SOLUZIONI DEGLI ESERCIZI SUI GRUPPI

SOLUZIONI DEGLI ESERCIZI PROPOSTI

Esercizio 1.

Dobbiamo verificare che:

(a) il prodotto di due elementi di G è un elemento di G;

(b) sono soddisfatti gli assiomi dei gruppi;

(c) il prodotto è commutativo.

Dimostriamo (a):
$\forall h, k \in \mathbb{Z}: \ 2^h \cdot 2^k = 2^{h+k} \in \mathbb{Z}$

Dimostriamo (b):

associatività:
$(2^h \cdot 2^k) \cdot 2^m = (2^{h+k}) \cdot 2^m = 2^{h+k+m} = 2^h \cdot (2^{k+m}) = 2^h \cdot (2^k \cdot 2^m)$;

esistenza identità:
$2^0 \cdot 2^k = 2^{0+k} = 2^k$;

esistenza reciproco:
$2^{-k} \cdot 2^k = 2^{-k+k} = 2^0$.

Dimostriamo (c):
$2^h \cdot 2^k = 2^{h+k} = 2^{k+h} = 2^k \cdot 2^h$.

Esercizio 2.

Iniziamo con il provare che la somma di due elementi di G è ancora un elemento di G : per ogni $a, b, a_1, b_2 \in \mathbb{Q}$ si ha

$$(a + b\sqrt{2}) + (a_1 + b_1\sqrt{2}) = (a + a_1) + (b + b_1)\sqrt{2} \in G.$$

Verifichiamo ora le altre proprietà dei gruppi.
associatività: per ogni a, b, a_1, b_1, a_2, b_2 si ha

$$\{[(a + b\sqrt{2}) + (a_1 + b_1\sqrt{2})] + (a_2 + b_2\sqrt{2})\} = \{(a + b\sqrt{2}) + [(a_1 + b_1\sqrt{2}) + (a + b\sqrt{2})]\}$$

esistenza identità: per ogni $a, b \in \mathbb{Q}$ si ha

$$(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (a + b\sqrt{2})$$

esistenza inverso: per ogni $a, b \in \mathbb{Q}$ si ha

$$(a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0 + 0\sqrt{2}$$

commutatitvità: per ogni a, b, a_1, b_1 si ha

$$(a + b\sqrt{2}) + (a_1 + b_1\sqrt{2}) = (a_1 + b_1\sqrt{2}) + (a + b\sqrt{2}).$$

Posto

$$G_1 = \{b\sqrt{2}: \ b \in \mathbb{Q}\}, \quad G_2 = \{b\sqrt{2}: \ b \in \mathbb{Z}\}, \quad G_3 = \{a + b\sqrt{2}: \ a, b \in \mathbb{Z}\},$$

si ha che i sottogruppi di G sono: $(G_1, +)$, $(G_2, +)$, $(G_3, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$.

Esercizio 3.

Dall'eguaglianza $a^{-1}b^2a = ba$ moltiplicando primo e secondo membro, a sinistra per a e a destra per $a^{-1}b^{-1}$ si ha

$$a\,a^{-1}b^2a\,a^{-1}b^{-1} \;=\; a\,ba\,a^{-1}b^{-1} \iff b^2b^{-1} \;=\; abb^{-1} \iff bbb^{-1} \;=\; a \iff b = a.$$

Esercizio 4.

Osserviamo che per ogni $a, b, c \in G$ risulta $a^{-1}, b^{-1}, c^{-1} \in G$ e si ha

$$a\;a^{-1}cb^{-1}b \;=\; (aa^{-1})c(b^{-1}b) \;=\; c$$

possimo quindi porre

$$x = a^{-1}cb^{-1}.$$

Dimostriamo l'unicità della soluzione. Sia $y \in G$ tale che

$$ayb \;=\; c,$$

Moltiplichiamo primo e secondo membro dell'equazione, a sinistra, per a^{-1}, a destra per b^{-1} :

$$a^{-1}\,ayb\,b^{-1} \;=\; a^{-1}\,c\,b^{-1},$$

da cui

$$y \;=\; a^{-1}cb^{-1} \;=\; x.$$

Esercizio 5.

