YOUR-NAME
Math A4900
Final proofs portfolio
December 15, 2020

Problem	$\star$**s**	**Points**	**Tot**
1A	2		
2A	2		
4A	2		
5A	2		
3A	2		
2B	2		
7B	1		
9B	1		
10A	1		
3C	2		

Problem:	**1A**
No. stars:	**2**

Statement: Let G be a group and let $x \in G$. If $|x| = n < \infty$, prove that the elements $1, x, x^2, \cdots, x^{n-1}$ are all distinct. Deduce that $|x| = |\langle x \rangle|$

Proof. Let $|x| = n < \infty$. Now suppose that there are numbers $m, k \in \mathbb{Z}$ with $0 \leqslant k < m \leqslant n-1$ such that $x^m = x^k$.

Then we have that,

$$\begin{aligned} x^k \cdot x &= x^m \cdot x \\ x^k \cdot x^2 &= x^m \cdot x^2 \\ x^k \cdot x^3 &= x^m \cdot x^3 \\ &\vdots \\ x^k \cdot x^{n-m} &= x^m \cdot x^{n-m} \end{aligned}$$

However, on the right side of the equality, we have

$$\begin{aligned} x^m \cdot x^{n-m} &= x^{m+n-m} \\ &= x^n \\ &= e \end{aligned}$$

This implies that,

$$\begin{aligned} x^k \cdot x^{n-m} &= x^{k+n-m} \\ &= e \end{aligned}$$

where $k+n-m \in \mathbb{Z}$ and $0 < k+n-m < m+n-m = n$. However, we know that the order of x is n, which is defined to be the smallest positive integer of x that yields the identity element. Hence, we have a contradiction and thus $e, x, x^2, \ldots, x^{n-1}$ are all distinct.

Now consider $\langle x \rangle$. We know that each x^c is distinct for every $c \in \mathbb{Z}$ such that $0 \leqslant k \leqslant n-1$. Now fix an $m \in \mathbb{Z}$ such that $m \geqslant n$. Choose $k \in \mathbb{N}$ as the greatest positive integer such that $m \geqslant kn$. Then we have,

$$\begin{aligned} x^m &= x^{kn+(m-kn)} \\ &= x^{kn}x^{m-kn} \\ &= x^{m-kn} \end{aligned}$$

Note that $0 \leqslant m-kn$ since $m \geqslant kn$. In addition, $m-kn < n$ because, if $m-kn \geqslant n$, it would mean that $(k+1)n \leqslant m$. But we chose k such that it was the greatest positive integer with $m \geqslant kn$, so this is not possible.

Hence we have that $0 \leqslant m-kn < n$, and so $x^{m-kn} \in \{1, x, x^2, \cdots, x^{n-1}\}$. Since $m \geqslant n$ was an arbitrary integer, this holds for any x^m with $m \geqslant n$. Thus, for any $a \in \mathbb{Z}$, we have that,

$$x^a \in \{1, x, x^2, \cdots, x^{n-1}\}$$

and so $|\langle x \rangle| = n = |x|$. $\square$

	Points Possible					
complete	0	1	2	3	4	5
mathematically valid	0	1	2	3	4	5
readable/fluent	0	1	2	3	4	5
Total:						(out of 15)

Problem:	**2A**
No. stars:	**2**

Statement: Prove that if H and K are subgroups of G, then so is $H \cap K$. On the other hand, prove $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

Proof. Suppose $H, K \leqslant G$. Consider $H \cap K$. Note that $1 \in H, K$ by the definition of groups, so $1 \in H \cap K$. Hence, $H \cap K \neq \varnothing$. Now let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$, both of which are groups. Hence, $y^{-1} \in H$ and $y^{-1} \in K$, which implies $xy^{-1} \in H$ and $xy^{-1} \in K$. Thus, $xy^{-1} \in H \cap K$. As a result, $H \cap K$ satisfies the subgroup criterion and is hence a subgroup of G.

Now consider $H \cup K$. Suppose for contraposition that $H \not\subset K$ and $K \not\subset H$. Then $\exists x \in H$ such that $x \notin K$ and $\exists y \in K$ such that $y \notin H$. Then we have $y^{-1} \notin H$ and $x \notin K$, so $xy^{-1} \notin H, K$. Hence $xy^{-1} \notin H \cup K$ and so $H \cup K$ does not satisfy the subgroup criterion. As a result, we have that if $H \cup K$ is a subgroup of G, then $H \subset K$ or $K \subset H$.

Now for the other direction of the proof. Suppose $H \subset K$. Then $\forall\ x \in H$ we have $x \in K$. Hence, $H \cup K = K$. Since $K \leqslant G$, we have $H \cup K \leqslant G$ as well.

