**University of Birmingham**
**School of Mathematics**

# 1AC Algebra: Feedback Sheet 4

**Marking guidance**

AQ1 and AQ4 are the questions to be marked using the guidance after those questions. There are a total of 20 marks for these algebra questions. The mark out of 20 for the algebra questions should be combined with the mark for the combinatorics questions.
More importantly than giving the mark, you should provide detailed written feedback. There should be comments to explain where improvements can be made, even when it is just minor improvements. This could include: places where there are mathematical errors or inaccuracies; places where mathematics should be explained more clearly or in more detail; places where the mathematics should be set out better; or places where the solution is longer than necessary or overly verbose. You should ensure that feedback is given to explain reasons why marks have not been gained.

**AQ1.** (SUM)

(a) (i) Calculate the multiplication table of $\mathbb{Z}_8$.
*You may wish to use the notation $\bar{a}$ rather than $[a]_8$ for elements of $\mathbb{Z}_8$ and it would be ok for you to omit the row and column for $[0]_8$.*

(ii) Determine all $x \in \mathbb{Z}_8$ for which there exists $x^{-1} \in \mathbb{Z}_8$ such that $x \cdot x^{-1} = [1]_8$.
*You do not need to write too much for (a)(ii) and just explain how this can be determined from the multiplication table.*

(b) Let $n \in \mathbb{N}$, and let $x, y, z \in \mathbb{Z}_n$.

(i) Suppose that $x + z = y + z$. Prove that $x = y$.

(ii) Prove that $x \cdot (y \cdot z) + (y \cdot x) \cdot x = x \cdot (y \cdot (z + x))$.

**Solution**

(a) We use the notation where we write $\bar{a}$ rather than $[a]_8$ for $a \in \mathbb{Z}$.

(i) We work out the multiplication table for $\mathbb{Z}_8$ below, where we omit the row and column for $\bar{0}$.

| $\cdot$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{6}$ | $\bar{7}$ |
|---|---|---|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{6}$ | $\bar{7}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{6}$ | $\bar{1}$ | $\bar{4}$ | $\bar{7}$ | $\bar{2}$ | $\bar{5}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{0}$ | $\bar{4}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{2}$ | $\bar{7}$ | $\bar{4}$ | $\bar{1}$ | $\bar{6}$ | $\bar{3}$ |
| $\bar{6}$ | $\bar{6}$ | $\bar{4}$ | $\bar{2}$ | $\bar{0}$ | $\bar{6}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{7}$ | $\bar{7}$ | $\bar{6}$ | $\bar{5}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

(ii) We observe that $\bar{1}$ occurs in the rows of the multiplication table labelled by $\bar{1}$, $\bar{3}$, $\bar{5}$ and $\bar{7}$. This means that for $x \in \mathbb{Z}_8$, there exists $x^{-1} \in \mathbb{Z}_8$ such that $x \cdot x^{-1} = \bar{1}$ if and only if $x \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

(b) Let $n \in \mathbb{N}$ and $x, y, z \in \mathbb{Z}_n$.

(i)

**Claim.** *Suppose that $x + z = y + z$. Then $x = y$.*

*Proof.* Let $x_0, y_0, z_0 \in \mathbb{Z}$ such that $x = [x_0]_n$, $y = [y_0]_n$ and $z = [z_0]_n$.
Since $x + z = y + z$, we have $[x_0 + z_0]_n = [y_0 + z_0]_n$, so that $x_0 + z_0 \equiv y_0 + z_0 \bmod n$ by Lemma 3.21.
Thus $x_0 \equiv y_0 \bmod n$ using Lemma 3.6, and thus $[x_0]_n = [y_0]_n$ by Lemma 3.21.
Hence, $x = y$. □

(ii)