Consideriamo per primo il caso $n > 0$ ed utilizziamo il *Principio di Induzione*. Per $n = 1$ la proposizione è vera per ipotesi. Verifichiamo l'induttività della proposizione, ovvero

$$a^nb = ba^n \Longrightarrow a^{n+1}b = ba^{n+1}.$$

A tale scopo scriviamo le seguenti eguaglianze:

$$a^{n+1}b = (a^na)b = \qquad \text{(proprietà associativa)}$$

$$= a^n(ab) = a^n(ba) = (a^nb)a = \qquad \text{(ipotesi induttiva)}$$

$$= (ba^n)a = b(a^na) = ba^{n+1}.$$

Se $n = 0$ si ha $a^0b = ba^0$, ovvero $b = b$.
Consideriamo ora il caso $n < 0$. Dall'ipotesi $ab = ba$ segue moltiplicando per a destra e a sinistra entrambi i membri per a^{-1} :

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

Ovvero *se un elemento b commuta con un altro a allora commuta anche con il suo inverso* a^{-1}. Dal fatto che $n < 0$ segue che $-n > 0$, quindi $a^{-n}b = ba^{-n}$. Ma allora, per quanto detto sopra: b deve commutare con l'inverso $(a^{-n})^{-1} = a^n$ di a^{-n}, ovvero $a^nb = ba^n$.

Esercizio 6.

Nell'eguaglianza $a^n b^m = b^m a^n$ si pone $c = b^m$ ottenendo $a^n c = ca^n$ che è stata dimostrata nel precedente esercizio, e quindi la tesi è banalmente vera.

Esercizio 7.

Si procede per induzione su k. Per $k = 1$ è vera (vedi Esercizio 5).
Dimostriamo l'induttività:

$$(a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}) b^m = b^m (a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}) \Longrightarrow (a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} a_{k+1}^{n_{k+1}}) b^m = b^m (a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} a_{k+1}^{n_{k+1}})$$

Infatti:

$$(a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} a_{k+1}^{n_{k+1}}) b^m = (a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k})(a_{k+1}^{n_{k+1}} b^m)$$

Dall' Esercizio 6 sappiamo che $a_{k+1}^{n_{k+1}} b^m = b^m a_{k+1}^{n_{k+1}}$ sotituendo al secondo membro dell'eguaglianza sopra:

$$\begin{aligned}
(a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k})(a_{k+1}^{n_{k+1}} b^m) &= (a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k})(b^m a_{k+1}^{n_{k+1}}) = \\
&= (a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} b^m) a_{k+1}^{n_{k+1}} = \quad \text{(ipotesi induttiva)} \\
&= (b^m a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}) a_{k+1}^{n_{k+1}} = \\
&= b^m a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} a_{k+1}^{n_{k+1}}
\end{aligned}$$

Esercizio 8.

Dimostriamo per induzione su k. Se $k = 2$ si tratta del Lemma dimostrato nel Capitolo sui gruppi. Dimostriamo l'induttività:

$$(a_1 a_2 \cdots a_k)^n = a_1^n a_2^n \cdots a_k^n \Longrightarrow (a_1 a_2 \cdots a_k a_{k+1})^n = a_1^n a_2^n \cdots a_k^n \, a_{k+1}^n$$

Infatti

$$\begin{aligned}
& (a_1 a_2 \cdots a_k a_{k+1})^n = \quad \text{(perchè vale per il prodotto di due fattori)} \\
= \; & (a_1 a_2 \cdots a_k)^n \, a_{k+1}^n = \quad \text{(per l'ipotesi induttiva)} \\
= \; & a_1^n a_2^n \cdots a_k^n a_{k+1}^n
\end{aligned}$$

Esercizio 9.

