ALGEBRA MAST30005 ASSIGNMENT 1 2017

JON XU

Contents

Date: May 10, 2017.

These are solutions and mark allocation for Assignment 1 of Nora Ganter's MAST30005 Algebra course, written by Jon Xu, tutor for the Thursday 3:15PM practise class.

Any constructive comments are welcome, my email address is

jyxu[at]student.unimelb.edu.au.

Mark distribution:

Q1: (a) 3 (b) 3 (c) 2

Q2: (a) 5 (b) 2

Q3: (a) 2 (b) 2 [bonus]

Q4: (a) 2 (b) 2 (c),(d) 4.

Total marks: 25 (plus up to 2 extra marks for 3b).

General comments:

- If you received 0-15 marks, you should: make sure to attempt all questions, revise definitions, learn vocabulary and examples - what is a ring? a ring homomorphism? a ring isomorphism? is $\mathbb{Z}$ isomorphic to $\mathbb{Z}/10\mathbb{Z}$? Why/ why not? What are the examples of groups in our course that were constructed by semidirect products? Keep asking questions like these and work them out thoroughly using a pen and paper.
- If you received 15-20 marks, you should: read the email exchange below, rewrite your assignment while clarifying your writing - how can you make your writing more concise while maintaining its impact/logic/flow?
- If you received 20+ marks, you should: read the email exchange below

Below is an email exchange from my PhD supervisor which has been highly influential with respect to how I think about mathematical writing. I've highlighted what I think are the key paragraphs in italics.

On 12/02/2013, at 9:48 PM, Jon Xu wrote:

> Dear Arun,
>
> Just something I wanted to clarify:
>
> You wrote: '(1) On "The orbit stabilizer theorem". The word "clearly" should not be used in mathematics proofs. Its only purpose is to create errors and unhappy readers. The only reason for its use is because some authors are too lazy to actually write the proof propoerly.
>
> (3) In your Twisted F4.pdf, (b) I don't like the "(after some calculation)" very much. Find a nice quick short way to display this calculation in a way that can be followed by the reader without interrupting the overall flow of the presentation.'
>
> I'm trying to understand the objection to using words like 'clearly' or 'a quick calculation shows that...'. To me, it signposts to the reader that something has been omitted to save space and maintain the flow of the writing, and that it's something that can be resolved by the reader in his/her own time. What's the problem with this? The alternatives seem to be to explicitly write out the omitted step (which wastes time and space), or to not mention that a step

has been omitted (which seems disingenuous). I've received similar criticism in assignments at USyd, but I never really understood it.

Best wishes, Jon

On Thu, Mar 7, 2013 at 6:23 PM, Arun Ram wrote:

Dear Jon,

This one is difficult for me to do over email. *Writing is something that takes lots of practice and thought and more practice and more thought and even more practice and even more thought, followed by some further practice.*

It is a challenge to reach your readers. It is a challenge to get any readers at all. It is difficult to keep the readers that you do get for more than a a paragraph or two. Great writing achieves all of these, and make the reader feel happily satisfied afterwards. We can always improve our writing.

On a baser note, to get a job, you need some people with money to read your work and find it useful and satisfying. These people tend to have very little time, so if you are expecting them to do anything on their own time then you are expecting them not to do it all all, because they don't have any of their own time. I think that's the heart of difficulty of the "leaving to the reader" issue.

I can work with you on the good questions you are asking (how to make your writing flow and still be complete and thorough and transparent) but it is easier for me to do this by having you write something up in TeX, me marking it up, and then us sitting together and my showing you and discussing how I would rewrite it to try to improve it for the reader. I don't have all the answers and I still struggle daily with my own writing, but I have put lots of thought into this process and tried to improve over the 20 years that I have been writing mathematics. So I can try to help, little by little. Perhaps a good goal is that you have a first draft of a thesis starting to be in place by June, and then when we both get back to Melbourne we can go through it line by line and hash through all the thoughts and considerations that go into improving each line, the structure, the formats and the overall look (all of which are important in the end).

tt is also helpful to have good models. Do a search for the word "clear" in some of my more recent papers. Then have a look at places where you think that I might have wanted to use that word. How was it avoided? Was the solution helpful to the reader? Did the solution disrupt the flow? What were the positives and negatives of this solution? Do the positives outweigh the negatives in the context?