**Claim.** $x \cdot (y \cdot z) + (y \cdot x) \cdot x = x \cdot (y \cdot (z + x))$

*Proof.* Let $x_0, y_0, z_0 \in \mathbb{Z}$ such that $x = [x_0]_n, y = [y_0]_n, z = [z_0]_n$. Then

$$
\begin{aligned}
& x \cdot (y \cdot z) + (y \cdot x) \cdot x \\
&= [x_0]_n \cdot [y_0 z_0]_n + [y_0 x_0] \cdot [x_0]_n && \text{by definition of } \cdot \text{ in } \mathbb{Z}_n \\
&= [x_0 y_0 z_0]_n + [y_0 x_0 x_0]_n && \text{by definition of } \cdot \text{ in } \mathbb{Z}_n \\
&= [x_0 y_0 z_0 + y_0 x_0 x_0]_n && \text{by definition of } + \text{ in } \mathbb{Z}_n \\
&= [x_0 y_0 z_0 + x_0 y_0 x_0]_n && \text{using commutativity of multiplication in } \mathbb{Z} \\
&= [x_0 (y_0 z_0 + y_0 x_0)]_n && \text{using the distributivity property of } \mathbb{Z} \\
&= [x_0 (y_0 (z_0 + x_0))]_n && \text{using the distributivity property of } \mathbb{Z} \\
&= [x_0]_n \cdot [y_0 (z_0 + x_0)]_n && \text{by definition of } \cdot \text{ in } \mathbb{Z}_n \\
&= [x_0]_n \cdot [y_0]_n \cdot [z_0 + x_0]_n && \text{by definition of } \cdot \text{ in } \mathbb{Z}_n \\
&= [x_0]_n \cdot [y_0]_n \cdot ([z_0]_n + [x_0]_n) && \text{by definition of } + \text{ in } \mathbb{Z}_n \\
&= x \cdot (y \cdot (z + x)) && \text{by definition of } + \text{ and } \cdot \text{ in } \mathbb{Z}_n. \qquad \square
\end{aligned}
$$

**Feedback**

Part (a) shouldn't cause much trouble. It is just to give you some practice doing calculations in $\mathbb{Z}_n$. In (ii) you just have to make the observation about the multiplication table as above.

Part (b) is here to give you some practice at proving properties of $\mathbb{Z}_n$. The main thing you need to do is make sure you set out your proofs correctly. There are different ways to do these proofs.

One way is to approach them similarly to Lemma 3.24 as we have done for (b)(i). In this case the proof of Lemma 3.24 should give you an idea of how to write your proof.

An alternative way is to use the properties of $\mathbb{Z}_n$ covered in Section 3.7, as we have done above for (b)(ii). In this case you should ensure that you justify each of the steps by saying which of the properties of $\mathbb{Z}_n$ you are using. It would be a good exercise to do (b)(i) in this way if you have not already done so.

**10 marks**

(a) 5 marks

(i) 3 marks for the multiplication table wiht partial credit given if there are any errors.

(a)(ii) 2 marks. 1 mark for the correct answer, 1 mark for the justification

(b) 5 marks.

(i) 2 marks. For 2 marks the proof should be complete and clearly explained. Award 1 mark is reasonable progress is made and 0 marks if little or no progress is made.

(ii) 3 marks. For 3 marks the proof should be complete and clearly explained. Award 2 marks if the proof essentially complete and there are only minor errors. Award 1 mark is reasonable progress is made and 0 marks if little or no progress is made.

**AQ2.** (a) Let $n, p \in \mathbb{N}$. Suppose that $p$ is an odd prime and that $p \mid n^2 + 1$. Prove that $p \equiv 1 \bmod 4$.

(b) Show that there are infinitely many primes $p$ with $p \equiv 1 \bmod 4$.

*This question is quite challenging, so you're likely to want to look at the hints that will be put on canvas.*

**Solution**

(a) Let $n, p \in \mathbb{N}$. Suppose that $p$ is an odd prime and that $p \mid n^2 + 1$.

**Claim.** $p \equiv 1 \bmod 4$.

*Proof.* Since $p$ is odd, we have $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. Suppose for a contradiction that $p \equiv 3 \bmod 4$, so that $p = 4m + 3$ for some $m \in \mathbb{N}$.