Osserviamo per prima cosa che per ogni $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ risulta $(a + c, (-1)^c b + d) \in \mathbb{Z} \times \mathbb{Z}$
Dimostriamo che sono verificati gli assiomi dei gruppi.
Associatività: per ogni $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}$ risulta:

$$\begin{aligned}
[(a, b) \times (c, d)] \times (e, f) &= (a + c, (-1)^c \, b + d) \times (e, f) = \\
&= (a + c + e, (-1)^e ((-1)^c \, b + d) + f) = \\
&= (a + c + e, (-1)^{e+c} \, b + (-1)^e \, d + f).
\end{aligned}$$

D'altra parte

$$\begin{aligned}(a,b)\times[(c,d)\times(e,f)] &= (a,b)\times(c+e,(-1)^e\,d+f)=\\ &= (a+c+e,(-1)^{c+e}\,b+(-1)^e\,d+f).\end{aligned}$$

Quindi

$$[(a,b)\times(c,d)]\times(e,f) \;=\; (a,b)\times[(c,d)\times(e,f)].$$

esistenza identità: per ogni $(a,b)\in\mathbb{Z}\times\mathbb{Z}$:

$$(a,b)\times(0,0) \;=\; (a+0,(-1)^0\,b+0)=(a,b)$$

esistenza inverso: dobbiamo dimostrare che per ogni $(a,b)\in\mathbb{Z}$ esiste $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ tale che $(a,b)\times(x,y)=(0,0)$. Quindi

$$(a,b)\times(x,y)=(0,0) \iff (a+x,(-1)^x b+y) \;=\; (0,0) \Longrightarrow \begin{cases} a+x &= 0\\ (-1)^x\,b+y &= 0.\end{cases}$$

Da cui segue

$$\begin{cases} x &= -a\in\mathbb{Z}\\ y &= -(-1)^{-a}\,b\in\mathbb{Z}.\end{cases}$$

Esercizio 10.

Verifichiamo che il prodotto di due elementi di G è ancora un elemento di G. Per ogni m_1,n_1,m_2,n_2 si ha

$$\frac{1+2m_1}{1+2n_1}\cdot\frac{1+2m_2}{1+2n_2}=\frac{1+2(m_1+m_2+2m_1m_2)}{1+2(n_1+n_2+2n_1n_2)}\in G.$$

Verifica delle proprietà dei gruppi.
Associativa: Per ogni m_1,n_1,m_2,n_2,m_3,n_3 si ha

$$\left(\frac{1+2m_1}{1+2n_1}\cdot\frac{1+2m_2}{1+2n_2}\right)\cdot\frac{1+2m_3}{1+2n_3} \;=\; \frac{1+2m_1}{1+2n_1}\cdot\left(\frac{1+2m_2}{1+2n_2}\cdot\frac{1+2m_3}{1+2n_3}\right).$$

Identità: Per ogni m,n si ha

$$\frac{1+2m}{1+2n}\cdot\frac{1+2\cdot0}{1+2\cdot0}=\frac{1+2m}{1+2n}.$$

Quindi l'identità per $(G,\cdot)$ è

$$\frac{1+2\cdot0}{1+2\cdot0}.$$

Inverso: Per ogni m,n si ha

$$\frac{1+2m}{1+2n}\cdot\frac{1+2n}{1+2m}=\frac{1+2\cdot0}{1+2\cdot0},$$

da cui

$$\left(\frac{1+2m}{1+2n}\right)^{-1}=\frac{1+2n}{1+2m}.$$

Commutatività: Per ogni m_1, n_1, m_2, n_2 si ha

$$\frac{1+2m_1}{1+2n_1} \cdot \frac{1+2m_2}{1+2n_2} = \frac{1+2m_2}{1+2n_2} \cdot \frac{1+2m_1}{1+2n_1}.$$

Esercizio 11.

