, con $1_G = (1,0)$ (non si chiede di verificare tali affermazioni).

(a) Siano $H = \{(2^z,0)|z \in \mathbb{Z}\}$ e $K = \{(0,2^z)|z \in \mathbb{Z}\}$. Si provi che $H \leq G$, che $H \cup K \leq G$, e si determini l'indice $[H \cup K : H]$.

(b) Si provi che G è isomorfo al gruppo moltiplicativo del campo $\mathbb{Q}[\sqrt{2}]$.

Esercizio 100 Sia G un gruppo di ordine 35.

(a) Si dica quali sono i possibili ordini dei sottogruppi di G.

(b) Si dimostri che se H, K sono sottogruppi propri allora $H \cap K = \{1\}$.

(c) Si provi che G ha uno ed un solo sottogruppo di ordine 7.

(d) Si provi che G ha almeno un sottogruppo di ordine 5.

[Se G non ha sottogruppi di ordine 7, allora G non è ciclico, e tutti gli elementi $g \neq 1$ generano un sottogruppo di ordine 5. Sia Γ l'insieme di tutti i sottogruppi di ordine 5 di G; allora $G = \bigcup_{H\in\Gamma} H$ e, poiché sottogruppi distinti propri di G hanno intersezione $\{1\}$, si ha $|G| = 1 + |\Gamma|(5-1)$, e quindi $4|\Gamma| = |G| - 1 = 34$, assurdo. Se poi $U, V \leq G$ hanno ordine 7, e $U \neq V$, allora $|UV| = ...$]

Esercizio 101 Si G un gruppo di ordine 77.

(a) Si provi che G ha un unico sottogruppo N di ordine 11.

(b) Si provi che N è normale in G.

(c) Si provi che se esiste un omomorfismo $\phi : G \to H$ dove H è un gruppo di ordine 33, e $\phi \neq 1$ (cioè esiste $x \in G$ tale che $\phi(x) \neq 1_H$), allora G è ciclico.

Risposte e soluzioni di alcuni esercizi.

1. Siano $X, Y \in P_B$, allora $B \subseteq X \subseteq X \cup Y$, cioè $X \cup Y \in P_B$. Dunque P_B è chiuso. Non è un **sottomonoide** del monoide $(\mathcal{P}(A), \cup)$ perchè non contiene l'elemento identico di $(\mathcal{P}(A), \cup)$ che è $\emptyset$. Tuttavia $(P_B, \cup)$ è un monoide con elemento identico B; infatti, per ogni $X \in P_B$ si ha: $X \cup B = X$ dato che $B \subseteq X$.

2. Sia M come nelle ipotesi, e siano $a, b, c \in M$; allora

$$(a\#b)\#c = (a \cdot m \cdot b)\#c = (a \cdot m \cdot b) \cdot m \cdot c = a \cdot m \cdot (b \cdot m \cdot c) = a\#(b \cdot m \cdot c) = a\#(b\#c)$$

quindi $\#$ è associativa e $(M, \#)$ è un semigruppo.

Supponiamo ora che esista un elemento identico e di $(M, \#)$. Allora, per ogni $a \in M$: $a = a\#e = a \cdot m \cdot e$ e $a = e\#a = e \cdot m \cdot a$. In particolare, se 1_M è l'elemento identico del monoide $(M, \cdot)$, deve essere $1_M = 1_M\#e = 1_M \cdot m \cdot e = m \cdot e$ e $1_M = e\#1_M = e \cdot m \cdot 1_M = e \cdot m$, quindi m è invertibile in $(M, \cdot)$ ed $e = m^{-1}$.

Viceversa, supponiamo che m sia invertibile in $(M, \cdot)$. Allora, per ogni $a \in M$ si ha: $m^{-1}\#a = m^{-1} \cdot m \cdot a = 1_M \cdot a = a$ e $a\#m^{-1} = a \cdot m \cdot m^{-1} = a \cdot 1_M = a$, e dunque m^{-1} è l'elemento identico di $(M, \#)$.

3. (i) $C(\mathrm{a})$ è un sottomonoide. Infatti, se $x, y \in C(\mathrm{a})$ allora: $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$ e dunque $xy \in C(\mathrm{a})$; inoltre $1_M \in C(\mathrm{a})$ poichè $1_M a = a = a1_M$.

(ii) $D(\mathrm{a})$ non è in generale un sottoinsieme chiuso. Ad esempio, nel monoide S_3 di tutte le permutazioni di $\{1, 2, 3\}$ si considerino le permutazioni α, β definite da: $\alpha(1) = 2$, $\alpha(2) = 1$, $\alpha(3) = 3$ e $\beta(1) = 3$, $\beta(2) = 2$, $\beta(3) = 1$. Allora $\alpha \circ \iota \circ \alpha = \alpha \circ \alpha = \iota$ e $\beta \circ \beta = \iota$ dove ι è l'applicazione identica. Quindi $\alpha, \beta \in D(\iota)$, ma (lo si verifichi) $\alpha \circ \beta \notin D(\iota)$.

