University of Birmingham
School of Mathematics

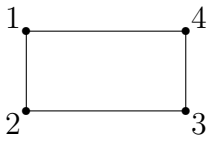
1AC Algebra: Feedback Sheet 5

Marking guidance

AQ2 and AQ3 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, and then a total mark given as a percentage.

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. Let G be the symmetry group of the rectangle below.

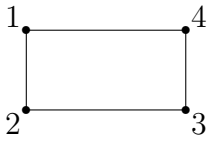


(a) Write down all elements of G expressed as permutations of the vertices.

(b) Calculate the multiplication table of G.
The multiplication table has rows and columns labelled by the elements of G and the entries are given by the products in G.

Solution

Let G be the symmetry group of the rectangle below.



(a) There are 4 elements of G: the identity, a rotation by π radians and two reflections. These are given by the following elements of S_4.

$e =$ do nothing.

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$
$$= \text{a rotation through } \pi \text{ radians}$$
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$
$$= \text{a reflection in the horizontal axis}$$
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$
$$= \text{a reflection in the vertical axis}$$

(b) The multiplication table of G is given below.

	e	ρ	σ_1	σ_2
e	e	ρ	σ_1	σ_2
ρ	ρ	e	σ_2	σ_1
σ_1	σ_1	σ_2	e	ρ
σ_2	σ_2	σ_1	ρ	e

Feedback

This question gives you some practice in determining symmetry groups. You should be careful to think about what are the isometries of the rectangle, and once you have worked this out you can write them down as permutations of the vertices. We have done this for symmetries of the square and pentagon in the notes or in the lectures, so you can use those examples to give you an idea of what to do.

Working out the multiplication table gives you some more practice calculating with permutations. You'll want to pick a good notation for the elements of G so that you can write the multiplication table compactly. You also need to be careful to make sure you don't make any mistakes with the calculations required. Each row and column of the table should contain each element of G exactly once, so you would know that you have made a mistake if that is not the case – you should also think about why each row and column has this property.

AQ2. (SUM) Let $p, q \in \mathbb{N}$ be primes with $p \neq q$ and let $G = \{[a]_{pq} \in \mathbb{Z}_{pq} : p \nmid a \text{ and } q \nmid a\}$. Prove that G is a group under multiplication.

Solution

Let $p, q \in \mathbb{N}$ be primes with $p \neq q$ and let $G = \{[a]_{pq} \in \mathbb{Z}_{pq} : p \nmid a \text{ and } q \nmid a\}$.

We let $n \in pq$. We first make the following claim about G showing that $G = U(\mathbb{Z}_n)$. We recall that $U(\mathbb{Z}_n)\{[a]_n \in \mathbb{Z}_n : \text{hcf}(a, n) = 1\}$ is defined in Section 5.3 of the lecture notes.

Claim. $G = U(\mathbb{Z}_n) = \{[a]_n \in \mathbb{Z}_n : \text{hcf}(a, n) = 1\}$.

Proof. Let $a \in \mathbb{Z}$. Since the only positive factors of $n = pq$ are 1, p, q and pq, we have that $\text{hcf}(a, n)$ is equal to 1, p, q and pq. If $p \nmid a$ and $q \nmid a$, we deduce that $\text{hcf}(a, n) = 1$. Conversely if $p \mid a$ or $q \mid a$, then we have that $\text{hcf}(a, n) \neq 1$. Thus we have that $[a]_n \in G$ if and only if $\text{hcf}(a, n) = 1$, and hence that $G = \{[a]_n \in \mathbb{Z}_n : \text{hcf}(a, n) = 1\}$. □

We use the previous claim to move on to prove the statement given in the question, and note here that the proof here works more generally when n is any natural number.

Claim. *$U(\mathbb{Z}_n)$ is a group under multiplication.*

Proof. We have to check the axioms.

(G0). Let $x, y \in U(\mathbb{Z}_n)$, and let $x_0, y_0 \in \mathbb{Z}$ such that $x = [x_0]_n$ and $y = [y_0]_n$.
Then x_0 is coprime to n and y_0 is coprime to n.
Thus $x_0 y_0$ in coprime to n by Lemma 3.16(b).
Therefore, $x \cdot y = [x_0 y_0]_n \in U(\mathbb{Z}_n)$.
Hence (G0) holds.