Verifichiamo che il prodotto di due elementi di G è ancora un elemento di G. Infatti per ogni $t_1, t_2 \in \mathbb{R}$ si ha

$$\frac{1+it_1}{1-it_1} \cdot \frac{1+it_2}{1-it_2} = \frac{1-t_1t_2+i(t_1+t_2)}{1-t_1t_2-i(t_1+t_2)} = \frac{1+i\frac{t_1+t_2}{1-t_1t_2}}{1-i\frac{t_1+t_2}{1-t_1t_2}}.$$

L'ultimo passaggio è possibile se $1-t_1t_2 \neq 0$. Quindi la relazione sopra è verificata per ogni t_1, $t_2 \in \mathbb{R}$ tali che $t_1t_2 \neq 1$. Se invece $t_1t_2 = 1$ si ha che

$$\frac{1+it_1}{1-it_1} \cdot \frac{1+it_2}{1-it_2} = \frac{1-t_1t_2+i(t_1+t_2)}{1-t_1t_2-i(t_1+t_2)} = \frac{i(t_1+t_2)}{-i(t_1+t_2)} = -1.$$

Dobbiamo poi verificare che il prodotto di -1 per i termini del tipo $\dfrac{1+it}{1-it}$ con $t \in \mathbb{R}$ appartiene a G. Ovvero dimostriamo che esiste $s \in \mathbb{R}$ tale che

$$-1 \cdot \frac{1+it}{1-it} = \frac{1+is}{1-is} \tag{1}$$

Risolvendo l'equazione si ottiene che se $t \neq 0$ allora $s = \dfrac{-1}{t}$, mentre se $t = 0 : -1 \cdot 1 = -1 \in G$.
Un altro modo di procedere, ovviamente più complicato, ma che fornisce un'idea della struttura dell'insieme G è il seguente.
Per ogni $t \in \mathbb{R}$

$$\frac{1+it}{1-it} = \frac{(1+it)(1+it)}{(1-it)(1+it)} = \frac{(1+it)^2}{(1-it)(1+it)} = \frac{1-t^2}{1+t^2} + i\,\frac{2t}{1+t^2}$$

Posto

$$t = \tan\frac{\varphi}{2}$$

segue

$$\cos\varphi = \frac{1-t^2}{1+t^2}, \qquad \sin\varphi = \frac{2t}{1+t^2}.$$

Possiamo quindi scrivere:

$$\frac{1+it}{1-it} = \cos\varphi + i\sin\varphi.$$

Analogamente poniamo

$$\frac{1+is}{1-is} = \cos\theta + i\sin\theta.$$

Sostituendo queste relazioni in (1) otteniamo

$$-\cos\varphi - i\sin\varphi = \cos\theta + i\sin\theta \iff \begin{cases} -\cos\varphi &= \cos\theta \\ -\sin\varphi &= \sin\theta \end{cases}$$

Da cui $\theta = \varphi + \pi$.

Verifichiamo le proprietà dei gruppi.
Associativa: per ogni $t_1, t_2, t_3 \in \mathbb{R}$ si ha:

$$\left(\frac{1+it_1}{1-it_1} \cdot \frac{1+it_2}{1-it_2}\right) \cdot \frac{1+it_3}{1-it_3} = \frac{1+it_1}{1-it_1} \cdot \left(\frac{1+it_2}{1-it_2} \cdot \frac{1+it_3}{1-it_3}\right).$$

Identità: Per ogni $t \in \mathbb{R}$:

$$\frac{1+it}{1-it} \cdot \frac{1+i\cdot 0}{1-i\cdot 0} = \frac{1+it}{1-it}$$

Inverso: per ogni $t \in \mathbb{R}$:

$$\frac{1+it}{1-it} \cdot \frac{1+i(-t)}{1-i(-t)} = \frac{1+i\cdot 0}{1-i\cdot 0}.$$

Ovviamente l'inverso di -1 è -1.
Poiché i numeri complessi del tipo $\cos\varphi + i\sin\varphi$ hanno modulo 1, come conseguenza di quanto sopra dimostrato, l'insieme dei complessi di modulo unitario è un gruppo con il prodotto.