(ii) $I(\mathrm{a})$ è un sottoinsieme chiuso: infatti siano $x, y \in I(\mathrm{a})$, allora xa e ya sono invertibili; siano b, c gli inversi rispettivamente di xa e di ya; allora $(xy)a(cab) = x((ya)c)ab = x(ab) = (xa)b = 1_M$ e $(cab)a(xy) = ca(b(ax))y = (ca)y = c(ay) = 1_M$. Quindi $(xy)a$ è invertibile e dunque $xy \in I(\mathrm{a})$. Tuttavia $I(\mathrm{a})$ non è in generale un sottomonoide. Infatti $1_M \in I(\mathrm{a})$ se e solo se a è invertibile.

4. (a) Siano $x, y, z, x', y', z', x'', y'', z'' \in L$, allora:

$$xyz \,\#\, (x'y'z' \,\#\, x''y''z'') = xyz \,\#\, x'y''z' = xy''z = xy'z \,\#\, x''y''z'' = (xyz \,\#\, x'y'z') \,\#\, x''y''z''$$

dunque $(X, \#)$ è un semigruppo. Non è commutativo perchè se x, y sono elementi distinti di L allora $xxx \,\#\, yyy = xyx \neq yxy = yyy \,\#xxx$.

(b) No. Consideriamo $U = \{\, x_1x_2x_3 \in X \mid x_3 = x \,\}$. Si verifica facilmente che U è un sottosemigruppo e che contiene xyx e yxx. Dunque U contiene il sottosemigruppo generato da $\{\, xyx, yxx \,\}$; ma $xxy \notin U$ e dunque xxy non appartiene al sottosemigruppo generato da $\{\, xyx, yxx \,\}$.

(c) $(X, \#)$ non è un monoide a meno che L non contenga un solo simbolo x; in tal caso $X = \{\, xxx \,\}$.

5. Sia $x \in S$ e poniamo $e = x^2 = x \cdot x$. Allora, per ogni $y \in S$ si ha $e = x \cdot x = x(yxy) = (xyx)y = yy = y^2$ e $ey = y^2y = yyy = y = yy^2 = ye$. Dunque S è un monoide con identità e.

Inoltre

$$xy = e(xy) = y^2(xy) = (yy)(xy) = y(yxy) = yx.$$

quindi $(S, \cdot)$ è commutativo. Infine, ogni elemento ammette inverso; infatti, se $y \in S$: $1_S = e = y \cdot y$ dunque $y^{-1} = y$.

6. Osserviamo che $b^3 = bbb = b$. Sia ora $a \in S$, allora

$$ba = b(bab) = b^2ab = b^2ab^3 = b(bab)b^2 = bab^2 = (bab)b = ab$$

dunque $ab = ba$. Inoltre $(S, \cdot)$ è un monoide con identità b^2; infatti, per ogni $a \in S$: $b^2a = b(ba) = b(ab) = bab = a$ e
$ab^2 = (ab)b = bab = a$.

7. Siano $(a, b), (a_1, b_1), (a_2, b_2) \in \mathbb{Q}^2$. Allora

$$(a, b) * ((a_1, b_1) * (a_2, b_2)) = (a, b) * (a_1a_2, a_1b_2 + b_1) = (a(a_1a_2), a(a_1b_2 + b_1) + b) =$$

$$= ((aa_1)a_2), (aa_1)b_2 + ab_1 + b) = (aa_1, ab_1 + b) * (a_2, b_2) = ((a, b) * (a_1, b_1)) * (a_2, b_2).$$

Dunque la operazione è associativa. L'elemento identico è $(1, 0)$, infatti, per ogni $(a, b) \in \mathbb{Q}^2$:

$$(1, 0) * (a, b) = (1a, 1b + 0) = (a, b) \quad \text{e} \quad (a, b) * (1, 0) = (a1, a0 + b) = (a, b).$$

Infine, per ogni $n \in \mathbb{N}$ si ha $(1, b)^n = (1, nb)$.

8. Siano $a, b, c \in \mathbb{Z}$. Allora

$$a * (b * c) = a + (b * c) - a(b * c) = a + (b + c - bc) - a(b + c - bc) = a + b + c - bc - ab - ac + abc =$$

$$(a + b - ab) + c - (a + b - ab)c = (a * b) + c - (a * b)c = (a * b) * c$$

Quindi $(\mathbb{Z}, *)$ è un semigruppo (e chiaramente commutativo). Inoltre, per ogni $a \in \mathbb{Z}$ si ha $0 * a = 0 + a - 0a = a$ e quindi $(\mathbb{Z}, *)$ è un monoide e 0 è l'elemento identico.
Sia u un elemento invertibile in $(\mathbb{Z}, *)$, allora esiste $b \in \mathbb{Z}$ tale che $0 = u * b = u + b - ub$. Quindi $u \neq 1$ e $b = \frac{u}{u-1} \in \mathbb{Z}$, che comporta $u = 0$ o $u = 2$; in entrambi i casi u coincide con il proprio inverso.

9. (a) NO (b) SI (c) SI (d) SI .

14. (b) $H = \mathbb{Z}/6\mathbb{Z}$

15. Sia G un gruppo privo di torsione, e siano $1 \neq x \in G$ e $n, m \in \mathbb{N}$, tali che $x^n = x^m$. Allora $x^{n-m} = x^n x^{-m} = x^n(x^m)^{-1} = x^n(x^n)^{-1} = 1$ e quindi, per la definizione di gruppo privo di torsione, $n = m$.

