MAST30005 Algebra

Assignment 1 — 2017 Semester 1

Solutions

Question 1

(a)

We claim that the map

$$\begin{aligned} f\colon \qquad & G \longrightarrow N \times (G/N) \\ & g \longmapsto (p(g),\, gN) \end{aligned}$$

is a group homomorphism which satisfies the required conditions.

The map f is a group homomorphism, as we have

$$\begin{aligned} f(gh) &= (p(gh),\, (gh)N), \\ &= (p(g)p(h), (gN)(hN)) \\ &\quad \text{as } p \text{ is a group homomorphism and by the operation in the quotient group } G/N, \\ &= (p(g),\, gN)(p(h),\, hN) \\ &\quad \text{by the operation in the direct product,} \\ &= f(g)f(h), \end{aligned}$$

for any $g, h \in G$.

Moreover,

$$\forall n \in N, \quad f(n) = (p(n),\, nN) = (n, N),$$

where we have used the fact that $p(n) = n$ (as p is the left-inverse of inclusion of N into G) and $nN = N$ (as $n \in N$). (In the sequel we will use the fact that $p(n) = n$ for all $n \in N$ without comment.)

By construction, projection of $f(g)$ to the second factor is gN.

Thus f is a group homomorphism satisfying the required conditions.

(b) As we have shown f is a group homomorphism, it remains to show that f is a bijection. We will do this by constructing the inverse of f.

Suppose $m \in N$ and $h \in G$. We can derive the preimage of $(m,\, hN)$ (assuming that it exists). The preimage of $(m,\, hN)$ must be an element of the coset hN, so it must be of the form hn for some $n \in N$. Furthermore, by equality of the first factors, we require $p(hn) = m$, so that

$$p(hn) = p(h)p(n) = p(h)n = m \quad \Longrightarrow \quad n = p(h)^{-1}m.$$

This motivates the definition of the map

$$\begin{aligned} r\colon \qquad & N \times (G/N) \longrightarrow G \\ & (n,\, gN) \longmapsto g\, p(g)^{-1} n, \end{aligned}$$

which our work above suggests is the inverse of f.

We first note that $r(n, gN)$ is independent of the choice of representative for the coset gN. Indeed, as any representative of the coset gN is of the form gs for some $s \in N$, it is sufficient to show that $r(n, (gs)N)$ is invariant with respect to s. For any $s \in N$,

$$\begin{aligned} r(n,\, (gs)N) &= gs\, p(gs)^{-1} n, \\ &= gs\, p(s)^{-1} p(g)^{-1} n, \\ &= gss^{-1} p(g)^{-1} n, \\ &= g\, p(g)^{-1} n, \end{aligned}$$

1(b) (cont.) which does not depend on s, so our definition of r is sound.

We now wish to verify that $f \circ r = \mathrm{id}_{N\times(G/N)}$ and $r \circ f = \mathrm{id}_G$.

$$\begin{aligned}(f\circ r)(n,\, gN) &= f(g\,p(g)^{-1}n),\\ &= (p(g\,p(g)^{-1}n),\, (g\,p(g)^{-1}n)N),\\ &= (p(g)p(g)^{-1}n,\, gN),\\ &= (n,\, gN).\end{aligned}$$

$$\begin{aligned}(r\circ f)(g) &= r(p(g),\, gN),\\ &= gp(p(g))^{-1}p(g),\\ &= gp(g)^{-1}p(g),\\ &= g.\end{aligned}$$

Thus r is the inverse of f, which means that f is a group isomorphism.

(c) We rewrite the questions and answers as follows.

Reformulated questions

Let $N \trianglelefteq G$ be a normal subgroup, and assume that there exists a group homomorphism $p\colon G \longrightarrow N$ that is left inverse to the inclusion of N in G.

Define

$$G' \coloneqq N \times (G/N)$$

and subgroups of G'

$$N' \coloneqq \{(n,\, N) \mid n \in N\} \quad \text{and} \quad H \coloneqq \{(1_G,\, gN) \mid g \in G\}.$$

(a) Show that there exists a homomorphism $f\colon G \longrightarrow G'$ such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xhookrightarrow{\iota_1} & G & \xrightarrow{q_1} & G/N & \longrightarrow & 1\\ & & \cong\downarrow{\scriptstyle \phi_1} & & \vdots{\scriptstyle \exists f} & & \cong\downarrow{\scriptstyle \phi_2} & & \\ 1 & \longrightarrow & N' & \xhookrightarrow{\iota_2} & G' & \xrightarrow{q_2} & H & \longrightarrow & 1 \end{array}$$

commutes.

Note that the rows are short exact sequences. Here

- ι_1 and ι_2 are the natural inclusion mappings;
- $q_1\colon G \longrightarrow G/N$ is the quotient map;
- q_2 is the homomorphism $(n,\, gN) \longmapsto (1_G,\, gN)$ for all $n \in N$ and $g \in G$; and
- ϕ_1 and ϕ_2 are the canonical isomorphisms.

(b) Prove that G is isomorphic to G'.

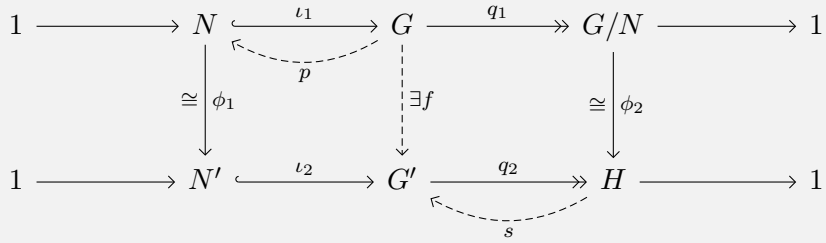
1(c) (cont.)

Reformulated answers

(a) Let $s\colon H \longrightarrow G'$ be the natural inclusion map. Then s is a right inverse group homomorphism of q_2, i.e. $q_2 \circ s = \mathrm{id}_H$.

By definition, p is a left inverse group homomorphism of ι_1, i.e. $p \circ \iota_1 = \mathrm{id}_N$.

We augment our diagram with s and p.



We claim that

$$\begin{aligned} f\colon \quad & G \longrightarrow G' \\ & g \longmapsto (p(g),\, gN) \end{aligned}$$

is a group homomorphism which allows the diagram to commute.

First, we check that $f \circ \iota_1 = \iota_2 \circ \phi_1$. Note that $(\iota_2 \circ \phi_1)(n) = (n, N)$ for all $n \in N$. In the original answer, we showed that $f(n) = (n, N)$ for all $n \in N$, so we indeed have $f \circ \iota_1 = \iota_2 \circ \phi_1$, noting that ι_1 is merely the inclusion map.