Esercizio 12.

$(G, \cdot)$ definito dalla tabella (a) è un gruppo. Infatti si vede che a è l'unica identità del gruppo, d è l'inverso di b e viceversa. c è l'inverso di c. La proprietà associativa è poi banalmente verificata.
$(G, \cdot)$ definito dalla tabella (b) non è un gruppo. Infatti osserviamo che $ab = b$ e $cb = b$ quindi
$ab = cb \iff abd = cbd \iff aa = ca = c \iff c = a$.

Esercizio 13.

Non è possibile completare la tabella in modo che $(G, \cdot)$ risulti un gruppo in quanto, essendo $ab = b$ e $ud = d$, si avrebbero due identità distinte nel gruppo.

Esercizio 14.

Osserviamo nella tabella che $ed = d$, questo implica che l'identità del gruppo è e. Possimo quindi scrivere:

$\cdot$	a	b	c	d	e
a	b	c			a
b	c				b
c					c
d					d
e	a	b	c	d	e

Nella prima riga dobbiamo determinare i prodotti ac e ad. Ovviamente non possiamo mettere come risultato un elemento già presente nella stessa riga, ad esempio $ac = b$ perché altrimenti si avrebbe, dal fatto che sappiamo che $aa = b$, $ac = aa$ da cui, moltiplicando per a^{-1}, $a = c$. Quindi si deve avere: $ac = d$ oppure $ac = e$ e $ad = e$ oppure $ad = d$. Non può essere $ad = d$ perché altrimenti a è l'identità, che invece, come abbiamo visto sopra è e. Allora si ha necessariamente $ad = e$ e quindi

$\cdot$	a	b	c	d	e
a	b	c	d	e	a
b	c				b
c	d				c
d	e				d
e	a	b	c	d	e

Osserviamo che da $aa = b$ segue $baa = bb$ e quindi, essendo $ba = c$, $ca = bb$, dalla tabella $ca = d$ onde $bb = d$. Nella seconda riga restano da inserire e ed a. Non puòo essere $db = e$ in quanto la prima riga stabilisce che $da = e$ ed allora si avrebbe che l'elemento d ammette due inversi. Possiamo allora scrivere

$\cdot$	a	b	c	d	e
a	b	c	d	e	a
b	c	d	e	a	b
c	d	e			c
d	e	a			d
e	a	b	c	d	e

Nella terza riga si debbono inserire gli elementi a e b. a va messo nella terza colonna perché è già presente nella quarta. Infine la tebella completa è

$\cdot$	a	b	c	d	e
a	b	c	d	e	a
b	c	d	e	a	b
c	d	e	a	b	c
d	e	a	b	c	d
e	a	b	c	d	e

Esercizio 15.

Osserviamo per prima cosa che il prodotto di due elementi di G è ancora un elemento di G :

$$(a + b\sqrt{2})(a_1 + b_1\sqrt{2}) = (aa_1 + 2bb_1) + (ab_1 + a_1b)\sqrt{2} \in G$$

Verifichiamo poi le proprietà dei gruppi.