16. Sia G un gruppo finito di ordine pari. Allora la famiglia di sottoinsiemi

$$\{ \{x, x^{-1}\} \mid x \in G \}$$

è una partizione di G. Ora, a tale partizione appartiene anche l'insieme $\{1, 1^{-1}\} = \{1\}$. Poichè l'ordine di G (che è pari) è la somma degli ordini degli elementi della partizione, deve esistere,

oltre a $\{1\}$, almeno un altro elemento della partizione che abbia ordine dispari, quindi deve esistere $1 \neq x \in G$ tale che $\{x, x^{-1}\} = \{x\}$, cioè $x = x^{-1}$.

17. (c) Supponiamo che $D = \{\ x \in G \mid xg = g^{-1}x\ \} \neq \emptyset$ e sia $x \in D$. Dimostriamo che $D = xC$.
Sia $y \in C$, allora applicando il punto (a) :

$$(xy)g = x(yg) = x(gy) = (xg)y = (g^{-1}x)y = g^{-1}(xy)$$

dunque $xy \in D$, e ciò dimostra l'inclusione $xC \subseteq D$. Viceversa, sia $z \in D$, allora

$$(x^{-1}z)g = x^{-1}(zg) = x^{-1}(g^{-1}z) = (x^{-1}g^{-1})z = (x^{-1}g^{-1})(xx^{-1})z =$$

$$= x^{-1}(g^{-1}x)(x^{-1}z) = x^{-1}(xg)(x^{-1}z) = (x^{-1}x)g(x^{-1}z) = g(x^{-1}z)$$

cioè $x^{-1}z \in C$ e dunque $xC = zC$ che in particolare significa $z \in xC$. Quindi $D \subseteq xC$ e pertanto $D = xC$.
Infine, sia $H = C \cup D = C \cup xC$. Allora $H \neq \emptyset$ e se $x, y \in H$ allora, per quanto visto nei punti precedenti:
- $xy^{-1} \in C$ se $x, y \in C$;
- $xy^{-1} \in C$ se $x, y \in D$;
- $xy^{-1} \in D$ se $x \in D\ , y \in C$ o se $x \in C\ , y \in D$;

in ogni caso $xy^{-1} \in H$ e quindi per il criterio dei sottogruppi $H \leq G$.

18. (a) Sia $Hx = Ky$ e osserviamo che allora $x = 1x \in Ky$ e dunque $Kx = Ky$. Quindi, se $h \in H$, allora $hx \in Hx = Ky = Kx$ e quindi esiste $k \in K$ tale che $hx = kx$ cioè $h = k \in K$. Dunque $H \subseteq K$. Analogamente si prova che $K \subseteq H$ e quindi $H = K$.

23. Ricordo che se G è un gruppo finito allora, per ogni $g \in G :\ g^{|G|} = 1_G$.
Poichè $(15, 56) = 1$ esistono numeri interi a e b tali che $1 = 15a + 56b$, ed allora :

$$g = g^1 = g^{15a+56b} = (g^{15})^a(g^{56})^b = 1_G 1_G = 1_G$$

24. Se $G =< g >$ e $H \leq G$, allora $G/H =< Hg >$.

27. Siano $H_1, H_2, \ldots, H_n$ tutti i sottogruppi propri e diversi da $\{1\}$ di G. Allora, per il Teorema di Lagrange, $|H_i| = p$ per ogni $i = 1, \ldots, n$, e se $i \neq j\ :\ H_i \cap H_j = \{1\}$ (infatti $H_i \cap H_j$ è un sottogruppo proprio di H_i e $p = |H_i|$ è primo). Quindi

$$p^2 = |G| \geq \left| \bigcup_{i+1}^{n} H_i \right| = \sum_{i=1}^{n} |H_i \setminus \{1\}| \ + 1 = n(p-1) + 1$$

e dunque $n \leq \frac{p^2-1}{p-1} = p + 1$. Ora, oltre ai sottogruppi H_i, il gruppo G ha il sottogruppo improprio G e il sottogruppo banale $\{1\}$. In totale G ha dunque al più $p + 3$ sottogruppi.

28. (a) Si verifica che l'applicazione $f :\ \mathbb{Z} \times \mathbb{Z} \ \to\ \mathbb{Z} \times \mathbb{Z}$ definita da $f(a, b) = (b, b - a)$, per ogni $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, è l'inversa di f.

(b) L'ordine di f nel gruppo $Sym(\mathbb{Z} \times \mathbb{Z})$ è 6.

(c) SI .

31. Chiaramente $H \neq \emptyset$. Siano $x, y \in H$. Allora esistono indici $i, j \in \mathbb{N}$, tali che $x \in H_i$ e $y \in H_j$. Se $i \leq j$ allora $H_i \leq H_j$ e quindi $x, y \in H_j$. Poichè H_j è un sottogruppo di G, $xy^{-1} \in H_j \subseteq H$. Per il criterio dei sottogruppi H è un sottogruppo di G.

Supponiamo ora che esista $k \in \mathbb{N}$ tale che, per $n \geq k$, H_n è normale in G, e siano $x \in H$, $g \in G$. Allora esiste $i \in \mathbb{N}$ tale che $x \in H_i$; quindi $x \in H_{i+k}$. Poichè H_{i+k} è normale in G: $g^{-1}xg \in H_{i+k} \subseteq H$ e, per il criterio di normalità, H è normale in G.