Axioms (G1) and (G2) are properties of $\mathbb{Z}_n$ given in Section 3.7, and the identity is $e = [1]_n$.

(G3). Let $x \in U(\mathbb{Z}_n)$, and let $x_0 \in \mathbb{Z}$ such that $x = [x_0]_p$.
Then x_0 is coprime to n.
Therefore, by Theorem 3.10 there exists $y_0 \in \mathbb{Z}$ such that

$$x_0 y_0 \equiv 1 \bmod n.$$

So for $x^{-1} = [y_0]_n$, we have $x \cdot x^{-1} = [1]_n$ and $x^{-1} \cdot x = [1]_n$.
Also from $x_0 y_0 \equiv 1 \bmod n$, we deduce that $\text{hcf}(y_0, n) = 1$, so that y_0 is coprime to n.
Hence, (G3) is true. □

Feedback

We have used a trick here of first showing that $G = U(\mathbb{Z}_n)$ and then giving a more general proof that $U(\mathbb{Z}_n)$ is a group. The proof here is similar to the proof of Proposition 5.7 in the lecture notes, so you can use this to suggest what you should do. It is also possible to prove that G is a group under multiplication more directly, where again you could use the proof of Proposition 5.7 to give you an idea of how to structure your proof.

You should remember that to prove that a set with a binary operation is a group, you need to prove that the axioms hold. So your proof needs to contain a justification that they do hold.

In this case it turns out that (G0) and (G3) require the most work, as (G1) and (G2) are properties of $\mathbb{Z}_n$ from Section 3.7. To check that (G0) holds you can follow a similar argument to that given in the proof of Proposition 5.7, but now you have to notice that Lemma 3.17(b) gives exactly the statement that you require. Similarly, for proving (G3) you can follow the proof of Proposition 5.7 quite closely.

As always you should make sure you explain everything in your proof, and the proof of Proposition 5.7 can be used to see how much you should include.

Marking guidance.

8 marks

3 marks for showing that (G0) holds. Thus must be well explained including explaning why x_0y_0 is coprime to $n = pq$ to gain 2 or 3 marks.

1 mark for saying that (G1) and (G2) are properties of $\mathbb{Z}_{pq}$. Here it is preferable to state that $e = [1]_{pq}$, so give feedback if that is not stated, but do not deduct the mark for this.

4 marks for showing that (G3) holds: 1 marks for explaining that the hypothesis of Theorem 3.10 hold, 1 mark for applying Theorem 3.10, 1 mark for giving the multiplicative inverse and 1 mark for overall explanation and justification of the proof. Preferably there should be justification that the multiplicative inverse does lie in G, so give some feedback on this, but do not deduct a mark for this.

AQ3. (SUM) Determine which of the following subsets of S_8 are subgroups of S_8.

(a) $H = \{g \in S_8 : g^2 = e\}$.

(b) $H = \{g \in S_8 : g(4) = 4 \text{ and } g(5) = 5\}$

(c) $H = \{g \in S_8 : g(i) \in \{1, 2, 3, 4\} \text{ for all } i \in \{1, 2, 3, 4\}\}$.

You should justify your answers.

Solution

(a) Let $H = \{g \in S_8 : g^2 = e\}$.

Rough-work/discussion

We want to use the subgroup test to determine whether $H \leq S_8$. First, we want to think about the definition of H and make sure we understand it. From the definition we see that the elements of H are the permutations $g \in S_8$ such that $g^2 = e$. So from Lemma 4.22 we see that the elements of H are the permutations, which are a disjoint product of 2-cycles.

Once we have a good understanding of the definition of H, we can start to think about whether the conditions (SG1), (SG2) and (SG3) hold. We see fairly quickly that $e \in H$, so that (SG1) holds and we move on to consider (SG2). So we want to think about whether for $g, h \in H$, we also have $g \circ h \in H$. That is we want to know whether $g^2 = e$ and $h^2 = e$ implies that $(g \circ h)^2 = e$. The easiest cases to consider first are when g and h are 2-cycles. We see that if g and h are disjoint 2-cycles, then their product is does still have order two, and so lies in H. So we may next consider what happens if g and h are not disjoint, and we can consider the case $g = (12)$ and $h = (23)$. For this case we see that $g \circ h = (123)$ and so is not an element of H. So we see that this gives a counterexample and we now have to write this up clearly and justify it.