Suppose $K \subset H$. Then $\forall\ x \in K$ we have $x \in H$. Hence, $H \cup K = H$. Since $H \leqslant G$, we have $H \cup K \leqslant G$ as well. Thus, we have proved that if $H \subset K$ or $K \subset H$, then $H \cup K$ is a subgroup of G. □

	Points Possible					
complete	0	1	2	3	4	5
mathematically valid	0	1	2	3	4	5
readable/fluent	0	1	2	3	4	5
Total:					(out of 15)	

Problem:	**4A**
No. stars:	**2**

Statement: Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.

Proof. Let H be a finitely generated subgroup of $\mathbb{Q}$ and suppose that there is a finite set $\mathbb{Q}$ such that $H = \langle A \rangle$. Now consider k, the product of all the denominators that appear in A. Then every element $a/b \in A$ can be re-written as $\frac{a \cdot k/b}{b \cdot k/b} = \frac{a \cdot k/b}{k}$ since b is in the product that yields k and hence is a divisor of k. Thus, we can rewrite every fraction in A as a fraction with denominator k. That is, every fraction in A can be written as n/k for some $n \in \mathbb{Z}$. This lets us conclude that,

$$H = \langle A \rangle \leqslant \langle 1/k \rangle$$

Thus, by Theorem 7 in §2.3 of DF, we have that H is cyclic since $\langle 1/k \rangle$ is cyclic. $\square$

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)

Problem:	**5A**
No. stars:	**2**

Statement: Prove that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. Suppose $G/Z(G)$ is cyclic. Then there exists an $a \in G$ such that $G/Z(G) = \langle aZ(G) \rangle$. Now, by Proposition 4 from Section 3.1 in Dummit and Foote, we have that the set of left cosets of $Z(G)$ forms a partition of G. Hence, each $g \in G$ occurs in one and only of the left cosets of $Z(G)$. Thus, every $g \in G$ can written in the form $a^k z$ for some $z \in Z(G)$ and for some k such that $1 \leqslant k \leqslant |a|$.

Now let us fix $g_1, g_2 \in G$. From the above, we can write $g_1 = a^k z_1$ and $g_2 = a^m z_2$. Then we have,

$$g_1 g_2 = a^k z_1 a^m z_2$$

Since every element in $Z(G)$ commutes with all elements of G and powers of a commute with each other, we derive the following equality,

$$\begin{aligned} g_1 g_2 &= a^k z_1 a^m z_2 \\ &= a^m z_2 a^k z_1 \\ &= g_2 g_1 \end{aligned}$$

Since g_1, g_2 were arbitrary in G, this holds for all elements of G and hence it is an abelian group.

□

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)

Statement: For some fixed $g \in G$, prove that conjugation by g (i.e. the map $G \to G$ defined by $a \mapsto gag^{-1}$) is an automorphism of G. Deduce that a and gag^{-1} have the same order, and for any non-empty $S \subseteq G$, the map

$$S \to gSg^{-1} \quad \text{defined by} \quad s \mapsto gsg^{-1}$$

is also a bijection.

Problem:	**3A**
No. stars:	**2**

Proof. Fix $g \in G$. Define $\varphi_g(a) = gag^{-1}$ for every $a \in G$. In order to show that φ_g is an automorphism of G, we must show that φ_G is a bijection from to G to G and that

$$\varphi_g(ab) = \varphi_g(a)\varphi_g(b)$$

for all $a, b \in G$.

First, we have that ϕ_g is well-defined. This is true because G is a group, so $gag^{-1} \in G$ for every $a \in G$.

Now fix $a, b \in G$ and suppose $\varphi_g(a) = \varphi_g(b)$. Then we have,

$$\begin{aligned} &\varphi_g(a) = \varphi_g(b) \\ \implies &gag^{-1} = gbg^{-1} \end{aligned}$$

Multiplying by g^{-1} on the left and g on the right on both sides of the equal signs yields

$$a = b$$

Hence, φ_g is injective.

Now fix $c \in G$. Since G is a group, we have $g^{-1}cg \in G$. Hence this gives us that,

$$\begin{aligned} \varphi_g(g^{-1}cg) &= g(g^{-1}cg)g^{-1} \\ &= c \end{aligned}$$

Since c was arbitrary, this holds for every element in G. Hence, φ is surjective as well and is thus a bijection from G to G.

Now we will check the homomorphism property. Fix $a, b \in G$. Then,

$$\begin{aligned} \varphi_g(ab) &= gabg^{-1} \\ &= ga(g^{-1}g)bg^{-1} \\ &= (gag^{-1})(gbg^{-1}) \\ &= \varphi_g(a)\varphi_g(b) \end{aligned}$$

Hence, φ_g is a bijective homorphism and thus an automorphism of G. So we have $|a| = |\varphi_g(a)| = |gag^{-1}|$ as a consequence of φ_g being an automorphism.