We now check that $\phi_2 \circ q_1 = q_2 \circ f$. Observe that

$$(\phi_2 \circ q_1)(g) = (1_G,\, gN) = q_2(p(g),\, gN) = q_2(f(g)) \quad \forall g \in G,$$

so that indeed $\phi_2 \circ q_1 = q_2 \circ f$.

In the original answer, it was already shown that f is a homomorphism, so we have a constructed a homomorphism that allows the diagram to commute.

(b) The original answer can be used verbatim. The significance here is the following: Given a short exact sequence of groups

$$1 \longrightarrow A \xrightarrow{\ i\ } B \xrightarrow{\ P\ } C \longrightarrow 1,$$

the existence of a right inverse group homomorphism for P only allows us to conclude that B is (isomorphic to) a semi-direct product of A and C.

In this question, we have shown that the existence of a left inverse group homomorphism for i allows us to conclude that B is (isomorphic to) the direct product of A and C; this is a much stronger statement.

Question 2

We will use the fact that the ring of Gaussian integers $\mathbf{Z}[i]$ is isomorphic to

$$G \coloneqq \mathbf{Z}\langle A\rangle/\langle A^2+1\rangle,$$

that is, the $\mathbf{Z}$-algebra generated by an alphabet of one letter $\{A\}$ with the relation A^2+1. A possible isomorphism $\phi_1 \colon G \longrightarrow \mathbf{Z}[i]$ is induced by setting $\phi_1(A) \coloneqq i$.

Similarly, the ring of integer quaternions $\mathbf{Z}[i,j,k]$ is isomorphic to

$$H \coloneqq \mathbf{Z}\langle A,B,C\rangle/\langle A^2+1, B^2+1, C^2+1, ABC+1\rangle,$$

that is, the $\mathbf{Z}$-algebra generated by the alphabet $\{A,B,C\}$ with relations $\{A^2+1, B^2+1, C^2+1, ABC+1\}$. A possible isomorphism $\phi_2 \colon H \longrightarrow \mathbf{Z}[i,j,k]$ is induced by setting

$$\phi_2(A) \coloneqq i, \qquad \phi_2(B) \coloneqq j, \quad \text{and} \quad \phi_2(C) \coloneqq k.$$

From the above ring presentations, by the universal property, we see that specifying a homomorphism from $\mathbf{Z}[i]$ to a ring R is equivalent to specifying an element $r \in R$ which satisfies $r^2 + 1_R = 0_R$ to become the image of i.

Similarly, specifying a homomorphism from $\mathbf{Z}[i,j,k]$ to a ring R is equivalent to specifying elements $r_1, r_2, r_3 \in R$ (not necessarily distinct) which satisfy

$$r_1^2 + 1_R = r_2^2 + 1_R = r_3^2 + 1_R = r_1 r_2 r_3 + 1_R = 0_R$$

to become the respective images of i, j, and k.

(a)

i. We seek possible images of i in $\mathbf{Z}[i]$.

Suppose $a, b \in \mathbf{Z}$ such that $(a+bi)^2 + 1 = 0$. We expand:

$$(a+bi)^2 + 1 = a^2 - b^2 + 1 + 2abi.$$

By comparing real and imaginary parts, we obtain the equations

$$a^2 - b^2 + 1 = 0 \quad \text{and} \quad 2ab = 0.$$

As $2ab = 0$, at least one of a and b is 0. From $a^2 - b^2 + 1 = 0$ we can conclude that $b^2 > a^2$, which means that b cannot be 0. Thus $a = 0$ and our equations simplify to

$$b^2 = 1 \quad \Longrightarrow \quad b = 1 \quad \text{or} \quad b = -1,$$

so that the only possible images of i are i or $-i$. (It is easy to verify that $i^2 + 1 = (-i)^2 + 1 = 0$.)

The ring homomorphisms from $\mathbf{Z}[i]$ to $\mathbf{Z}[i]$ are

$$\begin{array}{ccc} \mathbf{Z}[i] & \longrightarrow & \mathbf{Z}[i] \\ a+bi & \longmapsto & a+bi, \end{array} \quad \textbf{and} \quad \begin{array}{ccc} \mathbf{Z}[i] & \longrightarrow & \mathbf{Z}[i] \\ a+bi & \longmapsto & a-bi. \end{array}$$

ii. We seek possible images of i in $\mathbf{Z}[i,j,k]$.

Suppose $a_1, a_2, a_3, a_4 \in \mathbf{Z}$ such that $(a_1 + a_2 i + a_3 j + a_4 k)^2 + 1 = 0$. We expand (noting that a_1 commutes with everything so that we can place a_1 on the left of every term):

$$(a_1 + a_2 i + a_3 j + a_4 k)^2 + 1 = a_1^2 + 2a_1(a_2 i + a_3 j + a_4 k) + (a_2 i + a_3 j + a_4 k)^2 + 1.$$

Note that as multiplication between i, j, and k is anticommutative, we have

$$\begin{aligned}(a_2 i + a_3 j + a_4 k)^2 &= a_2^2 i^2 + a_2 a_3 ij + a_2 a_4 ik + a_3 a_2 ji + a_3^2 j^2 + a_3 a_4 jk + a_4 a_2 ki + a_4 a_3 kj + a_4^2 k^2,\\ &= -a_2^2 + a_2 a_3 k - a_2 a_4 j - a_3 a_2 k - a_3^2 + a_3 a_4 i + a_4 a_2 j - a_4 a_3 i - a_4^2,\\ &= -a_2^2 - a_3^2 - a_4^2 + (a_3 a_4 - a_4 a_3) i + (-a_2 a_4 + a_4 a_2) j + (a_2 a_3 - a_3 a_2) k,\\ &= -a_2^2 - a_3^2 - a_4^2,\end{aligned}$$

so that

$$(a_1 + a_2 i + a_3 j + a_4 k)^2 + 1 = a_1^2 - a_2^2 - a_3^2 - a_4^2 + 1 + 2a_1 a_2 i + 2a_1 a_3 j + 2a_1 a_4 k.$$

We now have the equations

$$a_1^2 - a_2^2 - a_3^2 - a_4^2 + 1 = 0, \qquad 2a_1 a_2 = 0, \qquad 2a_1 a_3 = 0, \quad \text{and} \quad 2a_1 a_4 = 0.$$

If $a_1 \neq 0$ then a_2, a_3, and a_4 are all 0, so that $a_1^2 - a_2^2 - a_3^2 - a_4^2 + 1 = a_1^2 + 1 = 0$, which is not possible as $a_1^2 \geq 0$. So $a_1 = 0$.