Counterexample to show that (SG2) does not hold.

Let $g = (12)$ and $h = (23)$.
Then we $g^2 = e = h^2$ so that $g, h \in H$.
But $g \circ h = (12)(23) = (123) \notin H$, as $(g \circ h)^2 \neq e$.

(b) Let $H = \{g \in S_8 : g(4) = 4 \text{ and } g(5) = 5\}$.

Rough-work/discussion

We want to use the subgroup test to determine whether $H \leq S_8$. We can do some rough work, and first that see that $e \in H$ because $e(4) = 4$ and $e(5) = 5$, so (SG1) holds. Then to test whether (SG2) holds, we check that if $g, h \in H$, so that $g(4) = 4 = h(4)$ and $g(5) = 5 = h(5)$, then we have $(g \circ h)(4) = g(h(4)) = g(4) = 4$ and similarly $(g \circ h)(5) = 5$, so that $g \circ h \in H$. So we see that (SG2) holds, and with a bit more work we can convince ourselves that (SG3) holds. Now we have to write this up properly

Proof that $H \leq S_8$.

We use the subgroup test to show that $H \leq S_8$.

(SG1) Consider $e \in S_8$, which is the identity function on $\{1, 2, \ldots, 8\}$.
We have $e(4) = 5$ and $e(5) = 5$.
Thus $e \in H$.

(SG2) Let $g, h \in H$.
Then $g(4) = 4 = h(4)$, so that $(g \circ h)(4) = g(h(4)) = g(4) = 4$.
Similarly, $(g \circ h)(5) = 5$.
Thus $g \circ h \in H$.

(SG3) Let $g \in H$.
By applying g^{-1} to $g(4) = 4$, we obtain $g^{-1}(g(4)) = g^{-1}(4)$.
Thus as $g^{-1}(g(4)) = 4$, we get $g^{-1}(4) = 4$.
Similarly, we can show that $g^{-1}(5) = 5$.
Thus $g^{-1} \in H$. □

(c) $H = \{g \in S_8 : g(i) \in \{1, 2, 3, 4\} \text{ for all } i \in \{1, 2, 3, 4\}\}$.

Rough-work/discussion

We want to use the subgroup test to determine whether $H \leq S_8$. First it is important to make sure we understand the definition of H. We can write out in more length by saying that in permutation $g \in S_8$ is an element of H if it satisfies that $g(1), g(2), g(3), g(4) \in \{1, 2, 3, 4\}$. So we see that g permute the numbers $\{1, 2, 3, 4\}$ amongst themselves, and with a bit more thought we see that this means that g permutes the numbers $\{5, 6, 7, 8\}$ amongst themselves.

Then we can do some rough work like we did in (b) and this should lead us to seeing that (SG1), (SG2) and (SG3) hold for H. We don't go in to that here, and just go straight to writing this up properly as a proof. We so note here that the proof that (SG3) holds does require some thought though.

Proof that $H \leq S_8$.

We use the subgroup test to show that $H \leq S_8$.

(SG1) Consider $e \in S_8$, which is the identity function on $\{1, 2, \ldots, 8\}$.
Then we have $e(i) = i \in \{1, 2, 3, 4\}$ for all $i \in \{1, 2, 3, 4\}$.
Thus $e \in H$.

(SG2) Let $g, h \in H$ and let $i \in \{1, 2, 3, 4\}$
Then $h(i) \in \{1, 2, 3, 4\}$ as $h \in H$, and thus $g(h(i)) \in \{1, 2, 3, 4\}$ as $g \in H$.
Therefore, $(g \circ h)(i) \in \{1, 2, 3, 4\}$.
Thus $g \circ h \in H$.

(SG3) Let $g \in H$ and let $i \in \{1, 2, 3, 4\}$.
We consider $j = g^{-1}(i)$. We have $g(j) = i \in \{1, 2, 3, 4\}$.
Now if $j \notin \{1, 2, 3, 4\}$, then we see that g sends the five elements of $\{1, 2, 3, 4, j\}$ into $\{1, 2, 3, 4\}$, which is not possible as g is a permutation and therefore is injective.
Therefore, we deduce that $j = g^{-1}(i) \in \{1, 2, 3, 4\}$.
Thus $g^{-1} \in H$. □

Feedback

This question gives you practice in using the subgroup test to check whether subsets of a group are indeed subgroups. For these types of questions you may want to start with some rough work to try to determine whether the conditions (SG1), (SG2) and (SG3) hold for H. The rough work that we have included in the solutions here is just there to help you, and you should not include this in your solutions (though it wouldn't really do any harm if you did).