Some of my favourite models for writing are Deligne, Macdonald and Grothendieck. I read their writing often so that I have their style running through my head (Like Beethoven Symph 3 runs through my head when I've been listening to it lots). It helps me when I'm writing to emulate their style and techniques.

Best, Arun

Question 1

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

Part (a). Show that there exists a group homomorphism $f\colon G \to N \times (G/N)$ satisfying

- $f(n) = (n, N)$ for all $n \in N$,
- $(pr_2 \circ f)(g) = gN$ for all $g \in G$,

where pr_2 denotes the projection to the second factor.

Solution: (3 marks). Define $f\colon G \to N \times (G/N)$ by

$$f(g) = (p(g), gN)$$

for $g \in G$.

To show:

(1) f is a homomorphism,
(2) f satisfies the two properties given in the question.

(1) Let $g, h \in G$. Then

$$\begin{aligned} f(g)f(h) &= (p(g), gN)(p(h), hN) \\ &= (p(g)p(h), gN \cdot hN) \\ &= (p(gh), gN \cdot hN) \quad \text{since } p\colon G \to N \text{ is a homomorphism} \\ &= (p(gh), ghN) \quad \text{by definition of multiplication on } G/N. \end{aligned}$$

So f is a homomorphism.

(2) Let $n \in N$. Then

$$\begin{aligned} f(n) &= (p(n), nN) \\ &= (p(n), N) \quad \text{since } n \in N, \\ &= (p \circ i(n), N) \quad \text{since } i(n) = n, \\ &= (n, N). \end{aligned}$$

Let $g \in G$. Then

$$\begin{aligned} (pr_2 \circ f)(g) &= pr_2(p(g), gN) \\ &= gN \end{aligned}$$

Part (b). Prove that the homomorphism F you constructed in part (a) is in fact an isomorphism.

Solution: (3 marks). To show: $f\colon G \to N \times (G/N)$ is a bijection

To show:

(1) f is surjective,
(2) f is injective.

(1) Let $(n, hN) \in N \times (G/N)$.
To show: There exists $g \in G$ such that $f(g) = (n, hN)$.
Let

$$g = hp(h^{-1})n.$$

Then

$$\begin{aligned} f(g) &= (p(hp(h^{-1})n), hp(h^{-1})nN) \\ &= (p(hp(h^{-1})n), hN) \quad \text{since } n \in N \text{ and } p(h^{-1}) \in N \\ &= (p(h)p \circ p(h^{-1})p(n), hN) \\ &= (p(h)p(h^{-1})p(n), hN) \quad \text{since } p \circ p = p \\ &= (p(n), hN) \\ &= (n, hN) \quad \text{since } p(n') = n' \text{ for all } n' \in N. \end{aligned}$$

(2) Let $g \in ker f$. To show: $g = 1$.
We know $f(g) = (1, N)$. So $(p(g), gN) = (1, N)$. So $gN = N$. So $g \in N$.
Hence $p(g) = g$. But $p(g) = 1$, so $g = 1$.

Part (c). Reformulate the questions and answers above in terms of short exact sequences.

Solution: (2 marks, many ways to answer this). Let G be a group and N be a normal subgroup. The following is an exact sequence:

$$1 \to N \xrightarrow{i} G \xrightarrow{\psi} G/N \to 1.$$

where

$$\begin{array}{rccc} i\colon & N & \hookrightarrow & G \\ & n & \mapsto & n, \end{array}$$

is the inclusion map, and

$$\begin{array}{rccc} \psi\colon & G & \hookrightarrow & G/N \\ & g & \mapsto & gN, \end{array}$$

is the projection map. The assumption of question 1 says that we assume there exists a map $p\colon G \to N$ such that $(p \circ i)(n) = n$ for all $n \in N$. In the language of homological algebra, this means that short exact sequence

$$1 \to N \underset{p}{\overset{i}{\rightleftarrows}} G \xrightarrow{\psi} G/N \to 1. \tag{1}$$

is *left split*. We have shown in part a) and b) that this implies

$$G \cong N \times (G/N).$$

This proves one of the implications of the *splitting lemma*. See [Lan05, III. §3, Proposition 3.2].

Question 2

Let $\mathbb{Z}[i]$ be the ring of Gaussian integers, and $\mathbb{Z}[i, j, k]$ the ring of integer quaternions.