We now have

$$a_2^2 + a_3^2 + a_4^2 = 1,$$

which means each of a_2, a_3, and a_4 is either -1, 0, or 1, as otherwise the left hand side would be too great. They cannot all be 0, however.

If $a_2 \in \{-1, 1\}$, then $a_3^2 + a_4^2 = 0$ so that $a_3 = a_4 = 0$. By symmetry exactly one of a_2, a_3, and a_4 is non-zero, i.e. one of the three is 1 or -1, and the other two are both 0.

It follows that the possible images of i are

$$i, \qquad -i, \qquad j, \qquad -j, \qquad k, \quad \text{and} \quad -k,$$

and it is simple to verify that $u^2 + 1 = 0$ for any $u \in \{i, -i, j, -j, k, -k\}$.

Hence, the ring homomorphisms from $\mathbf{Z}[i]$ to $\mathbf{Z}[i,j,k]$ are

$$\begin{aligned}\mathbf{Z}[i] &\longrightarrow \mathbf{Z}[i,j,k] & \mathbf{Z}[i] &\longrightarrow \mathbf{Z}[i,j,k] & \mathbf{Z}[i] &\longrightarrow \mathbf{Z}[i,j,k]\\ a + bi &\longmapsto a + bi, & a + bi &\longmapsto a + bj, & a + bi &\longmapsto a + bk,\end{aligned}$$

$$\begin{aligned}\mathbf{Z}[i] &\longrightarrow \mathbf{Z}[i,j,k] & \mathbf{Z}[i] &\longrightarrow \mathbf{Z}[i,j,k] & \text{and} \quad \mathbf{Z}[i] &\longrightarrow \mathbf{Z}[i,j,k]\\ a + bi &\longmapsto a - bi, & a + bi &\longmapsto a - bj, & a + bi &\longmapsto a - bk,\end{aligned}$$

iii. We seek possible images for each of i, j, and k in $\mathbf{Z}[i]$.

Suppose $\{a_i\}_{i=1}^3 \subseteq \mathbf{Z}$ and $\{b_i\}_{i=1}^3 \subseteq \mathbf{Z}$ such that

$$(a_1 + b_1 i)^2 + 1 = (a_2 + b_2 i)^2 + 1 = (a_3 + b_3 i)^2 + 1 = (a_1 + b_1 i)(a_2 + b_2 i)(a_3 + b_3 i) + 1 = 0.$$

As $(a_1 + b_1 i)^2 + 1$, $(a_2 + b_2 i)^2 + 1$, and $(a_3 + b_3 i)^2 + 1$ are all 0, from part i we know that

$$a_1 = a_2 = a_3 = 0 \quad \text{and} \quad b_1, b_2, b_3 \in \{-1, 1\}.$$

2(a)iii (cont.) The equation $(a_1 + b_1 i)(a_2 + b_2 i)(a_3 + b_3 i) + 1 = 0$ becomes

$$(b_1 i)(b_2 i)(b_3 i) + 1 = 0 \quad \Longrightarrow \quad -b_1 b_2 b_3 i + 1 = 0.$$

This is impossible as b_1, b_2, and b_3 are all integers.

Hence there are no ring homomorphisms from $\mathbf{Z}[i, j, k]$ to $\mathbf{Z}[i]$.

iv. We seek possible images for each of i, j, and k in $\mathbf{Z}[i, j, k]$.

Suppose $f\colon \mathbf{Z}[i, j, k] \longrightarrow \mathbf{Z}[i, j, k]$ is a ring homomorphism.

From our work in part ii we know that

$$f(i),\ f(j),\ f(k) \in \{i,\ -i,\ j,\ -j,\ k,\ -k\} =: U$$

is necessary and sufficient in order for

$$f(i)^2 + 1 = f(j)^2 + 1 = f(k)^2 + 1 = 0$$

to hold.

It remains to determine possible values for each of $f(i)$, $f(j)$, and $f(k)$ such that $f(i)f(j)f(k) + 1 = 0$.

Lemma 1

Suppose a, b, and c are elements of $U = \{i, -i, j, -j, k, -k\}$. Then $abc + 1 = 0$ if and only if $b \in U \setminus \{a, -a\}$ and $c = ab$.

Proof

We will use without comment the fact that $u^2 = -1$ for all $u \in U$.

($\Rightarrow$) Suppose $abc + 1 = 0$. First of all, note that it is possible to have such elements $a, b, c \in U$ (e.g. $(a, b, c) = (i, j, k)$).

Necessarily,

$$\begin{aligned} abc &= -1, & bc &= a, & -ab &= a^2 c, \\ a^2 bc &= -a, & bc^2 &= ac, & -ab &= -c, \\ -bc &= -a, & -b &= ac, & c &= ab. \end{aligned}$$

Note that $b \in \{a, -a\}$ implies $c = ab \notin U$, so we must also have $b \in U \setminus \{a, -a\}$.

($\Leftarrow$) A substitution allows us to see that $c = ab$ is sufficient:

$$(ab)c + 1 = c^2 + 1 = 0.$$

□

From our lemma, we know that f satisfies

$$f(i),\ f(j),\ f(k) \in U, \qquad f(j) \in U \setminus \{f(i), -f(i)\}, \quad \text{and} \quad f(k) = f(i)f(j),$$

giving 24 possibilities for f, because any set map from $\{i, j, k\}$ to $\mathbf{Z}[i, j, k]$ which satisfies these conditions can be uniquely extended to become an endomorphism of $\mathbf{Z}[i, j, k]$ (consequence of the universal property).

To generate all 24 possibilities:

2(a)iv (cont.)

1. Designate $f(i)$ to be any of the 6 elements in U.
2. Designate $f(j)$ to be any of the 4 elements in $U \setminus \{f(i), -f(i)\}$.
3. Designate $f(k)$ to be $f(i)f(j) \in U$.

(b) In this question we will use the result that a group homomorphism is injective if and only if it has a trivial kernel.

Lemma 2

Let A and B be groups, and suppose $f\colon A \longrightarrow B$ is a group homomorphism. Then f is injective if and only if $\ker(f) \subseteq A$ is the set $\{1_A\}$.