34. (c) Sia $g = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix} \in G \setminus N$. Allora $|g| = \infty$ e $|gN| = 3$.

37. Poniamo $N =< S >$, e sia $g \in G$. Per ogni $s \in S$ si ha, per ipotesi, $gsg^{-1} = s^{g^{-1}} \in S \subseteq N$, e quindi $s = (s^{g^{-1}})^g \in N^g$. Dunque $S \subseteq N^g$. Poiché N^g è un sottogruppo di G, dalla definizione di sottogruppo generato $\langle S \rangle$ segue $N \leq N^g$. Questo è vero per ogni g e quindi $N = N^g$, per ogni $g \in G$ (infatti, da $N \leq N^{g^{-1}}$ segue $N^g \leq N$, quindi $N^g = N$), e pertanto N è un sottogruippo normale di G.

38. (a) Siano $x, y \in G$. Allora, poichè G/M è abeliano:

$$Mxy = (Mx)(My) = (My)(Mx) = Myx$$

e dunque $(xy)(yx)^{-1} \in M$. Similmente si dimostra che $(xy)(yx)^{-1} \in N$. Quindi $(xy)(yx)^{-1} \in M \cap N$, e dunque:

$$(M \cap N)x(M \cap N)y = (M \cap N)xy = (M \cap N)yx = (M \cap N)y(M \cap N)y$$

cioè $G/(M \cap N)$ è abeliano.

(b) Per il secondo Teorema di omomorfismo :

$$H/(H \cap N) \simeq NH/N$$

poichè NH/N è un sottogruppo di G/N, esso è abeliano, e quindi $H/(H \cap N)$ è abeliano.

41. Sia $A = \{ g \in G \mid \psi(g) = \zeta(g) \}$. Allora $A \neq \emptyset$, infatti $\psi(1_G) = 1_{G'} = \zeta(1_G)$ e quindi $1_G \in A$. Siano ora $x, y \in A$, allora

$$\psi(xy^{-1}) = \psi(x)(\psi(y))^{-1} = \zeta(x)(\zeta(y))^{-1} = \zeta(xy^{-1})$$

dunque $xy^{-1} \in A$ e, per il criterio dei sottogruppi, $A \leq G$.
Supponiamo ora che S sia un sistema di generatori di G tale che $\psi(s) = \zeta(s)$ per ogni $s \in S$; allora $S \subseteq A$ e, poichè A è un sottogruppo $G =< S >\leq A$, cioè $G = A$ e di conseguenza $\psi = \zeta$.

43. Siano G e H gruppi finiti tali che $(|G|, |H|) = 2$, e sia $\phi : G \to H$ un omomorfismo tale che $Ker(\phi) \neq G$. Sia $K = Ker(\phi)$ e $L = \phi(G)$. Per il Teorema di omomorfismo: $G/K \simeq L$; in particolare $|G/K| = |L|$. Ora, per il Teorema di Lagrange, $|G/K|$ divide $|G|$ e $|G/K| = |L|$ divide $|H|$. Quindi $|G/K|$ divide $(|G|, |H|) = 2$. Poichè per ipotesi $K \neq G$, deve essere $|G/K| = 2$ e quindi K è un sottogruppo di indice 2 in G.

44. Sia

$$(a,b,c) \in \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

allora $2(a,b,c) = (2a,2b,2c) = (\bar{0},\bar{0},\bar{0})$. Sia

$$f \ : \ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \ \to \ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

un omomorfismo; allora $f(\bar{0},\bar{2}) = f((\bar{0},\bar{1})+(\bar{0},\bar{1})) = f(\bar{0},\bar{1})+f(\bar{0},\bar{1}) = 2f(\bar{0},\bar{1}) = (\bar{0},\bar{0},\bar{0})$. Quindi $(\bar{0},\bar{0}) \neq (\bar{0},\bar{2}) \in Ker(f)$ e dunque f non è iniettiva (e pertanto non è un isomorfismo). Similmente si dimostra il non isomorfismo delle altre coppie di gruppi da considerare.

46. Sia $g \in G$. Allora

$$\psi(\psi(g^{-1})g) = \psi(\psi(g^{-1}))\psi(g) = (\psi\circ\psi)(g^{-1})\psi(g) = \psi(g^{-1})\psi(g) = \psi(g)^{-1}\psi(g) = 1$$

dunque $h = \psi(g^{-1})g \in Ker(\psi)$, e quindi $g = \psi(g)h \in \psi(G)Ker(\psi)$.
Sia ora $g \in \psi(G) \cap Ker(\psi)$. Allora, poichè $g \in \psi(G)$, esiste $h \in G$ tale che $g = \psi(h)$ e quindi, poichè $g \in Ker(\psi)$:

$$g = \psi(h) = (\psi\circ\psi)(h) = \psi(\psi(h)) = \psi(g) = 1.$$

48. (a) Siano $\frac{m}{n}$, $\frac{m'}{n'} \in G$ e sia $r = m.c.m.(n,n')$. Allora $r \mid 12$ e quindi

$$\frac{m}{n} - \frac{m'}{n'} = \frac{m\frac{r}{n} - m'\frac{r}{n'}}{r} \in G$$

e dunque G è un sottogruppo di $(\mathbb{Q},+)$.
(b) Chiaramente $\mathbb{Z} \leq G$ ed è normale perchè G è commutativo. Dimostriamo che

$$G/\mathbb{Z} = \left\{ \ \frac{r}{12} + \mathbb{Z} \mid 0 \leq r \leq 11 \ \right\}.$$