Part (a). Find all ring homomorphisms

(1) from $\mathbb{Z}[i]$ to $\mathbb{Z}[i]$,
(2) from $\mathbb{Z}[i]$ to $\mathbb{Z}[i,j,k]$,
(3) from $\mathbb{Z}[i,j,k]$ to $\mathbb{Z}[i]$, and
(4) from $\mathbb{Z}[i,j,k]$ to $\mathbb{Z}[i,j,k]$.

Solution: (5 marks). Some key technical facts we use in this question are mentioned below. See [Bou98, Chapter III, §2.8]. Let R be a $\mathbb{Z}$-algebra and assume that R is finitely generated. Then R has a presentation

$$R = \mathbb{Z}\langle\{x_1, x_2, \ldots, x_n\}\rangle/\langle p_1, p_2, \ldots, p_k\rangle$$

If R' is a $\mathbb{Z}$-algebra and $\hat{\psi}\colon \mathbb{Z}\langle\{x_1, x_2, \ldots, x_n\}\rangle \to R'$ is a homomorphism of $\mathbb{Z}$-algebras such that $\{p_1, p_2, \ldots, p_k\} \subseteq ker\hat{\psi}$ then there exists a unique homomorphism $\psi\colon R \to R'$ such that

$$\psi(q) = \hat{\psi}(q)$$

for all $q \in \mathbb{Z}\langle\{x_1, x_2, \ldots, x_n\}\rangle$. Furthermore, every $\mathbb{Z}$-algebra homomorphism $\psi\colon R \to R'$ arises in this way. Note that every $\mathbb{Z}$-algebra homomorphism $R \to R'$ is a homomorphism of rings, and conversely every ring homomorphism $R \to R'$ is a homomorphism of $\mathbb{Z}$-algebras.

(1) We know (or, by definition),

$$\mathbb{Z}[i] = \mathbb{Z}\langle\{x\}\rangle/\langle x^2 + 1\rangle.$$

Every homomorphism $\psi\colon \mathbb{Z}[i] \to \mathbb{Z}[i]$ arises from a homomorphism $\hat{\psi}\colon \mathbb{Z}\langle\{x\}\rangle \to \mathbb{Z}[i]$ such that $x^2 + 1 \in \ker\hat{\psi}$. From the universal property of free $\mathbb{Z}$-algebras, $\hat{\psi}$ is uniquely determined by $\hat{\psi}(x)$.

Suppose $\hat{\psi}(x) = a + bi$ for some $a, b \in \mathbb{Z}$. Since $x^2 + 1 \in \ker\hat{\psi}$, we have $\hat{\psi}(x)^2 + 1 = 0$. So

$$a^2 - b^2 + 1 + 2abi = 0.$$

So

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

So $a = 0$ or $b = 0$. We show that $b \neq 0$. Suppose for the sake of contradiction that $b = 0$. Then $a^2 + 1 = 0$, but there does not exist $a \in \mathbb{Z}$ such that $a^2 + 1 = 0$. So $b \neq 0$, hence $a = 0$.

Since $-b^2 + 1 = 0$, we have $b = 1$ or $b = -1$. So $\hat{\psi}(x) = i$ or $\hat{\psi}(x) = -i$. Therefore

$$\begin{array}{rcl}\psi_1\colon \mathbb{Z}[i] & \to & \mathbb{Z}[i] \\ a + bi & \mapsto & a + bi,\end{array} \text{ and } \begin{array}{rcl}\psi_2\colon \mathbb{Z}[i] & \to & \mathbb{Z}[i] \\ a + bi & \mapsto & a - bi,\end{array}$$

are all the homomorphisms $\mathbb{Z}[i] \to \mathbb{Z}[i]$.

(2) We know (or, by definition),

$$\mathbb{Z}[i,j,k] = \mathbb{Z}\langle\{x,y,z\}\rangle/\langle x^2 + 1, y^2 + 1, z^2 + 1, xyz + 1\rangle.$$

Every homomorphism $\psi\colon \mathbb{Z}[i] \to \mathbb{Z}[i,j,k]$ arises from a homomorphism $\hat{\psi}\colon \mathbb{Z}\langle\{x\}\rangle \to \mathbb{Z}[i,j,k]$ such that $x^2 + 1 \in \ker\hat{\psi}$. From the universal property of free $\mathbb{Z}$-algebras, $\hat{\psi}$ is uniquely determined by $\hat{\psi}(x)$.