Since $p \mid n^2 + 1$, we have $n^2 \equiv -1 \bmod p$, and thus $n^4 \equiv 1 \bmod p$. We have $n^{p-1} = n^{4m+2} = (n^4)^m n^2$. Therefore,

$$\begin{aligned} n^{p-1} &\equiv 1^m(-1) \bmod p \\ &\equiv -1 \bmod p. \end{aligned}$$

Also we note that as $p \mid n^2 + 1$, we have $p \nmid n$ so that $n$ is coprime to $p$. Therefore, $n^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem.

This is a contradiction, so we deduce that $p \equiv 1 \bmod 4$. □

(b)

**Claim.** *There are infinitely many primes $p$ with $p \equiv 1 \bmod 4$.*

*Proof.* Suppose for a contradiction that there are only finitely many primes $p$ with $p \equiv 1 \bmod 4$. Then we can list them as $p_1, p_2, \ldots, p_k$. Now consider $n = 2p_1p_2 \cdots p_k$ and

$$m = (2p_1p_2 \cdots p_k)^2 + 1 = n^2 + 1.$$

Let $p \in \mathbb{N}$ be a prime such that $p \mid m$. Then $p$ is odd, because $m$ is odd. Further, $p \equiv 1 \bmod 4$ by (a). Thus $p = p_i$ for some $i$.

However,

$$\frac{m}{p_i} = \frac{(2p_1p_2 \cdots p_k)^2}{p_i} + \frac{1}{p_i}$$

and $\frac{(2p_1p_2\cdots p_k)^2}{p_i} \in \mathbb{Z}$, so $\frac{m}{p_i}$ is not an integer, which is a contradiction.

Hence, there are infinitely many primes $p$ with $p \equiv 1 \bmod 4$. □

**Feedback**

This proof is tougher to come up with than others that we have seen. We need a clever application of Fermat's little theorem in (a), and the proof requires a neat proof by contradiction. It would be impressive if you came up with this proof by yourself.

For the proof in (b), you can follow similar lines to the proof of Theorem 1.7, once you have realised that you should use $m$ as above.

It is also possible to prove that there are infinitely many primes $p$ with $p \equiv 3 \bmod 4$. In fact this is one of the extra exercises for Chapter 1, and is an easier proof than the one above.

This is part of a much bigger story as Dirichlet's theorem on arithmetic progressions says that given coprime natural numbers $a$ and $n$, there are infinitely many primes $p$ with $p \equiv a \bmod n$.

**AQ3.** Determine the cycle notation, cycle shape and order of each of the following permutations in $S_9$.

(a) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 4 & 1 & 8 & 9 & 3 & 2 & 6 \end{pmatrix}$

(b) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 3 & 6 & 9 & 4 & 7 & 1 & 2 \end{pmatrix}$

**Solution**

(a) To work out the cycle notation for $f$ we first look for the cycle containing 1 and find that it is

$$(1734).$$

Next we look for the cycle containing 2 and get

$$(258).$$

Last we look for the cycle containing 6 and get

$$(69).$$

Therefore, the cycle notation for $f$ is

$$f = (1734)(258)(69).$$

Remember that in cycle notation we omit the symbol $\circ$ for composition and we omit 1-cycles (though in this case there are no 1-cycles).

The cycle shape of $f$ is $(4, 3, 2)$.

To determine the order of $f$ we use the formula given in Lemma 4.22, which says that the order of $f$ is the lowest common multiple of the entries in the cycle shape. Therefore, we have $o(f) = \text{lcm}(4, 3, 2) = 12$.

(b) We work out the cycle notation for $g$ as we did for $f$ in (a) and get

$$g = (18)(259)(46).$$

Remember that we omit the 1-cycles.

The cycle shape of $g$ is $(3, 2, 2, 1, 1)$.

The order of $g$ is $o(g) = \text{lcm}(3, 2, 2, 1, 1) = 6$.

**Feedback**

Working out the cycle notation and cycle shape hopefully shouldn't cause many problems. Just make sure you are careful so that don't make any mistakes. Once you've done enough practice, the calculation of cycle notation should hopefully be ok.

Remember that we have the convention that we omit the composition symbol $\circ$ and we omit 1-cycles.

However, you must remember that the cycle shape does include 1s to show that there are some 1-cycles.