Sia $\frac{m}{n} \in G$; allora $n \mid 12$ e quindi esiste $c \in \mathbb{N}$ tale che $12 = nc$. Siano $q, r \in \mathbb{Z}$ con $mc = 12q + r$ e $0 \leq r \leq 11$. Allora

$$\frac{m}{n} - \frac{r}{12} = \frac{mc}{12} - \frac{r}{12} = \frac{mc-r}{12} = \frac{12q}{12} = q \in \mathbb{Z}$$

e dunque :

$$\frac{m}{n} + \mathbb{Z} = \frac{r}{12} + \mathbb{Z}$$

con $0 \leq r \leq 11$, che è ciò che si voleva provare.
Ora se $0 \leq r, s \leq 11$, si ha

$$\frac{r}{12} + \mathbb{Z} = \frac{s}{12} + \mathbb{Z} \quad \Leftrightarrow \quad \frac{r-s}{12} = \frac{r}{12} - \frac{s}{12} \in \mathbb{Z} \quad \Leftrightarrow \quad 12 \mid (r-s) \quad \Leftrightarrow \quad r = s \ ,$$

dunque gli elementi di $G/\mathbb{Z}$ sopra descritti sono tutti distinti e quindi $|G/\mathbb{Z}| = 12$.
infine $G/\mathbb{Z}$ è un gruppo ciclico generato da $\frac{1}{12} + \mathbb{Z}$.
(c) Poichè $\mathbb{Z}/3\mathbb{Z} = [\mathbb{Z} \ : \ 3\mathbb{Z}] = 3$, si ha, per la formula dei gradi,
$|G/3\mathbb{Z}| = [G \ : \ 3\mathbb{Z}] = [G \ : \ \mathbb{Z}][\mathbb{Z} \ : \ 3\mathbb{Z}] = 12 \cdot 3 = 36$.

49. (a,b) Consideriamo l'applicazione $\Phi : \mathbb{C}^* \to GL(2,\mathbb{R})$ definita da, per ogni $z = a+bi \in \mathbb{C}^*$:

$$\phi(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ;$$

proviamo che è un omomorfismo di gruppi. Infatti, siano $z = a + bi$, $z_1 = a_1 + b_1 i \in \mathbb{C}^*$; allora

$$\Phi(z)\phi(z_1) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} = \begin{pmatrix} aa_1 - bb_1 & -(ab_1 + a_1 b) \\ (ab_1 + a_1 b) & aa_1 - bb_1 \end{pmatrix} =$$

$$= \Phi(aa_1 - bb_1 + (ab_1 + a_1 b)i) = \phi(zz_1)$$

quindi Φ è un omomorfismo. Per un fatto noto si ricava in particolare che $\Phi(\mathbb{C}^*) = G$ è un sottogruppo di $GL(2,\mathbb{R})$.
Ora, ϕ è la applicazione ottenuta da Φ restringendo il codominio alla sola immagine, dunque ϕ è un omomorfismo suriettivo. Esso è anche iniettivo; infatti,

$$\phi(a + bi) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \Leftrightarrow \qquad a = 1 \ , \ b = 0$$

quindi $Ker(\phi) = 1$ e dunque ϕ è iniettiva e un isomorfismo.

(c) Sia $A \in G$ tale che $A^3 = 1$. Allora, se $z \in C^*$ è tale che $\phi(z) = A$, si ha $1 = (\phi(z))^3 = \phi(z^3)$ e quindi, per l'iniettività, $z^3 = 1$. Dunque gli elementi di G cercati sono le immagini tramite ϕ delle radici terze dell'unità in C^*. Le radici terze sono:

$$\zeta_1 = 1 \ , \quad \zeta_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2} i \ , \quad \zeta_3 = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$$

quindi gli elementi cercati sono

$$A_1 = \phi(\zeta_1) = 1, \quad A_2 = \phi(\zeta_2) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad A_3 = \phi(\zeta_3) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} .$$

(d) Sia $z = a + bi \in C^*$. Allora, osservando che $C^{-1} = C$:

$$(\phi(z))^C = C^{-1}(\phi(z))C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ a & -b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \phi(a - bi) = \phi(\overline{z}) \ .$$

53. (a) Poichè $G = H \times K$ è un gruppo finito e $|G| = |H||K|$, applicando il Teorema di Lagrange si ha:

$$[G : S] = \frac{|G|}{|S|} = \frac{|H||K|}{|S|} = |K|\frac{|H|}{|S|} = |K|[H : S] \ .$$

(b) Certamente $S \leq G$. Aplichiamo il criterio per provare che S è normale in G. Poichè G è il prodotto diretto di H e K sappiamo che $hk = kh$ per ogni $h \in H$ e $k \in K$; in particolare, $xk = kx$ per ogni $x \in S$ ed ogni $k \in K$.