Suppose $\hat{\psi}(x) = a + bi + cj + dk$ for some $a, b, c, d \in \mathbb{Z}$. Since $x^2 + 1 \in \ker\hat{\psi}$, we have $\hat{\psi}(x)^2 + 1 = 0$. So

$$(a + bi + cj + dk)^2 + 1 = 0.$$

So

$$(a^2 - b^2 - c^2 - d^2 + 1) + (2ab)i + (2ac)j + (2ad)k = 0.$$

So

$$a^2 - b^2 - c^2 - d^2 + 1 = 2ab = 2ac = 2ad = 0.$$

If $b = c = d = 0$ then $a^2 + 1 = 0$, which does not hold for any $a \in \mathbb{Z}$. Hence $b \neq 0$ or $c \neq 0$ or $d \neq 0$. So $a = 0$ and $b^2 + c^2 + d^2 = 1$. The possible solutions for $b, c, d \in \mathbb{Z}$ are

$$\begin{aligned} b = 1, c = 0, d = 0, \\ b = -1, c = 0, d = 0, \\ b = 0, c = 1, d = 0, \\ b = 0, c = -1, d = 0, \\ b = 0, c = 0, d = 1, \\ b = 0, c = 0, d = -1. \end{aligned} \tag{2}$$

The maps

$$\begin{array}{rcl} \psi\colon \mathbb{Z}[i] & \to & \mathbb{Z}[i, j, k] \\ \alpha + \beta i & \mapsto & \alpha + \beta(bi + cj + dk), \end{array}$$

where b, c, d are as in Equation 2, give all the homomorphisms $\mathbb{Z}[i] \to \mathbb{Z}[i, j, k]$. There are 6 in total.

(3) Every homomorphism $\psi\colon \mathbb{Z}[i, j, k] \to \mathbb{Z}[i]$ arises from a homomorphism $\hat{\psi}\colon \mathbb{Z}\langle\{x, y, z\}\rangle \to \mathbb{Z}[i]$ such that

$$\{x^2 + 1, y^2 + 1, z^2 + 1, xyz + 1\} \subseteq \ker(\hat{\psi})$$

From the universal property of free $\mathbb{Z}$-algebras, $\hat{\psi}$ is uniquely determined by the tuple $(\hat{\psi}(x), \hat{\psi}(y), \hat{\psi}(z))$. Then $\hat{\psi}(x)^2 + 1 = 0$. So $\hat{\psi}(x) = \varepsilon_1 i$ for some $\varepsilon_1 \in \{-1, 1\}$. Similarly, $\hat{\psi}(y) = \varepsilon_2 i$ and $\hat{\psi}(z) = \varepsilon_3 i$ for some $\varepsilon_2, \varepsilon_3 \in \{-1, 1\}$.

Since $xyz + 1 \in \ker(\hat{\psi})$, we have

$$\hat{\psi}(x)\hat{\psi}(y)\hat{\psi}(z) + 1 = 0.$$

So

$$\varepsilon_1 i \varepsilon_2 i \varepsilon_3 i + 1 = 0.$$

So

$$-\varepsilon_1\varepsilon_2\varepsilon_3 i + 1 = 0,$$

which has no solutions for $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{-1, 1\}$. Hence there are no homomorphisms $\mathbb{Z}[i, j, k] \to \mathbb{Z}[i]$.

(4) Every homomorphism $\mathbb{Z}[i, j, k] \to \mathbb{Z}[i, j, k]$ arises from a homomorphism $\hat{\psi}\colon \mathbb{Z}\langle\{x, y, z\}\rangle \to \mathbb{Z}[i, j, k]$ such that

$$\{x^2 + 1, y^2 + 1, z^2 + 1, xyz + 1\} \subseteq \ker(\hat{\psi}).$$

From the universal property of free $\mathbb{Z}$-algebras, $\hat{\psi}$ is uniquely determined by the tuple $(\hat{\psi}(x), \hat{\psi}(y), \hat{\psi}(z))$. Suppose

$$\hat{\psi}(x) = a + bi + cj + dk \in \mathbb{Z}[i, j, k].$$

Then $\hat{\psi}(x)^2 + 1 = 0$. As shown in part ii) of the question, this implies