Proof

Observe that, for all $h, k \in A$,

$$f(h) = f(k) \iff f(h)f(k)^{-1} = 1_B \iff f(hk^{-1}) = 1_B \iff hk^{-1} \in \ker(f).$$

($\Rightarrow$) Suppose f is injective.

$$\begin{aligned} m \in \ker(f) &\implies (\forall h \in A)\,(f(h)f(m) = f(h)), \\ &\implies (\forall h \in A)\,(f(hm) = f(h)), \\ &\implies (\forall h \in A)\,(hm = h) && \text{as } f \text{ is injective}, \\ &\implies m = 1_A. \end{aligned}$$

Hence $\ker(f) \subseteq \{1_A\}$. Because $\ker(f)$ is non-empty ($f(1_A) = 1_B$), we have $\ker(f) = \{1_A\}$.

($\Leftarrow$) Suppose $\ker(f) = \{1_A\}$.

Let h and k be elements of A such that $f(h) = f(k)$. Then $hk^{-1} \in \ker(f)$. As 1_A is the only element of $\ker(f)$, we have $hk^{-1} = 1_A$, so that $h = k$.

Hence f is injective. □

i. $\mathbf{Z}[i] \longrightarrow \mathbf{Z}[i]$

Map induced by	Automorphism	Endomorphism	Kernel	Image
$i \longmapsto i$	Yes	Yes	$\{0\}$	$\mathbf{Z}[i]$
$i \longmapsto -i$	Yes	Yes	$\{0\}$	$\mathbf{Z}[i]$

As these are ring homomorphisms from $\mathbf{Z}[i]$ to $\mathbf{Z}[i]$, both maps are endomorphisms (the domain and codomain are the same).

The first is the identity map on $\mathbf{Z}[i]$, so it is naturally an automorphism with the trivial kernel and $\mathbf{Z}[i]$ as its image.

Observe that the second is an involution, which means it is actually a ring isomorphism. Hence it is an automorphism with the trivial kernel and $\mathbf{Z}[i]$ as its image.

ii. $\mathbf{Z}[i] \longrightarrow \mathbf{Z}[i,j,k]$

Map induced by	Automorphism	Endomorphism	Kernel	Image
$i \longmapsto i$	No	No	$\{0\}$	$\{a+bi \mid a,b \in \mathbf{Z}\}$
$i \longmapsto -i$	No	No	$\{0\}$	$\{a+bi \mid a,b \in \mathbf{Z}\}$
$i \longmapsto j$	No	No	$\{0\}$	$\{a+bj \mid a,b \in \mathbf{Z}\}$
$i \longmapsto -j$	No	No	$\{0\}$	$\{a+bj \mid a,b \in \mathbf{Z}\}$
$i \longmapsto k$	No	No	$\{0\}$	$\{a+bk \mid a,b \in \mathbf{Z}\}$
$i \longmapsto -k$	No	No	$\{0\}$	$\{a+bk \mid a,b \in \mathbf{Z}\}$

As the domain and codomain are different, none of the maps are endomorphisms, and none of the maps are automorphisms.

All the maps are injective because two elements in $\mathbf{Z}[i,j,k]$ are equal if and only if their real, i-, j-, and k-parts are respectively equal.

For example, consider the homomorphism $f\colon \mathbf{Z}[i] \longrightarrow \mathbf{Z}[i,j,k]$ where $f(i) = -k$.

Suppose $a,b,c,d \in \mathbf{Z}$ such that $f(a+bi) = f(c+di)$.

We have $f(a+bi) = a - bk$ and $f(c+di) = c - dk$, and

$$a - bk = c - dk \quad \Longrightarrow \quad (a=c) \wedge (-b=-d) \quad \Longrightarrow \quad (a=c) \wedge (b=d) \implies a+bi = c+di,$$

so that f is injective and by Lemma 2 must therefore have trivial kernel.

iii. $\mathbf{Z}[i,j,k] \longrightarrow \mathbf{Z}[i]$

In (a) part iii we showed that there are no such ring homomorphisms.

iv. $\mathbf{Z}[i,j,k] \longrightarrow \mathbf{Z}[i,j,k]$

As the domain and codomain are the same set, all 24 homomorphisms are endomorphisms.

We claim that all 24 ring homomorphisms are actually isomorphisms, from which it will follow that all 24 ring homomorphisms are automorphisms, have kernel $\{0\}$ (by Lemma 2), and have image $\mathbf{Z}[i,j,k]$.

Suppose that $f\colon \mathbf{Z}[i,j,k] \longrightarrow \mathbf{Z}[i,j,k]$ is one of the 24 ring homomorphisms.

Define

$$U \coloneqq \{i,\ -i,\ j,\ -j,\ k,\ -k\} \quad \text{and} \quad V \coloneqq \{i,\ j,\ k\}.$$

We will show that $\operatorname{im}(f|_U) = U$ and, following that, that there exists a ring homomorphism g such that $f \circ g = g \circ f = \mathrm{id}_{\mathbf{Z}[i,j,k]}$.

2(b)iv (cont.)

Lemma 3

Suppose a, b, and c are elements of $U = \{i, -i, j, -j, k, -k\}$ such that $abc + 1 = 0$. Then

$$U = \{a, -a, b, -b, c, -c\}.$$

Proof

From Lemma 1, we know that a, $-a$, b, and $-b$ must be distinct elements of U. Partitioning U as

$$U = V \cup \{-v \mid v \in V\},$$

we see that there must exist distinct $v_1, v_2 \in V = \{i, j, k\}$ such that

$$\{a, -a, b, -b\} = \{v_1, -v_1, v_2, -v_2\}.$$

This is possible because

$$b \neq a \quad \text{and} \quad b \neq -a.$$

Without loss of generality, suppose that v_1 and v_2 are such that

$$\{a, -a\} = \{v_1, -v_1\} \quad \text{and} \quad \{b, -b\} = \{v_2, -v_2\}.$$

Let v_3 be the element of V distinct from v_1 and v_2.

From Lemma 1, we know that $c = ab$. Because $\{v_1v_2, -v_1v_2\} = \{v_3, -v_3\}$ (a consequence of the multiplication of unit quaternions), we necessarily have that

$$\{c, -c\} = \{v_3, -v_3\}.$$

Thus

$$U = \{a, -a, b, -b, c, -c\}$$

as required. □

Showing $\mathrm{im}(f|_U) = U$

From Lemma 1 and Lemma 3, we can see that

$$\{f(i), -f(i), f(j), -f(j), f(k), -f(k)\} = U.$$

We can show that the left-hand side is indeed $\mathrm{im}(f|_U)$. We will use the fact that $f(-1) = -1$, which we now show.

$$\begin{aligned} f(0) &= 0 && (f(0) = f(0+0) = f(0) + f(0) \implies f(0) = 0), \\ f(-1+1) &= 0, \\ f(-1) + f(1) &= 0, \\ f(-1) + 1 &= 0 && \text{as } f(1) = 1 \text{ for all ring homomorphisms}, \\ f(-1) &= -1. \end{aligned}$$

2(b)iv (cont.)