If you think the conditions (SG1), (SG2) and (SG3) do hold, then you'll next want to write out a proof that they do hold. In this case you should make sure that you cover and explain everything to justify that (SG1), (SG2) and (SG3) hold.

If you think that one of the conditions does not hold for H, then you have to justify that this condition does not hold and you must do this by providing an explicit counterexample. Note that once you justify that one of (SG1), (SG2) or (SG3) does not hold you have shown that H is not a subgroup; so you don't need to worry about whether the other conditions hold.

As already mentioned you should remember that you have to ensure that you explain your work, and justify everything. You can use the model solutions above as a guide for the amount of explanation that is expected.

The most tricky part of the question is proving that (SG3) holds in (c). Here some thought is required to see how to do this.

Marking guidance.

12 marks

(a) 3 marks: 1 mark for saying that H is not a subgroup, 1 mark for a correct counterexample and 2 marks for justifying that it is a counterexample.

(b) 4 marks: 1 mark for explaining that $e \in H$, 2 marks for showing that (SG2) holds and 1 mark for showing the (SG3) hold.

(c) 5 marks: 1 mark for explaining that $e \in H$, 2 marks for showing that (SG2) holds and 2 marks for showing the (SG3) hold.

In both (b) and (c) it is important that the steps are well explained and justified, so do reduce the mark awarded if this is not the case.

AQ4. Prove Lemma 5.15.

Lemma. *Let G be a group and let $g \in G$. Then*

(a) $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$ *is a subgroup of G.*

(b) *If g has finite order, then $\langle g \rangle$ is finite and $|\langle g \rangle| = o(g)$.*

Solution

Lemma. *Let G be a group and let $g \in G$. Then*

(a) $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$ *is a subgroup of* G.

(b) *If g has finite order, then $\langle g \rangle$ is finite and $|\langle g \rangle| = o(g)$.*

Proof. (a) We apply the subgroup test to show that $\langle g \rangle$ is a subgroup of G.
(SG1) We have $e = g^0 \in \langle g \rangle$.
(SG2) Let $g^r, g^s \in \langle g \rangle$, where $r, s \in \mathbb{Z}$.
Then $g^r g^s = g^{r+s} \in \langle g \rangle$, as $r + s \in \mathbb{Z}$.
(SG3) Let $g^r \in \langle g \rangle$, where $r \in \mathbb{Z}$.
Then $(g^r)^{-1} = g^{-r} \in \langle g \rangle$, as $-r \in \mathbb{Z}$.

(b) Let $o(g) = m$. We show that $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$. Clearly, we have that $\{e, g, g^2, \ldots, g^{m-1}\} \subseteq \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Now let $n \in \mathbb{Z}$, and write $n = mq + r$ where $q, r \in \mathbb{Z}$ with $0 \leq r < m$. Then we have $g^n = g^{mq+r} = (g^m)^q g^r = e^q g^r = g^r$, because $e^q = e$. It follows that $\langle g \rangle \subseteq \{e, g, g^2, \ldots, g^{m-1}\}$. Hence, $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$.

Now let $i, j \in \{0, 1, 2, \ldots, m-1\}$ with $i \leq j$ and suppose that $g^i = g^j$. Then we have $0 \leq j - i < m$ and $g^{j-i} = e$. This implies that $i = j$, because $m = o(g)$. Therefore, there are no repeats in $\{e, g, g^2, \ldots, g^{m-1}\} = \langle g \rangle$. Hence, $|\langle g \rangle| = m = o(g)$. □

Feedback

It will take you a bit of time to think through what you have to do for this proof.

For (a), it is easiest to use the subgroup test. Then you have to think through what you need to do and then write it out clearly.

For (b), there is a fair amount to do in order to check that $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$. You should remember that whenever you are showing that two sets are equal, the best way is usually to show that they are subsets of each other, and this will give you a nice format to write out the proof. Also you have to do the last part of checking that we get no repeated elements in $\{e, g, g^2, \ldots, g^{m-1}\}$, so that $|\langle g \rangle| = m$.