$$\hat{\psi}(x) \in \{i, -i, j, -j, k, -k\}.$$

Similiarly

$$\hat{\psi}(y), \hat{\psi}(z) \in \{i, -i, j, -j, k, -k\}. \tag{3}$$

Since $xyz+1 \in \ker(\hat{\psi})$, we have

$$\hat{\psi}(x)\hat{\psi}(y)\hat{\psi}(z)+1=0 \tag{4}$$

There are 6 choices for $\hat{\psi}(x)$. If $\hat{\psi}(y) \in \{\hat{\psi}(x), -\hat{\psi}(x)\}$, then by Equation 4, $\varepsilon\hat{\psi}(z)+1=0$ for some $\varepsilon \in \{-1,1\}$, contradicting Equation 3. Hence

$$\hat{\psi}(y) \in \{i,-i,j,-j,k,-k\}\backslash\{\hat{\psi}(x),\hat{\psi}(x)\},$$

so that there are 4 choices for $\hat{\psi}(y)$. Given choices of $\hat{\psi}(x)$ and $\hat{\psi}(y)$, the element $\hat{\psi}(z)$ is uniquely determined. So there are 24 homomorphisms $\mathbb{Z}[i,j,k] \to \mathbb{Z}[i,j,k]$.

Part (b). For each of your answers in (a) indicate which are endomorphisms, which are automorphisms, what are the respective kernels and images.

Solution: (2 marks). By definition of endomorphism, the homomorphisms $\mathbb{Z}[i] \to \mathbb{Z}[i]$, $\mathbb{Z}[i,j,k] \to \mathbb{Z}[i,j,k]$ are endomorphisms, i.e those in part i) and iv) are endomorphisms, those in part ii) and part iii) are not endomorphisms. All endomorphisms in part i) and iv) are automorphisms. Therefore, for the homomorphisms in part i) and iv), the kernels are $\{0\}$ and the images are the entire codomain. There are no homomorphisms in part iii). The kernels for the homomorphisms in part ii) are $\{0\}$, and the images of the homomorphisms corresponding to 2 are, respectively, $\mathbb{Z}[i], \mathbb{Z}[i], \mathbb{Z}[j], \mathbb{Z}[j], \mathbb{Z}[k], \mathbb{Z}[k]$.

Question 3

Let $A = (\mathbb{Z}/4\mathbb{Z})^3$.

Part (a). Identify the endomorphism ring of A.

Solution: (2 marks). Let $A = (\mathbb{Z}/4\mathbb{Z})^3$. Then

$$\begin{aligned}\mathrm{End}(A) &= \{f\colon A \to A \mid f \text{ is a homomorphism of groups }\}\\ &= \{f\colon A \to A \mid f \text{ is a } \mathbb{Z}/4\mathbb{Z}\text{-module homomorphism}\}.\end{aligned}$$

Note that A is the free $\mathbb{Z}/4\mathbb{Z}$-module on $\{e_1,e_2,e_3\}$. The universal property of free $\mathbb{Z}/4\mathbb{Z}$-modules says that if M is a $\mathbb{Z}/4\mathbb{Z}$-module and $\psi\colon \{e_1,e_2,e_3\} \to M$ is a function then there exists a unique homomorphism $\phi\colon A \to M$ such that $\psi = \phi \circ i$ where $i\colon \{e_1,e_2,e_3\} \hookrightarrow A$ is the inclusion map. Furthermore, every homomorphism $\phi\colon A \to M$ arises in this way. In other words, we have a bijection

$$\begin{array}{ccc}\mathrm{Hom}_{\mathrm{sets}}(\{e_1,e_2,e_3\},M) & \longleftrightarrow & \mathrm{Hom}_{\mathbb{Z}/4\mathbb{Z}\text{-modules}}(A,M)\\ \psi & \longmapsto & \phi.\end{array}$$

Letting $M=A$, we have a bijection

$$\begin{array}{ccc}\mathrm{Hom}_{\mathrm{sets}}(\{e_1,e_2,e_3\},A) & \longleftrightarrow & \mathrm{End}_{\mathbb{Z}/4\mathbb{Z}\text{-modules}}(A)\\ \psi & \longmapsto & \phi.\end{array}$$

An element $\psi \in \mathrm{Hom}_{\mathrm{sets}}(\{e_1,e_2,e_3\},A)$ is uniquely specified by a 3×3 matrix

$$\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}$$

where $a_{ij} \in \mathbb{Z}/4\mathbb{Z}$ and

$$\psi(e_1) = a_{11}e_1 + a_{21}e_2 + a_{31}e_3$$

$$\psi(e_2) = a_{12}e_1 + a_{22}e_2 + a_{32}e_3$$
$$\psi(e_3) = a_{13}e_1 + a_{23}e_2 + a_{33}e_3.$$

So $\mathrm{End}(A) \cong \mathrm{Mat}_{3\times 3}(\mathbb{Z}/4\mathbb{Z})$.