With this we can see that

$$\begin{aligned}\mathrm{im}(f|_U) &= \{f(i),\, f(-i),\, f(j),\, f(-j),\, f(k),\, f(-k)\},\\ &= \{f(i),\, f(-1)f(i),\, f(j),\, f(-1)f(j),\, f(k),\, f(-1)f(k)\},\\ &= \{f(i),\, -f(i),\, f(j),\, -f(j),\, f(k),\, -f(k)\},\\ &= U.\end{aligned}$$

This completes the proof that $\mathrm{im}(f|_U) = U$.

Now, consider the sequence of ring homomorphisms

$$f,\, f\circ f,\, f\circ f\circ f,\, \ldots$$

We will denote

$$f^n \coloneqq \underbrace{f\circ\cdots\circ f}_{n\ f\text{'s}},\quad n\in\mathbf{N}.$$

Note that f^n is an endomorphism of $\mathbf{Z}[i,j,k]$ for all $n\in\mathbf{N}$.

From (a) part iv we determined that there were 24 endomorphisms of $\mathbf{Z}[i,j,k]$. This means that by the pigeonhole principle, the first 25 terms

$$\{f^n\}_{n=1}^{25}$$

necessarily contain at least two terms which are the same endomorphism of $\mathbf{Z}[i,j,k]$. Thus there exist $r,s\in\mathbf{N}$ satisfying $r+s\leq 25$ and

$$f^r = f^{r+s}.$$

We can show that $f^s = \mathrm{id}_{\mathbf{Z}[i,j,k]}$.

Observe that as a corollary of the universal property, any set map

$$\begin{aligned}V=\{i,j,k\} &\longrightarrow \mathbf{Z}[i,j,k]\\ i &\longmapsto r_1\\ j &\longmapsto r_2\\ k &\longmapsto r_3,\end{aligned}$$

satisfying

$$r_1^2+1 = r_2^2+1 = r_3^2+1 = r_1r_2r_3+1 = 0$$

extends uniquely to become an endomorphism of $\mathbf{Z}[i,j,k]$.

Call all such set maps *basic*.

Because $f^r = f^{r+s}$,

$$f^s(f^r(u)) = f^r(u)\quad \forall u\in U.$$

Because $\mathrm{im}(f|_U) = U$, we also have $\mathrm{im}(f^r|_U) = U$, so that, as set maps,

$$f^s|_U = \mathrm{id}_U,$$

implying in particular

$$f^s|_V = \mathrm{id}_V,$$

because $V\subset U$. From this we see that $f^s|_V$ is basic, because id_V is basic. That $f^s|_V$ is basic is consistent with f^s being an endomorphism of $\mathbf{Z}[i,j,k]$.

2(b)iv (cont.) Thus we have the equivalence of basic set maps

$$f^s|_V = \mathrm{id}_V = \mathrm{id}_{\mathbf{Z}[i,j,k]}|_V$$

which implies that

$$f^s = \mathrm{id}_{\mathbf{Z}[i,j,k]}$$

because both f^s and $\mathrm{id}_{\mathbf{Z}[i,j,k]}$ are endomorphisms of $\mathbf{Z}[i,j,k]$ and, when restricted to V, are the same basic set map.

If $s = 1$, then $f = \mathrm{id}_{\mathbf{Z}[i,j,k]}$ and f is an isomorphism.

Otherwise, if $s > 1$, we see that

$$f \circ f^{s-1} = f^{s-1} \circ f = \mathrm{id}_{\mathbf{Z}[i,j,k]},$$

meaning that f^{s-1} is the inverse of f, proving that f is an isomorphism.

As f was any of the 24 ring homomorphisms, all 24 ring homomorphisms are automorphisms, have kernel $\{0\}$, and have image $\mathbf{Z}[i,j,k]$.

Question 3

(a) Every element in A has order 1, 2, or 4.

This is because, for any $(r, s, t) \in A$,

$$4(r, s, t) = (4r, 4s, 4t) = (0, 0, 0),$$

so that the order of (r, s, t) must be a divisor of 4. The last equality follows from the fact that every element in $\mathbf{Z}/4\mathbf{Z}$ has an order which divides 4.

We present A as

$$\langle a, b, c \mid a^4 = b^4 = c^4 = 1,\ ab = ba,\ ac = ca,\ bc = cb \rangle,$$

where we identify

$$\begin{array}{lll} a & \text{with} & (1, 0, 0), \\ b & \text{with} & (0, 1, 0), \text{ and} \\ c & \text{with} & (0, 0, 1). \end{array}$$

As a corollary of the universal property, specifying an endomorphism of A is equivalent to specifying images x, y, and z in A for a, b, and c respectively such that

$$x^4 = y^4 = z^4 = 1, \qquad xy = yx, \qquad xz = zx, \quad \text{and} \quad yz = zy.$$

As A is abelian it is equivalent to seek x, y, and z such that

$$x^4 = y^4 = z^4 = 1.$$

This is, in turn, equivalent to specifying any three elements $x, y, z \in A$, because all elements in A have an order which divides 4.

Thus any set map from $\{a, b, c\}$ to A extends uniquely to an endomorphism of A.

As the endomorphisms of A are naturally $\mathbf{Z}/4\mathbf{Z}$-linear, we can represent each endomorphism uniquely as a 3×3 matrix with entries in $\mathbf{Z}/4\mathbf{Z}$ (i.e. an element of $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$). Specifically, we represent $g \in \mathrm{End}(A)$ as the matrix

$$\begin{bmatrix} | & | & | \\ g(a) & g(b) & g(c) \\ | & | & | \end{bmatrix},$$

that is, the matrix where the columns are the coordinates of $g(a)$, $g(b)$, and $g(c)$.

This means that application of $g \in \mathrm{End}(A)$ to an element $(r, s, t) \in A$ is equivalent to the matrix multiplication

$$\begin{bmatrix} | & | & | \\ g(a) & g(b) & g(c) \\ | & | & | \end{bmatrix} \begin{bmatrix} r \\ s \\ t \end{bmatrix}.$$

In the reverse direction, every $m \in M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$ represents a unique endomorphism of A: it is the unique endomorphism extension of the set map

3(a) (cont.)

$$\begin{aligned} \{a,b,c\} &\longrightarrow A \\ a &\longmapsto m \begin{bmatrix}1\\0\\0\end{bmatrix} \\ b &\longmapsto m \begin{bmatrix}0\\1\\0\end{bmatrix} \\ c &\longmapsto m \begin{bmatrix}0\\0\\1\end{bmatrix}. \end{aligned}$$

We have actually specified a ring isomorphism between $\mathrm{End}(A)$, where multiplication is composition and addition is point-wise addition, and $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$, where multiplication is matrix multiplication and addition is entry-wise addition. The multiplicative identity of $\mathrm{End}(A)$ is id_A which in our construction corresponds to I_3 (the 3×3 identity matrix), which is the multiplicative identity in $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$.