Siano ora $x \in S$ e $g \in G$; allora esistono $h \in H,\ k \in K$ tali che $g = kh$ e quindi

$$x^g = g^{-1}xg = (kh)^{-1}x(kh) = h^{-1}k^{-1}xkh = h^{-1}k^{-1}kxh = h^{-1}xh \in S$$

perchè $S \trianglelefteq H$. Dunque, per il criterio di normalità, $S \trianglelefteq G$.

54. Sia $[G : H] = n$ e $[G : K] = m$ con $(n, m) = 1$.
Proviamo innanzi tutto che allora $[G\ :\ H \cap K] = nm$. Poichè $H \cap K \leq H$ si ha $n = [G : H] \mid [G\ :\ H \cap K]$ e similmente $m \mid [G\ :\ H \cap K]$. Dunque $nm = \text{m.c.m.}(n, m)$ divide $[G\ :\ H \cap K]$ e quindi, per il Lemma di Poincare:

$$nm = [G : H][G : K] \geq [G\ :\ H \cap K] \geq nm$$

da cui $nm = [G\ :\ H \cap K]$.
Ora, applicando la formula per il prodotto di sottogruppi, ed il Teorema di Lagrange :

$$|G||HK| = \frac{|G||H||K|}{|H \cap K|} = \frac{|G|}{|H \cap K|} \cdot |H||K| =$$

$$= [G : H][G : K]|H||K| = |G|^2$$

e dunque $|HK| = |G|$ da cui segue $HK = KH = G$.

55. (a) $(1, 1) \in D \neq \emptyset$. Se $(g, g), (h, h) \in D$ (quindi $g, h \in G$) allora: $(g, g)(h, h)^{-1} = (g, g)(h^{-1}, h^{-1}) = (gh^{-1}, gh^{-1}) \in D$ e quindi D è un sottogruppo di W.
Si consideri ora la applicazione $f\ :\ G \to W$ definita da, per ogni $g \in G\ :\ f(g) = (g, g)$. Verificate che f è un isomorfismo di gruppi.

(b) Sia D normale in W. Allora, per ogni $g, h \in G$ si ha che D contiene $(h, 1)^{-1}(g, g)(h, 1) = (h^{-1}, 1)(g, g)(h, 1) = (h^{-1}gh, g)$, e quindi $h^{-1}gh = g$; moltiplicando a destra per h si ottiene $gh = hg$. Poichè ciò vale per ogni $g, h \in G$, G è abeliano.
Viceversa, sia G abeliano e siano $(x, y) \in W$ e $(g, g) \in D$. Allora

$$(x, y)^{-1}(g, g)(x, y) = (x^{-1}, y^{-1})(g, g)(x, y) = (x^{-1}gx, y^{-1}gy) = (x^{-1}xg, y^{-1}yg) = (g, g)$$

e dunque D è normale in W.
(Si poteva anche osservare che se G è abeliano, allora anche W è abeliano, e quindi ogni suo sottogruppo - in particolare D - è normale.)

57. (a) $\sigma = (1\ 3\ 6)(2\ 7\ 4)$.

(b) Sia, per assurdo, $\tau = (i\ j)$ una trasposizione di $\{1, 2, ..., 7\}$ tale che $\sigma\tau = \tau\sigma$. Si osserva che si ha $\sigma(i) \notin \{i, j\}$ o $\sigma(j) \notin \{i, j\}$. Supponiamo, scambiando eventualmente i con j, $\sigma(i) \notin \{i, j\}$. Allora $\tau(\sigma(i)) = \sigma(i)$ e quindi

$$\sigma(i) = \tau(\sigma(i)) = \tau\sigma(i) = \sigma\tau(i) = \sigma(j)$$

che è assurdo perchè σ è biettiva e $i \neq j$.

58. (a) $\sigma = (1\ 5)(3\ 4)(2\ 8\ 7)$ ha classe pari.

(b) $|\sigma| = 6$ e $|C_{S_8}(\sigma)| = 24$.

60. (a) $\sigma = (1\ 4\ 6\ 3)(2\ 7\ 8)$ ha classe dispari.

(b) L'esercizio chiede di trovare una tale permutazione τ , non di determinarle tutte. Possiamo innanzi tutto cercare se esiste una tale τ che abbia ordine 2. Allora la condizione diventa $(16)\sigma = \sigma\tau$; e moltiplicando a sinistra per σ^{-1} si ottiene $\tau = \sigma(1\ 6)\sigma^{-1} = (4\ 7)$.

61. Si consideri la permutazione di $\{1, 2, \ldots, 6\}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix}.$$

(a) $\sigma = (1\ 4)(2\ 6\ 3)$.

(b) $| < s > | = |s| = 6$.
(infatti $< s >= \{\ \iota,\ \sigma,\ \sigma^2 = (2\ 3\ 6),\ \sigma^3 = (1\ 4),\ \sigma^4 = (2\ 6\ 3),\ \sigma^5 = \sigma^{-1} = (1\ 4)(2\ 3\ 6)\ \}$)

62. (a) $\alpha\beta = (1\ 2\ 3\ 4)(1\ 5\ 2\ 4) = (1\ 4\ 5\ 2\ 3)$ ha ordine 5.