Associativa:

$$[(a + b\sqrt{2})(a_1 + b_1\sqrt{2})](a_2 + b_2\sqrt{2}) = (a + b\sqrt{2})[(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})]$$

Identità: l'elemento $1 = 1 + 0\sqrt{2}$ appartiene a G e si ha

$$(a + b\sqrt{2})(1 + 0\sqrt{2}) = (a + b\sqrt{2})$$

Inverso: Per ogni $a + b\sqrt{2} \in G$ dobbiamo determinare un elemento di $x + y\sqrt{2}$ appartenente a G tale che:

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 + 0\sqrt{2}$$

ovvero

$$(ax + 2by) + (ay + bx)\sqrt{2} = 1 + 0\sqrt{2},$$

questo implica il dover risolvere il sistema

$$\begin{cases} ax + 2by &= 1 \\ ay + bx &= 0 \end{cases}$$

La soluzione è

$$x = \frac{a}{a^2 - 2b^2}, \qquad y = \frac{-b}{a^2 - 2b^2}$$

ossia

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Si noti che se $a^2 - 2b^2 \neq 0$ per ogni $a, b \in \mathbb{Q}$.

Esercizio 16.

Tabella relativa a $(\mathbb{Z}_4, +)$:

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Tabella relativa a $(\mathbb{Z}_5 \setminus \{[0]_5\}, \cdot)$:

$\cdot$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Definiamo $\varphi : (\mathbb{Z}_4, +) \longrightarrow (\mathbb{Z}_5 \setminus \{[0]_5\}, \cdot)$ nel modo seguente:

$$\begin{aligned} \varphi([0]_4) &= [1]_5 \\ \varphi([1]_4) &= [3]_5 \\ \varphi([2]_4) &= [4]_5 \\ \varphi([3]_4) &= [2]_5 \end{aligned}$$

φ è bigettiva ed è un omomorfismo, infatti osserviamo che ogni termine a di $(\mathbb{Z}_4, +)$ diverso da $[0]_4$ si può scrivere come
$a = \overbrace{[1]_4 + \cdots + [1]_4}^{n-\text{volte}} = n[1]_4$
Quindi $\varphi(a) = \varphi(n[1]_4) = ([3]_5)^n$.([1] Analogamente se $b \in (\mathbb{Z}_4, +)$ e $b = m[1]_4$ allora $\varphi(b) = \varphi(m[1]_4) = ([3]_5)^m$ Di conseguenza:
$\varphi(a + b) = \varphi((n + m)[1]_4) = ([3]_5)^{n+m} = ([3]_5)^n([3]_5)^m = \varphi(n[1]_4)\varphi(m[1]_4) = \varphi(a)\varphi(b)$.
D'altra parte $\varphi([0]_4 + a) = \varphi(a) = [1]_5\varphi(a) = \varphi(0)\varphi(a)$.

Esercizio 17.

Definiamo $\varphi : (\mathbb{Z}_9, +) \longrightarrow (\mathbb{Z}_3, +)$ nel modo seguente:

$$\begin{aligned} \varphi([0]_9) &= [0]_3 \\ \varphi([1]_9) &= [1]_3 \\ \varphi([2]_9) &= [2]_3 \\ \varphi([3]_9) &= [0]_3 \\ \varphi([4]_9) &= [1]_3 \\ \varphi([5]_9) &= [2]_3 \\ \varphi([6]_9) &= [0]_3 \\ \varphi([7]_9) &= [1]_3 \\ \varphi([8]_9) &= [2]_3 \end{aligned}$$

[1] Si dimostra facilmente per induzione.

Verifichiamo che si tratta di un omomorfismo. Ogni $a \in \mathbb{Z}_9$ diverso da $[0]_9$ si può scrivere come $a = \overbrace{[1]_9 + \cdots + [1]_9}^{n-\text{volte}} = n[1]_9$. Quindi se $b = m[1]_9$
$\varphi(a+b) = \varphi(n[1]_9 + m[1]_9) = \varphi((n+m)[1]_9) = (n+m)\varphi([1]_9) = (n+m)[1]_3 = n[1]_3 + m[1]_3 = n\varphi([1]_9) + m\varphi([1]_9) = \varphi(n[1]_9) + \varphi(m[1]_9) = \varphi(a) + \varphi(b)$.
Invece $\varphi([0]_9 + a) = \varphi(a) = [0]_3 + \varphi(a) = \varphi([0]_9) + \varphi(a)$.
Il nucleo dell'omomorfismo è:
$\ker\varphi = \{[0]_9, [3]_9, [6]_9\}$.