Thus we may identify $\mathrm{End}(A)$ as the ring $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$.

(b) Equipping A with the structure of a $\mathbf{Z}[S_3]$-module is equivalent to finding a ring homomorphism between $\mathbf{Z}[S_3]$ and $\mathrm{End}(A) \cong M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$. Specifying a ring homomorphism from $\mathbf{Z}[S_3]$ to $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$ is in turn equivalent to specifying a monoid homomorphism from S_3 to the monoid $(M_{3\times 3}(\mathbf{Z}/4\mathbf{Z}), \cdot)$.

Note that S_3 is in fact a group as well as a monoid, so the image of any monoid homomorphism from S_3 to $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$ will actually be a group. In particular, all elements in the image will have left and right inverses, so it is equivalent to consider group homomorphisms from S_3 to $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})^\times$, the group of all units in the ring $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})$.

We can use the following group presentation of S_3 to further investigate the group homomorphisms from S_3 to $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})^\times$:

$$\langle a,\, b \mid a^2 = b^2 = (ab)^3 = 1 \rangle.$$

Each group homomorphism from S_3 to $M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})^\times$ corresponds uniquely to an ordered pair (A, B) where $A, B \in M_{3\times 3}(\mathbf{Z}/4\mathbf{Z})^\times$, $A^2 = B^2 = I$ and $(AB)^3 = I$.

Question 4

(a) As $\mathbf{Z}$ is the free group generated by one letter, which we identify as $1 \in \mathbf{Z}$, any endomorphism of $\mathbf{Z}$ is completely specified by the image of 1.

Every $g \in \mathrm{End}(\mathbf{Z})$ is of the form

$$\begin{aligned} \mathbf{Z} &\longrightarrow \mathbf{Z} \\ n &\longmapsto kn \end{aligned}$$

for some $k \in \mathbf{Z}$.

This is because

$$\begin{aligned} g(1) = k \quad &\implies \quad g(\underbrace{1+1+\cdots+1}_{n \text{ 1's}}) = \underbrace{k+k+\cdots+k}_{n \text{ } k\text{'s}}, \quad n \in \mathbf{N} \\ &\implies \quad g(n) = kn, \quad n \in \mathbf{N} \\ g(1) = k \quad &\implies \quad g(-1) = -g(1) = -k \\ &\implies \quad g(\underbrace{-1+(-1)+\cdots+(-1)}_{n \text{ } -1\text{'s}}) = \underbrace{-k+(-k)+\cdots+(-k)}_{n \text{ } -k\text{'s}}, \quad n \in \mathbf{N} \\ &\implies \quad g(-n) = -kn, \quad n \in \mathbf{N} \end{aligned}$$

and $g(0) = 0$.

In particular, every element in $\mathrm{im}(g)$ is an integer multiple of $g(1)$, so if $\mathrm{im}(g) = \mathbf{Z}$ then $g(1) = 1$ or $g(1) = -1$. (If this were not the case, then $|g(1)|+1 \notin \mathrm{im}(g)$, because $|g(1)|+1$ is never an integer multiple of $g(1)$ when $|g(1)| \neq 1$.)

If $g(1) = 1$, then $g = \mathrm{id}_{\mathbf{Z}}$, so that $\mathrm{im}(g) = \mathbf{Z}$.

If $g(1) = -1$, then g is an involution, so that g is an isomorphism and $\mathrm{im}(g) = \mathbf{Z}$.

So $\mathrm{Aut}(\mathbf{Z}) = \{g \in \mathrm{End}(\mathbf{Z}) \mid g(1) \in \{1, -1\}\}$. This is isomorphic to the cyclic group of order 2, because we noted before that for $g \in \mathrm{End}(\mathbf{Z})$, $g(1) = 1$ implies $g = \mathrm{id}_{\mathbf{Z}}$ and $g(1) = -1$ implies $g^2 = \mathrm{id}_{\mathbf{Z}}$.

(b) The set of actions on $\mathbf{Z}$ by $\mathbf{Z}$ are in bijection with the set of group homomorphisms $\mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z})$.

As $\mathbf{Z}$ is the free group generated by one letter, which we identify as 1, specifying such a group homomorphism is equivalent to specifying an image of 1 in $\mathrm{Aut}(\mathbf{Z})$. There are only 2 elements in $\mathrm{Aut}(\mathbf{Z})$, so there are 2 actions.

Let $f \in \mathrm{Aut}(\mathbf{Z})$ be the automorphism with $f(1) = -1$.

One possible action on $\mathbf{Z}$ by $\mathbf{Z}$ is given by the homomorphism specified by $1 \longmapsto \mathrm{id}_{\mathbf{Z}}$, which is the trivial homomorphism, as $\mathrm{id}_{\mathbf{Z}}$ is the identity element of $\mathrm{Aut}(\mathbf{Z})$. The other is specified by $1 \longmapsto f$.

$1 \longmapsto \mathrm{id}_{\mathbf{Z}}$

This action is:

$k \in \mathbf{Z}$ acts on $n \in \mathbf{Z}$ to produce

$$k \cdot n := \begin{cases} \underbrace{(\mathrm{id}_{\mathbf{Z}} \circ \mathrm{id}_{\mathbf{Z}} \circ \cdots \circ \mathrm{id}_{\mathbf{Z}})}_{k \text{ times}}(n) = n, & k \in \mathbf{N}, \\ \underbrace{(\mathrm{id}_{\mathbf{Z}}^{-1} \circ \mathrm{id}_{\mathbf{Z}}^{-1} \circ \cdots \circ \mathrm{id}_{\mathbf{Z}}^{-1})}_{-k \text{ times}}(n) = n, & k \in \mathbf{Z}_{<0}, \\ \mathrm{id}_{\mathbf{Z}}(n) = n, & k = 0. \end{cases}$$

4(b) (cont.) That is, the result is n regardless of k.