AQ5. (a) Let G be a group. Suppose that $g^2 = e$ for all $g \in G$. Prove that G is abelian.

(b) Prove Corollary 5.20.

Corollary. *Let $p \in \mathbb{N}$ be a prime and let G be a finite group of order p. Then G is cyclic.*

Solution

(a) Let G be a group. Suppose that $g^2 = e$ for all $g \in G$.

Claim. *G is abelian.*

Proof. Let $g, h \in G$. We have to show that $gh = hg$.
We have $g^2 = e$, $h^2 = e$ and $(gh)^2 = e$ by the assumption. From $(gh)^2 = e$ we obtain $ghgh = e$. Multiplying on the left by g gives $g^2hgh = g$, so $hgh = g$, because $g^2 = e$. Then multiplying on the right by h we get $hgh^2 = gh$, so $hg = gh$, because $h^2 = e$. Thus $gh = hg$ as required. □

(b)

Corollary. *Let $p \in \mathbb{N}$ be a prime and let G be a finite group of order p. Then G is cyclic.*

Proof. Let $g \in G$ with $g \neq e$. Then $o(g)$ is a factor of $|G| = p$ by Corollary 5.18. Also $o(g) \neq 1$, because $g \neq e$. Therefore, $o(g) = p$ and so $|\langle g \rangle| = p$ by Lemma 5.14. Since, $\langle g \rangle \subseteq G$ and $|\langle g \rangle| = |G|$, we have $G = \langle g \rangle$. Hence, G is cyclic. □

Feedback

The proofs for both (a) and (b) here are quite short.

Once you've got to the point of saying that you want to show that $gh = hg$ for $g, h \in G$, the key step for (a) is to realise that you should apply the hypothesis to gh to get that $(gh)^2 = e$. Then from here it is a matter of trying to get to from there to $gh = hg$, and there are different ways to do this. As always you should make sure you justify all the steps in your proof.

For (b) the key steps involve realising which results to apply. Once you have shown that $o(g) = p$ for $g \in G$ with $g \neq e$, and therefore that $|\langle g \rangle| = p$, you should be in good shape to finish the proof. As always you should write your proof well and explain all the steps.

AQ6. Let $p = 37$ and $q = 43$, $N = pq = 1591$, and we let $e = 5$. Consider the RSA cryptosystem with public key (N, e).

(a) Calculate the private key d for the cryptosystem.

(b) You are sent the ciphertext $\mathbf{c} = (154, 798, 362)$. Decipher it.

It will help to use a modular arithmetic calculator for this question, and you should be able to find such a calculator online.

Solution

(a) We calculate that $(p-1)(q-1) = 1512$. The private key d is the unique natural number such that $0 < d < 1512$ and $5d \equiv 1 \mod 1512$. To find this we use the Euclidean algorithm.
We calculate that

$$\begin{aligned} 1512 &= 302 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

to see that $\text{hcf}(1120, 3) = \text{hcf}(3, 1) = 1$. Then reversing our calculations, we get

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(1512 - (302 \cdot 5) \\ &= -2 \cdot 1512 + 605 \cdot 5 \end{aligned}$$

Thus $605 \cdot 5 \equiv 1 \mod 1512$, so $d = 605 \pmod{1512} = 605$.

(b) To decrypt the ciphertext $\mathbf{c} = (c_1, c_2, c_3) = (154, 798, 362)$, we have to calculate

$$c_i^d \pmod{1591} = m_i.$$

We work out

$$\begin{aligned} 154^{605} \pmod{1591} &= 1042, \\ 798^{605} \pmod{1591} &= 928, \\ 362^{605} \pmod{1591} &= 162. \end{aligned}$$

So $\mathbf{m} = (1042, 928, 162)$.
These could be worked out using a square and multiply method, and done by hand. However, that would be a lot of work, so it is better to just use a computer to do some modular arithmetic calculations. For instance you could use
https://www.wolframalpha.com/

Feedback

This hopefully should not have caused too many problems as it can be done in a very similar way to Example 3.30 in the lecture notes. You should write enough to explain what you are doing rather than just doing it. The use of the extended Euclidean algorithm is quite short in this case, but it still needs to be set out well, so that it shows that you understand the material. As mentioned above the decryption is difficult to do by hand, so it is best to use a computer for this.