For working out the orders you should remember to use the formula given in Lemma 4.22. This makes it much quicker than trying to work out the order by calculating powers.

**AQ4.** (SUM) Let $f = (1546)(37) \in S_7$ and $g = (137)(245) \in S_7$ be permutations given in cycle notation.

Calculate the following permutations giving your solution in cycle notation.

(a) $f \circ g$

(b) $g \circ f$

(c) $f^2$

(d) $g^3$

(e) $f^{-1}$

(f) $g^{-1}$

(g) $g^{-1} \circ f^{-1}$

(h) $(f \circ g)^{-1}$

(i) Find $h \in S_7$ such that $f \circ h = g$

(j) Find $k \in S_7$ such that $k \circ f = g$

**Solution**

We work out the following using the methods given in Example 4.19. We only give some explanation of how this is done in (a), and then also some discussion of how to find $h$ and $k$ in (i) and (j).

(a) To work out $f \circ g$ we first write their cycle notation of $f$ and of $g$ next to each other:

$$(1546)(37)(137)(245).$$

Then going along the cycles **from right to left** we say:
1 goes to 3 goes to 7.
7 goes to 1 goes to 5.
5 goes to 2.
2 goes to 4 goes to 6.
6 goes to 1.
So (17526) is a cycle in $f \circ g$.
3 goes to 7 goes to 3.
So (3) is a cycle in $f \circ g$.
4 goes to 5 goes to 4.
So (4) is a cycle in $f \circ g$.

Therefore, $f \circ g = (17526)$. (Remember that we omit the composition symbol $\circ$ when writing permutations in cycle notation and we omit 1-cycles).

(b) $g \circ f = (12463)$.

(c) $f^2 = (14)(56)$.

(d) $g^3 = \mathrm{id}$

(e) $f^{-1} = (1645)(37)$

(f) $g^{-1} = (173)(254)$.

(g) $g^{-1} \circ f^{-1} = (16257)$.

(h) $(f \circ g)^{-1} = (16257)$.

(i) To find $h \in S_7$ such that $f \circ h = g$, we calculate that

$$\begin{aligned} h &= f^{-1} \circ f \circ h \\ &= f^{-1} \circ g \\ &= (1645)(37)(137)(245) \\ &= (1764)(25). \end{aligned}$$

(j) To find $k \in S_7$ such that $k \circ f = g$, we calculate that

$$\begin{aligned} k &= k \circ f \circ f^{-1} \\ &= g \circ f^{-} \\ &= (137)(245)(1645)(37) \\ &= (1653)(24). \end{aligned}$$

**Feedback**

This gives you some practice calculating with permutations in cycle notation. Once you have done enough practice, then these sorts of calculations shouldn't cause much difficulty, but you should make sure that you do enough practice. The best way to do these is to talk to yourself (better in your head than out loud) and then write out the answer. It's always worth checking your answers, as it's not too difficult to make a mistake. Also there are ways that you will see that something has gone wrong: for example if a number is in two cycles, then you have definitely made a mistake.

You should remember to read the question carefully. For this question it is clearly stated that the solution should be given in cycle notation, so that is what you must do. As you will see from the marking guidance you will have been penalised for any answers given in two-row notation.

**Marking guidance.**

**10 marks**

The marking is primarily based on getting the correct answer with 1 mark for each correct answer.

If $g \circ f$ is calculated in (a) and $f \circ g$ is calculated in (b), then this can be counted as just one incorrect answer. Similarly if there are similars error in (i) and (j). Follow through marks should also be given in (g) and (h) if the answer is incorrect due to an earlier error.

If some correct working is shown but an error is made, then you can show some leniency on this system.

Do not penalize if 1-cycles are left in, but do give a comment about this. Similarly do not penalize if the cycles are not written in the conventional way, having the smallest element at the start of each cycle and ordering the cycles by their first element, but do give a feedback comment about this.

The question clearly states that the solutions should be given in cycle notation. So although it may seem harsh, answers given in two-row notation should be viewed as incorrect. It is ok for students to convert to two-row notation to do the calculation, but the final solution must be given in cycle notation.

Do give feedback if you can see why an answer is incorrect.