$1 \longmapsto f$

This action is:

$k \in \mathbf{Z}$ acts on $n \in \mathbf{Z}$ to produce

$$k \cdot n := \begin{cases} \underbrace{(f \circ f \circ \cdots \circ f)}_{k \text{ times}}(n) = (-1)^k n, & k \in \mathbf{N}, \\ \underbrace{(f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1})}_{-k \text{ times}}(n) = (-1)^k n, & k \in \mathbf{Z}_{<0}, \\ \mathrm{id}_{\mathbf{Z}}(n) = n, & k = 0. \end{cases}$$

That is, $k \cdot n = (-1)^k n$.

(c) $\varrho \colon \mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z})$, $\varrho(1) = \mathrm{id}_{\mathbf{Z}}$

The semi-direct product is

$$\mathbf{Z} \rtimes_{\varrho} \mathbf{Z} = \{(n,\, h) \mid n, h \in \mathbf{Z}\}$$

with operation

$$(n,\, h) * (m,\, k) = (n + \varrho(h)(m),\, h + k) = (n + m, h + k).$$

This operation is associative, as addition in $\mathbf{Z}$ is associative.

The identity is $(0, 0)$, and inverses are given by $(n, h)^{-1} = (-n, -h)$.

This semi-direct product is precisely the direct product $\mathbf{Z} \times \mathbf{Z}$, so it is generated by $(1, 0)$ and $(0, 1)$, resulting in the presentation

$$\langle a,\, b \mid ab = ba \rangle.$$

$\varrho \colon \mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z})$, $\varrho(1) = f$

The semi-direct product is

$$\mathbf{Z} \rtimes_{\varrho} \mathbf{Z} = \{(n,\, h) \mid n, h \in \mathbf{Z}\}$$

with operation

$$(n,\, h) * (m,\, k) = (n + \varrho(h)(m),\, h + k) = (n + (-1)^h m, h + k).$$

The identity is $(0, 0)$:

$$\begin{aligned} (0,\, 0) * (n,\, h) &= (0 + (-1)^0 n,\, 0 + h), \\ &= (n,\, h). \\ (n,\, h) * (0,\, 0) &= (n + (-1)^h (0),\, h + 0), \\ &= (n,\, h). \end{aligned}$$

Inverses are given by $(n, h)^{-1} = (-(-1)^{-h} n, -h)$:

$$\begin{aligned} (-(-1)^{-h} n,\, -h) * (n,\, h) &= (-(-1)^{-h} n + (-1)^{-h} n,\, -h + h), \\ &= (0,\, 0). \\ (n,\, h) * (-(-1)^{-h} n,\, -h) &= (n - (-1)^h (-1)^{-h} n,\, h + (-h)), \\ &= (0,\, 0). \end{aligned}$$

4(c) (cont.) We will show that $(n,h) = (1,0)^n * (0,1)^h$ for all $n,h \in \mathbf{Z}$, so that this semi-direct product can be generated by two letters.

Note that for all $n,h \in \mathbf{Z}$

$$(n,\,0) * (0,\,h) = (n + (-1)^0(0),\, 0+h) = (n,\,h).$$

We claim that $\{(n,0) \mid n \in \mathbf{Z}\} \subseteq \langle (1,0) \rangle$. Noting that the inverse of $(1,0)$ is $(-1,0)$, for any $n \in \mathbf{N}_0$,

$$\begin{aligned}(1,\,0) * (n,\,0) &= (1 + (-1)^0 n,\, 0+0),\\ &= (n+1,\,0).\\ (-1,\,0) * (-n,\,0) &= (-1 + (-1)^0(-n),\, 0+0),\\ &= (-(n+1),\,0).\end{aligned}$$

As $(0,0) \in \langle (1,0) \rangle$, we are done by mathematical induction.

We claim that $\{(0,h) \mid h \in \mathbf{Z}\} \subseteq \langle (0,1) \rangle$. Noting that the inverse of $(0,1)$ is $(0,-1)$, for any $h \in \mathbf{N}_0$,

$$\begin{aligned}(0,\,1) * (0,\,h) &= (0 + (-1)(0),\, 1+h),\\ &= (0,\,h+1).\\ (0,\,-1) * (0,\,-h) &= (0 + (-1)^{-1}(0),\, -1 + (-h)),\\ &= (0,\,-(h+1)).\end{aligned}$$

As $(0,0) \in \langle (0,1) \rangle$, we are done by mathematical induction.

Altogether, we have that any element in $\mathbf{Z} \rtimes_\varrho \mathbf{Z}$ can be written as

$$x * y, \quad \text{where } x \in \langle (1,0) \rangle \text{ and } y \in \langle (0,1) \rangle,$$

so that it is possible to present $\mathbf{Z} \rtimes_\varrho \mathbf{Z}$ with two generators.

Our relations needs to encode the operation

$$(n,\,h) * (m,\,k) = (n + \varrho(h)(m),\, h+k) = (n + (-1)^h m,\, h+k)$$

or

$$(1,\,0)^n * (0,\,1)^h * (1,\,0)^m * (0,\,1)^k = (1,\,0)^{n+(-1)^h m} * (0,\,1)^{h+k}.$$

Identifying a with $(1,0)$ and b with $(0,1)$, it can be shown that this operation can be encoded by the relation $bab^{-1} = a^{-1}$. That is,

$$bab^{-1} = a^{-1} \quad \iff \quad (\forall n,h,m,k \in \mathbf{Z})\,(a^n b^h a^m b^k = a^{n+(-1)^h m} b^{h+k}).$$

Thus our presentation for $\mathbf{Z} \rtimes_\varrho \mathbf{Z}$ is

$$\langle a,\, b \mid bab^{-1} = a^{-1} \rangle.$$

What follows are proofs that the relation encodes the operation of the semi-direct product.

$bab^{-1} = a^{-1} \quad \iff \quad (\forall n,h,m,k \in \mathbf{Z})\,(a^n b^h a^m b^k = a^{n+(-1)^h m} b^{h+k})$

($\Leftarrow$) Setting $n=0$, $h=1$, $m=1$, and $k=-1$:

$$a^0 bab^{-1} = a^{0+(-1)(1)} b^{1+(-1)} = a^{-1} \quad \implies \quad bab^{-1} = a^{-1}.$$

($\Rightarrow$) First note that

$$bab^{-1} = a^{-1} \quad \implies \quad (bab^{-1})^{-1} = a^{(-1)^2} \quad \implies \quad ba^{-1}b^{-1} = a$$

4(c) (cont.)

so that

$$ba^{(-1)^m}b^{-1} = a^{(-1)^{m+1}} \quad \forall m \in \mathbf{Z}. \tag{1}$$

We next show that $b^h ab^{-h} = a^{(-1)^h}$ for all $h \in \mathbf{Z}$.

$b^h ab^{-h} = a^{(-1)^h}$ for all $h \in \mathbf{Z}$

It is true for $h = 0$.