Part (b). Identify all possible ways to equip A with the structure of a module over the group algebra $\mathbb{Z}[S_3]$. Justify your answer.

Solution: (up to 2 bonus marks, though the maximum is still 25). A complete answer would give a classification of all $\mathbb{Z}[S_3]$-module structures on A up to isomorphism. I do not have a complete answer to this.

The question amounts to finding group homomorphisms $S_3 \to GL_3(\mathbb{Z}/4\mathbb{Z})$. We know

$$S_3 = \langle x, y \mid x^2 = y^2 = (xy)^3 = 1\rangle.$$

So a function $\psi\colon S_3 \to GL_3(\mathbb{Z}/4\mathbb{Z})$ is a homomorphism if and only if

$$\psi(x)^2 = \psi(y)^2 = (\psi(x)\psi(y))^3 = 1.$$

Calculating the possible $\psi(x)$ and $\psi(y)$ can be done on a computer program, which some students have done.

I believe this question could make a good start to a vacation scholarship/masters project (though first verify this with somebody more senior than myself!)

Now, I give a sketch of the answer to an easier and more 'mainstream' version of the question. We find all possible module structures of $\mathbb{C}^3$ over $\mathbb{C}[S_3]$. There is a good theory that can be used to answer this question efficiently. See any introductory book on representation theory (e.g [FH91]) for the missing details. A module M is *simple* if its only submodules are $\{0\}$ and M. There are exactly 3 simple finite dimensional $\mathbb{C}[S_3]$-modules. Specifically, let $M_1 = \mathbb{C}$, $M_2 = \mathbb{C}$, $M_3 = \mathbb{C}^2$, and define the action of S_3

$$\text{on } M_1, \text{ by } (12) = [1] \text{ and } (23) = [1],$$

$$\text{on } M_2, \text{ by } (12) = [-1] \text{ and } (23) = [-1],$$

$$\text{on } M_3, \text{ by } (12) = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } (23) = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}.$$

Then there are 6 possible ways of defining a $\mathbb{C}[S_3]$-module structure on $\mathbb{C}^3$ (up to isomorphism), given by the number of ways to direct sum the M_i to give $\mathbb{C}^3$. These are:

$$M_1 \oplus M_1 \oplus M_1$$
$$M_1 \oplus M_1 \oplus M_2$$
$$M_1 \oplus M_2 \oplus M_1$$
$$M_2 \oplus M_1 \oplus M_1$$
$$M_1 \oplus M_3$$
$$M_2 \oplus M_3.$$

More generally, these tools (which I have not explained) can be used to find all possible $\mathbb{C}[G]$-module structures on $\mathbb{C}^N$, where G is a finite group.

Question 4

In this question $\mathbb{Z}$ refers to the abelian group $(\mathbb{Z}, +)$.

Part (a). Identify the group of (group) automorphisms of $\mathbb{Z}$.

Solution (2 marks). Since $\mathbb{Z}$ is the free group on 1 generator, every homomorphism $\psi\colon \mathbb{Z} \to \mathbb{Z}$ is uniquely determined by $\psi(1)$, and every homomorphism arises in this way. A homomorphism $\psi\colon \mathbb{Z} \to \mathbb{Z}$ is bijective if and only $\psi(1) \in \{1, -1\}$. So there are exactly 2 automorphisms of $\mathbb{Z}$, defined below:

$$\begin{array}{rcl} \psi_1\colon \mathbb{Z} & \longrightarrow & \mathbb{Z}, \\ n & \longmapsto & n, \end{array} \quad \text{and} \quad \begin{array}{rcl} \psi_{-1}\colon \mathbb{Z} & \longrightarrow & \mathbb{Z}, \\ n & \longmapsto & -n. \end{array}$$

So $\mathrm{Aut}(\mathbb{Z}) = \{\psi_1, \psi_{-1}\}$. Furthermore, $\psi_{-1} \circ \psi_{-1} = \psi_1$, so

$$\mathrm{Aut}(\mathbb{Z}) \cong \{-1, 1\}.$$

Part (b). Find all possible actions of $\mathbb{Z}$ on itself.