(b) Sia $H =< \alpha, \beta >$. Poichè $\alpha(6) = 6 = \beta(6)$, $H \leq \mathrm{Stab}_{S_6}(6)$ e quindi $O_H(6) = \{6\}$. Inoltre H contiene $\alpha\beta = (1\ 4\ 5\ 2\ 3)$ e quindi $O_H(1) = \{\ 1, 2, 3, 4, 5\ \}$. Dunque le orbite di H su $\{1, 2, 3, 4, 5, 6\}$ sono $\{6\}$ e $\{\ 1, 2, 3, 4, 5\ \}$.

(c) - $(1\ 2\ 3\ 4)(1\ 4\ 3\ 2) = \iota$ ha ordine 1;
- $(1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4)$ ha ordine 2;
- $(1\ 2\ 3\ 4)(1\ 3\ 2\ 4) = (1\ 4\ 3)$ ha ordine 3;
- $\alpha\beta = (1\ 2\ 3\ 4)(1\ 5\ 2\ 4) = (1\ 4\ 5\ 2\ 3)$ ha ordine 5;
- in S_6 non esistono elementi di ordine 7 dato che 7 non divide l'ordine di S_6 che è 6! .

La risposta è dunque $n = 1,\ 2,\ 3,\ 5$.

64. Il solo sottogruppo normale proprio e non banale del gruppo alterno A_4 è

$$K = \{\ \iota,\ (12)(34),\ (13)(24),\ (14)(23)\ \}.$$

65. Sia, per assurdo, H un sottogruppo di ordine 6 di A_4 e sia K il sottogruppo normale di A_4 dell'esercizio precedente. Allora, poichè $|A_4| = 12$, $[A_4 : H] = 2$ e $[A_4 : K] = 3$. Quindi, per l'esercizio 2.57, $A_4 = HK$ e $|H \cap K| = 2$. Sia $H \cap K = \{\iota, \sigma\}$ dove σ è uno degli elementi non identici di K, possiamo supporre $\sigma = (12)(34)$. Ora, $H \cap K$ è normale in H perchè K è normale in A_4 ed è normale in K perchè K è abeliano. Quindi $H \cap K$ è normale in A_4, e questo è assurdo perchè $(123)^{-1}\sigma(123) = (14)(23) \notin H \cap K$. Dunque A_4 non ha sottogruppi di ordine 6.

66. $n = 4$. Infatti $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$ e 4 non divide gli ordini di S_2 e S_3 e quindi $\mathbb{Z}_2 \times \mathbb{Z}_2$ non può essere immerso in questi due gruppi. Infine il sottogruppo K di S_4 dell'esercizio 2.67 è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, quindi $\mathbb{Z}_2 \times \mathbb{Z}_2$ si immerge in S_4.

68. E' facile verificare che H e K sono sottogruppi. Vediamo che K è normale in H. Sia $\sigma \in K$ e osserviamo che poichè $\sigma(\{1, 2\}) = \{1, 2\}$ (dato che $K \subseteq H$) e $\sigma(1) = 1$, deve essere $\sigma(2) = 2$. Sia $\rho \in H$. Se $\rho(1) = 1$ allora $\rho \in K$ e quindi $\rho^{-1}\sigma\rho \in K$. Altrimenti, $\rho(1) = 2$ ed allora $\rho^{-1}(2) = 1$ e $\rho^{-1}\sigma\rho(1) = \rho^{-1}\sigma(2) = \rho^{-1}(2) = 1$, e quindi $\rho^{-1}\sigma\rho \in K$. Per il criterio noto, K è normale in H.

69. $\iota \in H$ e se $\sigma, \tau \in H$ allora $\sigma\tau(H) = \sigma(\tau(H)) = \sigma(H) = H$ e $\sigma^{-1}(H) = \sigma^{-1}(\sigma(H)) = \sigma^{-1}\sigma(H) = \iota(H) = H$. Dunque $H \leq S_n$.

Si consideri ora la applicazione $\Theta : H \to S_T$ definita da, per ogni $\sigma \in H : \Theta(\sigma) = \sigma_{|T}$ (la restrizione di σ a T). Verificate che Θ è un omomorfismo suriettivo e che $K = \mathrm{Ker}(\theta)$. Allora $H/K \simeq S_T$ e quindi $H/K \simeq S_k$ se $k = |T|$.

72. Le lunghezze delle orbite dell'azione di G su S sono divisori di $|G| = 2 \cdot 17 \cdot 59$ e non eccedono $|S| = 20$. Le possibilità sono quindi $1,\ 2,\ 17$. Poichè la somma delle lunghezze delle orbite deve dare 20, si conclude che G deve avere almeno 3 orbite su S. Se inoltre l'azione di G su S è priva di punti fissi, allora non c'è alcuna orbita di lunghezza 17, quindi ogni orbita ha lunghezza 2 e dunque vi sono 10 orbite.

78. (b) Supponiamo che l'azione di G su Ω sia 2-transitiva, sia $x \in \Omega$ e $y, z \in \Omega \setminus \{x\}$. Per la 2-transitività, esiste allora $g \in G$ tale che $x \cdot g = x$ e $y \cdot g = z$, il che dimostra che G_x opera transitivamente su $\Omega \setminus \{x\}$.