Suppose it is true for $h = t$ and $h = -t$ for some $t \in \mathbf{N}_0$.

$$\begin{aligned}
b^{t+1}ab^{-(t+1)} &= b(b^t ab^{-t})b^{-1}, \\
&= ba^{(-1)^t}b^{-1} && \text{by the induction hypothesis,} \\
&= a^{(-1)^{t+1}}. \\
b^{-t-1}ab^{-(-t-1)} &= b^{-1}(b^{-t}ab^{-(-t)})b, \\
&= b^{-1}a^{(-1)^{-t}}b && \text{by the induction hypotheis,} \\
&= b^{-1}a^{(-1)^{(-t-1)+1}}b, \\
&= b^{-1}ba^{(-1)^{-t-1}}b^{-1}b && \text{by (1),} \\
&= a^{(-1)^{-t-1}}
\end{aligned}$$

So the induction hypothesis is also true for $h = t + 1$ and $h = -t - 1$.

By mathematical induction, we have that $b^h ab^{-h} = a^{(-1)^h}$ for all $h \in \mathbf{Z}$.

We next show that $b^h a^m b^{-h} = a^{(-1)^h m}$ for all $h, m \in \mathbf{Z}$.

$b^h a^m b^{-h} = a^{(-1)^h m}$ for all $h, m \in \mathbf{Z}$

It is true for $m = 0$ and $h \in \mathbf{Z}$ and $m = 1$ and $h \in \mathbf{Z}$ (by the last induction proof).

Suppose it is true when $m = t$ and $h \in \mathbf{Z}$ and when $m = -t$ and $h \in \mathbf{Z}$ for some $t \in \mathbf{N}_0$.

$$\begin{aligned}
b^h a^t b^{-h} &= a^{(-1)^h t}, \\
(b^h a^t b^{-h})(b^h ab^{-h}) &= (a^{(-1)^h t})(a^{(-1)^h}) && \text{by the induction hypothesis for } m = 1 \text{ and } h \in \mathbf{Z}, \\
b^h a^{t+1} b^{-h} &= a^{(-1)^h (t+1)}.
\end{aligned}$$

$$\begin{aligned}
b^h a^{-t} b^{-h} &= a^{(-1)^h (-t)}, \\
b^h a^{-t-1} ab^{-h} &= a^{(-1)^h (-t)}, \\
b^h a^{-t-1} b^{-h} b^h ab^{-h} &= a^{(-1)^h (-t)}, \\
b^h a^{-t-1} b^{-h} (a^{(-1)^h}) &= a^{(-1)^h (-t)} && \text{by the induction hypothesis for } m = 1 \text{ and } h \in \mathbf{Z}, \\
b^h a^{-t-1} b^{-h} &= a^{(-1)^h (-t-1)}.
\end{aligned}$$

So the induction hypothesis is also true when $m = t + 1$ and $h \in \mathbf{Z}$ and when $m = -t - 1$ and $h \in \mathbf{Z}$.

By mathematical induction, we have that $b^h a^m b^{-h} = a^{(-1)^h m}$ for all $h, m \in \mathbf{Z}$.

4(c) (cont.) Now, for any $n \in \mathbf{Z}$,

$$b^h a^m b^{-h} = a^{(-1)^h m} \implies a^n b^h a^m b^{-h} = a^{n+(-1)^h m} \implies a^n b^h a^m b^{-h} b^{h+k} = a^{n+(-1)^h m} b^{h+k},$$

so that we finally have

$$a^n b^h a^m b^k = a^{n+(-1)^h m} b^{h+k} \quad \forall n, h, m, k \in \mathbf{Z}.$$

(d) $\varrho\colon \mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z})$, $\varrho(1) = \mathrm{id}_{\mathbf{Z}}$

In this case the semi-direct product $\mathbf{Z} \rtimes_\varrho \mathbf{Z}$ is the direct product $\mathbf{Z} \times \mathbf{Z}$.

The direct product $\mathbf{Z} \times \mathbf{Z}$ is the free abelian group on two generators, so it is isomorphic to the quotient of the free group on $\{a, b\}$ by the normal closure of $aba^{-1}b^{-1}$.

Let F be the free group on $\{a, b\}$. Then

$$\mathbf{Z} \times \mathbf{Z} \cong F/S,$$

where S is the normal closure of $\langle aba^{-1}b^{-1} \rangle$ in F.

We can describe S in more detail: S is actually the commutator subgroup of F, that is, the subgroup $\langle A \rangle < F$, where $A \coloneqq \{xyx^{-1}y^{-1} \mid x, y \in F\}$.

$S = \langle A \rangle$

Since F/S is abelian, we must have

$$(\forall x, y \in F)\,((xy)S = (yx)S)$$

which is equivalent to

$$(\forall x, y \in F)\,(xy(yx)^{-1} = xyx^{-1}y^{-1} \in S),$$

so that $\langle A \rangle \subseteq S$, since $A \subseteq S$ and S is a subgroup.

By an alternative characterisation of normal closures, S is the subgroup generated by all elements in F that are conjugate to $aba^{-1}b^{-1}$. That is, $S = \langle B \rangle$, where $B \coloneqq \{waba^{-1}b^{-1}w^{-1} \mid w \in F\}$

Observe that for any $w \in F$,

$$\begin{aligned} waba^{-1}b^{-1}w^{-1} &= wa(w^{-1}w)b(w^{-1}w)a^{-1}(w^{-1}w)b^{-1}w^{-1}, \\ &= (waw^{-1})(wbw^{-1})(wa^{-1}w^{-1})(wb^{-1}w^{-1}), \\ &= (waw^{-1})(wbw^{-1})(waw^{-1})^{-1}(wbw^{-1})^{-1}, \end{aligned}$$

which is an element of A. Hence $B \subseteq A$, so that $\langle B \rangle = S \subseteq \langle A \rangle$.

Because $\langle A \rangle \subseteq S \subseteq \langle A \rangle$, we have $S = \langle A \rangle$ as required.

$\varrho\colon \mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z})$, $\varrho(1) = f$

The semi-direct product $\mathbf{Z} \rtimes_\varrho \mathbf{Z}$ has the presentation

$$\langle a,\, b \mid bab^{-1} = a^{-1} \rangle.$$

Let F be the free group on $\{a, b\}$. Then

$$\mathbf{Z} \rtimes_\varrho \mathbf{Z} \cong F/S,$$

where S is the normal closure of $\langle abab^{-1} \rangle$ in F, that is,

$$S = \langle \{wabab^{-1}w^{-1} \mid w \in F\} \rangle.$$