Esercizio 18.

Definiamo $\varphi : \{1, i, -1-i\} \longrightarrow (\mathbb{Z}_4, +)$ nel modo seguente:

$$\begin{aligned} \varphi(1) &= [0]_4 \\ \varphi(i) &= [1]_4 \\ \varphi(-1) &= [2]_4 \\ \varphi(-i) &= [3]_4 \end{aligned}$$

Osserviamo che:
$\varphi(1 \cdot i) = \varphi(i) = [1]_4 = [0]_4 + [1]_4 = \varphi(1) + \varphi(i)$.
$\varphi(-1 \cdot i) = \varphi(-i) = [3]_4 = [2]_4 + [1]_4 = \varphi(-1) + \varphi(i)$.
$\varphi(i \cdot (-i)) = \varphi(1) = [0]_4 = [1]_4 + [3]_4 = \varphi(i) + \varphi(-i)$.
$\varphi(-1 \cdot (-i)) = \varphi(i) = [1]_4 = [2]_4 + [3]_4 = \varphi(-1) + \varphi(-i)$.

Esercizio 19.

Per ogni $a, b \in G$ $\varphi(ab) = 1 = \varphi(a)\varphi(b)$. Notiamo che per ogni $a, b \in G$ si ha che $ab \in G$.
Osserviamo che $\ker\varphi = G$
Mentre

$$\begin{aligned} \psi(1) &= 1 \\ \psi(i) &= -1 \\ \psi(-1) &= 1 \\ \psi(-i) &= -1 \end{aligned}$$

Osserviamo che $\ker\psi = \{1, -1\}$

Esercizio 20.

Definiamo l'applicazione $f : G_2 \longrightarrow G_1$ nel modo seguente, per ogni $a, b \in \mathbb{Z}$

$$f(a + ib) = 3^a\, 5^b$$

Si vede facilmente che è biunivoca. Inoltre è un omomorfismo, in quanto posto: $f(a_1 + ib_1) = 3^{a_1}\, 5^{b_1}$, $f(a_2 + ib_2) = 3^{a_2}\, 5^{b_2}$, abbiamo

$$\begin{aligned} f((a_1 + ib_1) + (a_2 + ib_2)) &= f((a_1 + a_2) + i(b_1 + b_2)) = 3^{a_1+a_2}\, 5^{b_1+b_2} = (3^{a_1}\, 5^{b_1})(3^{a_2}\, 5^{b_2}) = \\ &= f(a_1 + ib_1) \cdot f(a_2 + ib_2). \end{aligned}$$

Esercizio 21.

Dalle ipotesi fatte, per ogni $a, b \in G$:

$$f(a) \otimes f(b) = f(a \times b) \in B.$$

Verifichiamo le proprietà dei gruppi.
Associatività: per ogni $a, b, c \in G$ risulta

$$(a \times b) \times c = a \times (b \times c) \Longrightarrow f((a \times b) \times c) = f(a \times (b \times c)) \Longrightarrow f(a \times b) \otimes f(c) = f(a) \otimes f(b \times c)$$

Da cui

$$[f(a) \otimes f(b)] \otimes f(c) = f(a) \otimes [f(b) \otimes f(c)].$$

Idenità: se e l'identità di $(G, \times)$ allora $f(e)$ è l'identità di $(B, \otimes)$, infatti per ogni $a \in G$ risulta

$$f(a) = f(a \times e) = f(a) \otimes f(e)$$

Inverso: per ogni $a \in G$ si ha:

$$a \times a^{-1} = e \Longrightarrow f(a \times a^{-1}) = f(e) \iff f(a) \otimes f(a^{-1}) = f(e)$$

Da cui deduciamo che

$$[f(a)]^{-1} = f(a^{-1}).$$