Viceversa, sia data un azione transitiva di G su Ω tale che, per $x \in \Omega$, G_x è transitivo su $\Omega \setminus \{x\}$. Osserviamo che, poiché l'azione è transitiva, tale proprietà dello stabilizzatore vale per ogni elemento $x \in \Omega$. Siano $x, x_1, y, y_1 \in \Omega$ con $x \neq x_1$ e $y \neq y_1$. Per la transitività esiste $h \in G$ tale che $x \cdot h = y$. Poiché $x_1 \neq x$, si ha anche $x_1 \cdot h \neq y$; dunque y_1 e $x_1 \cdot h$ appartengono a $\Omega \setminus \{y\}$. Per la condizione sullo stabilizzatore G_y esiste quindi $s \in G_y$ tale che $(x_1 \cdot h) \cdot s = y_1$. Ponendo allora $g = hs$ si ottiene $x \cdot g = (x \cdot h) \cdot s = y \cdot s = y$ e $x_1 \cdot g = (x_1 \cdot h) \cdot s = y_1$. Quindi l'azione di G su Ω è 2-transitiva.

81. (b) $[U_m : U_n] = m/n$.

(c) Si consideri la applicazione $f : \mathbb{C}^* \longrightarrow \mathbb{C}^*$ definita da $f(x) = x^n$. Si verifica facilmente che f è un omomrfismo di gruppi moltiplicativi, e che $Ker(f) = U_n$. Inoltre f è suriettiva. Per il Teorema di omomorfismo si ha quindi che $\mathbb{C}^*/U_n$ è isomorfo a $\mathbb{C}^*$.

(d) $\mathbb{C}^*/U$ non è isomorfo a $\mathbb{C}^*$. Si può affermare questo osservando che $\mathbb{C}^*$ contiene elementi non banali di ordine finito (ad esempio -1 che ha ordine 2), mentre $\mathbb{C}^*/U$ non ne contiene. Infatti, sia $zU \in \mathbb{C}^*/U$ (con $z \in \mathbb{C}^*$) tale che $(zU)^2 = 1_{\mathbb{C}^*/U} = U$, allora $z^2 \in U$. Quindi esiste $0 \neq n \in \mathbb{N}$ tale che $z^{2n} = (z^2)^n = 1$, che comporta $z \in U$ e dunque $zU = U = 1_{\mathbb{C}^*/U}$.

82. Sia F l'insieme degli elementi di un gruppo G che hanno un numero finito di coniugati distinti in G. Innanzi tutto $F \neq \emptyset$, perchè $1_G \in F$. Osserviamo quindi che, per $x \in G$ si ha $x \in F$ se e solo se l'indice $[G : C_G(x)]$ è finito. Siano quindi $x, y \in F$; allora $C_G(xy^{-1}) \subseteq C_G(x) \cap C_G(y)$ e dunque

$$[G : C_G(xy^{-1})] \leq [G : C_G(x) \cap C_G(y)]$$

che è finito. Quindi $F \leq G$. Infine F è normale, perchè se $x \in F$ e $g \in G$, allora $C_G(x^g) = C_G(x)^g$, e quindi $[G : C_G(x^g)] = [G : C_G(x)]$ da cui segue $x^g \in F$.

83. Poiché H è normale, HK è un sottogruppo e per il secondo Teorema di omomorfismo si ha

$$\frac{HK}{H} \simeq \frac{K}{H \cap K}$$

Quindi l'ordine di HK/H divide sia $|G/H|$ che $|K| = |H|$. Poichè $(|H|, |G/H|) = 1$, deve essere $|HK/H| = 1$, cioè $HK = H$ che implica $H \leq K$ e, per questioni di ordine, $H = K$.

86. Procediamo per induzione su k. Poichè G è un p-gruppo finito, $Z(G) \neq \{1\}$. Quindi esiste un elemento $x \in Z(G)$ di ordine p. Sia $N =< x >$; allora N è normale in G e $|N| = p$. Dunque la cosa è provata per $k = 1$. Se $k \geq 2$ consideriamo il gruppo quoziente G/N. Per ipotesi induttiva, esso ammette un sottogruppo normale K/N di ordine p^{k-1}; dove, per il Teorema di corrispondenza, K è un sottogruppo normale di G contenente N. Infine si ha $|K| = |N|[K : N] = |N||K/N| = p \cdot p^{k-1} = p^k$.

87. Siano $K_1, K_2, \ldots, K_t$ le classi di coniugio distinte di G e, per ogni $i = 1, 2, \ldots, t$ fissiamo un rappresentante x_i della classe K_i. Osserviamo quindi che se $g \in K_i$, allora $C_G(g)$ è coniugato a $C_G(x_i)$ e quindi $|C_G(g)| = |C_G(x_i)|$ Dunque, per ogni $i = 1, 2, \ldots, t$

$$\sum_{g \in K_i} |C_G(g)| = \sum_{g \in K_i} |C_G(x_i)| = |K_i||C_G(x_i)| = [G : C_G(x_i)]|C_G(x_i)| = |G|$$

Infine, poichè le classi di coniugio costituiscono una partizione di G

$$\sum_{g \in G} |C_G(g)| = \sum_{i=1}^{t} \sum_{g \in K_i} |C_G(g)| = \sum_{i=1}^{t} |G| = t|G|$$

da cui la formula cercata.