Solution (2 marks). An *action* of a group G on another group H is a homomorphism $\rho\colon G \to \mathrm{Aut}(H)$. So an action of $\mathbb{Z}$ on $\mathbb{Z}$ is a homomorphism $\rho\colon \mathbb{Z} \to \{\psi_{-1}, \psi_1\}$. By the universal property of free abelian groups, any such homomorphism ρ is uniquely determined by $\rho(1)$, and every homomorphism $\rho\colon \mathbb{Z} \to \{\psi_{-1}, \psi_1\}$ arises in this way. Hence there are two actions of $\mathbb{Z}$ on $\mathbb{Z}$, given by

$$\begin{array}{rcl} \rho_1\colon \mathbb{Z} & \longrightarrow & \{\psi_1, \psi_{-1}\}, \\ n & \longmapsto & (\psi_1)^n, \end{array} \quad \text{and} \quad \begin{array}{rcl} \rho_{-1}\colon \mathbb{Z} & \longrightarrow & \{\psi_1, \psi_{-1}\}, \\ n & \longmapsto & (\psi_{-1})^n, \end{array}$$

Part (c) and (d). For each action ρ you found in (b), form the semi-direct product $\mathbb{Z} \rtimes_\rho \mathbb{Z}$ and describe it in terms of generators and relations. For each of these actions write $\mathbb{Z} \rtimes_\rho \mathbb{Z}$ as a quotient of a free group.

Solution (4 marks). Given two groups N and H and an action of H on N given by $\rho\colon H \to \mathrm{Aut}(N)$, the *semi-direct* product of N and H is the group $N \rtimes_\rho H$ whose underlying set is $N \times H$ (where $\times$ is the Cartesian product and *not* the direct product) and with multiplication defined by

$$(n, h)(m, k) = (n(\rho(h)m), hk).$$

In our case, the semidirect product $\mathbb{Z} \rtimes_{\rho_1} \mathbb{Z}$ is the group whose underlying set is $\mathbb{Z} \times \mathbb{Z}$ with multiplication defined by

$$\begin{aligned} (x_1, y_1)(x_2, y_2) &= (x_1 + (\rho_1(y_1)x_2), y_1 + y_2) \\ &= (x_1 + (\psi_1)^{y_1}(x_2), y_1 + y_2) \\ &= (x_1 + x_2, y_1 + y_2). \end{aligned}$$

So

$$\mathbb{Z} \rtimes_{\rho_1} \mathbb{Z} = \mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid xy = yx \rangle.$$

The semidirect product $\mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z}$ is the group whose underlying set is $\mathbb{Z} \times \mathbb{Z}$ with multiplication defined by

$$\begin{aligned} (x_1, y_1)(x_2, y_2) &= (x_1 + (\rho_{-1}(y_1)x_2), y_1 + y_2) \\ &= (x_1 + (\psi_{-1})^{y_1}(x_2), y_1 + y_2) \\ &= (x_1 + (-1)^{y_1}(x_2), y_1 + y_2). \end{aligned}$$

If $(x, y) \in \mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z}$ then

$$(x, y) = (1, 0)^x (0, 1)^y.$$

We have the presentation given by the multiplication table

$$\mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z} = \left\langle \mathbb{Z} \times \mathbb{Z} \mid \begin{array}{c} \text{if } (x_1,y_1)\in\mathbb{Z}\times\mathbb{Z} \text{ and } (x_2,y_2)\in\mathbb{Z}\times\mathbb{Z} \text{ then} \\ (x_1,y_1)(x_2,y_2)=(x_1+(-1)^{y_2}x_2,y_1+y_2) \end{array} \right\rangle$$

where $\mathbb{Z} \times \mathbb{Z}$ is the Cartesion and not the direct product. Let

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

We claim that the map

$$\begin{array}{rcl} \phi\colon G & \longrightarrow & \mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z} \\ a & \longmapsto & (1, 0), \\ b & \longmapsto & (0, 1), \end{array}$$

is an isomorphism.

To show:

(1) The relations in G can be derived by the relations in $\mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z}$ i.e
$$\phi(a)\phi(b)\phi(a)\phi(b)^{-1} = 1,$$
so that ϕ is a homomorphism.
(2) The map
$$\begin{array}{rcl} \xi\colon \mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z} & \longrightarrow & G \\ (x, y) & \longmapsto & a^x b^y, \end{array}$$
is a homomorphism.

(1)

$$\begin{aligned} \phi(a)\phi(b)\phi(a)\phi(b)^{-1} &= (1, 0)(0, 1)(1, 0)(0, -1) \\ &= (1, 1)(1, 0)(0, -1) \\ &= (0, 1)(0, -1) \\ &= (0, 0) \\ &= 1. \end{aligned}$$

(2) To show: If $(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z}$ then
$$\xi(x_1, y_1)\xi(x_2, y_2) = \xi((x_1, y_1)(x_2, y_2)).$$
Let $(x_1, y_1), (x_2, y_2) \in \mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z}$. Then
$$\xi(x_1, y_1)\xi(x_2, y_2) = a^{x_1} b^{y_1} a^{x_2} b^{y_2},$$
$$\xi((x_1, y_1)(x_2, y_2)) = \xi(x_1 + (-1)^{y_1} x_2, y_1 + y_2) = a^{x_1+(-1)^{y_1} x_2} b^{y_1+y_2}.$$
If $n \in \mathbb{Z}_{\geq 0}$ then
$$\begin{aligned} b &= aba = aabaa = \cdots = a^n b a^n, \\ b &= a^{-1}ba^{-1} = a^{-1}a^{-1}ba^{-1}a^{-1} = \cdots = a^{-n}ba^{-n}. \end{aligned} \tag{5}$$
We assume that $y_1 \in \mathbb{Z}_{\geq 1}$ and prove by induction on y_1 that
$$a^{x_1} b^{y_1} a^{x_2} b^{y_2} = a^{x_1+(-1)^{y_1} x_2} b^{y_1+y_2},$$
(the case $y_1 = 0$ is quick to check and the case $y_1 < 0$ should be similar to our induction).
Base case: If $y_1 = 1$, then
$$a^{x_1} b^{y_1} a^{x_2} b^{y_2} = a^{x_1} b a^{x_2} b^{y_2}$$

$$\begin{aligned}
&= a^{x_1}(a^{-x_2}ba^{-x_2})a^{x_2}b^{y_2} \quad \text{(by Equation 5)}\\
&= a^{x_1-x_2}b^{y_2+1}\\
&= a^{x_1+(-1)^{y_1}x_2}b^{y_1+y_2}.
\end{aligned}$$

Induction step: If $y_1 > 1$, then

$$\begin{aligned}
a^{x_1}b^{y_1}a^{x_2}b^{y_2} &= a^{x_1}b^{y_1-1}ba^{x_2}b^{y_2}\\
&= a^{x_1}b^{y_1-1}(a^{-x_2}ba^{-x_2})a^{x_2}b^{y_2} \quad \text{(by Equation 5)}\\
&= a^{x_1}b^{y_1-1}a^{-x_2}b^{y_2+1}\\
&= a^{x_1+(-1)^{y_1-1}(-x_2)}b^{y_1-1+y_2+1}\text{(by the induction hypothesis)}\\
&= a^{x_1+(-1)^{y_1}(x_2)}b^{y_1+y_2}.
\end{aligned}$$

So

$$a^{x_1}b^{y_1}a^{x_2}b^{y_2} = a^{x_1+(-1)^{y_1}x_2}b^{y_1+y_2},$$

for $y_1 \in \mathbb{Z}_{\geq 1}$ by induction.

As quotients of free groups, we have

$$\begin{aligned}
\mathbb{Z} \rtimes_{\rho_1} \mathbb{Z} &= \mathrm{Fr}\{x, y\}/\mathrm{NCl}\{xyx^{-1}y^{-1}\}\\
\mathbb{Z} \rtimes_{\rho_{-1}} \mathbb{Z} &= \mathrm{Fr}\{x, y\}/\mathrm{NCl}\{xyxy^{-1}\},
\end{aligned}$$

where $\mathrm{NCl}(X)$ is the normal closure of X i.e the intersection of all the normal subgroups containing X. Note that there is a more 'pedestrian' definition of $\mathrm{NCl}(X)$ as the subgroup generated by $\{gxg^{-1} \mid g \in G, x \in X\}$.

References

[Bou98] N. Bourbaki, *Algebra i: Chapters 1-3*, Actualités scientifiques et industrielles, Springer, 1998.

[FH91] W. Fulton and J. Harris, *Representation theory: A first course*, Graduate Texts in Mathematics, Springer New York, 1991.

[Lan05] S. Lang, *Algebra*, Graduate Texts in Mathematics, Springer New York, 2005.