Now for any non-empty $S \subset G$ we consider the map

$$S \to gSg^{-1} \text{ defined by } s \to gsg^{-1}$$

Since every element of S is an element of G and G is a group, we have that $gsg^{-1} \in G$ for every $g \in G$ and $s \in S$. Hence, for every g, we have that

$$gSg^{-1} \subset G$$

So our map sends the subsets of G to the subsets of G. Let $S, R \in \mathcal{P}(G)\backslash\varnothing$. Suppose $gSg^{-1} = gRg^{-1}$. Then we have

$$\begin{aligned}(g^{-1}g)S(g^{-1}g) &= (g^{-1}g)R(g^{-1}g) \\ \implies S &= R\end{aligned}$$

So our map is injective. Now let $S \in \mathcal{P}(G)\backslash\varnothing$. Observe, that since G is a group, for every $s \in S$, there exists an element $g^{-1}sg \in G$. Hence, we can define the set $R \subset G\backslash\varnothing$ such that every element $r \in R$ is defined to be $g^{-1}sg$ for some $s \in S$. Ensure that each s is used to define exactly one r. Then, we have for all $r \in R$,

$$\begin{aligned}grg^{-1} &= g(g^{-1}sg)g^{-1} \\ &= s\end{aligned}$$

Hence, we have that $gRg^{-1} = S$, and so our map is surjective and hence bijective.

Now consider again sets $S, R \in \mathcal{P}(G)\backslash\varnothing$. Then we have

$$\begin{aligned}gSRg^{-1} &= gS(g^{-1}g)Rg^{-1} \\ &= (gSg^{-1})(gRg^{-1})\end{aligned}$$

So the map is homomorphism and hence an isomorphism. $\square$

	Points Possible					
complete	0	1	2	3	4	5
mathematically valid	0	1	2	3	4	5
readable/fluent	0	1	2	3	4	5
Total:	(out of 15)					

Statement: Let G be a group. Show that the map

$$\varphi : G \to G \qquad \text{defined by} \quad \varphi : g \mapsto g^{-1}$$

is a homomorphism if and only if G is abelian. Now, verify that

$$\psi : D_{2n} \to D_{2n} \text{ defined by } \quad \psi(s) = s^{-1} \text{ and } \psi(r) = r^{-1}$$

extends to a well-defined homomorphism, and explain why this does not contradict the first statement.

Problem:	**2B**
No. stars:	**2**

Proof. Suppose φ is a homomorphism. Then $\varphi(xy) = \varphi(x)\varphi(y)$ for every $x, y \in G$. By the definition of φ we have

$$\begin{aligned} \varphi(xy) &= y^{-1}x^{-1} \\ &= \varphi(x)\varphi(y) \\ &= x^{-1}y^{-1} \end{aligned}$$

Hence $y^{-1}x^{-1} = x^{-1}y^{-1}$ for every $x, y \in G$. Thus, G is abelian. Now suppose G is abelian. Then for every $x, y \in G$, we have that $xy = yx$.

Define the map $\varphi : G \to G$ by $\varphi : g \to g^{-1}$. Then we have,

$$\begin{aligned} \varphi(xy) &= (xy)^{-1} \\ &= y^{-1}x^{-1} \end{aligned}$$

and

$$\varphi(x)\varphi(y) = x^{-1}y^{-1}$$

Since G is abelian, we can rewrite

$$\begin{aligned} \varphi(x)\varphi(y) &= x^{-1}y^{-1} \\ &= y^{-1}x^{-1} \end{aligned}$$

Hence we have that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$, so φ is a homomorphism.

Now consider the map ψ as described above.

□

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)

Statement: If the center of G is of index n, prove that every conjugacy class has at most n elements.

Problem:	**7B**
No. stars:	**1**

Proof. Suppose the center of G, $Z(G) = \{g \in G \mid gx = gx \text{ for all } x \in G\}$, is of index n. That is, the number of left cosets of $Z(G)$ in G is n. Now fix $a \in G$. By Proposition 6 in Section 4.3 of Dummit and Foote, we have that the number of conjugates of a is $|G : C_G(a)|$. Note that $C_G(a) = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}$. In other words, $C_G(s)$ is the set of elements in G which commute with s. Since all of the elements of $Z(G)$ commute with every element of G, we must have that $Z(G) \subset C_G(a)$. Hence, we have that $|G/C_G(a)| \leqslant |G/Z(G)| = n$ and so the number of conjugates of a is at most n. Since a was arbitrary in G, this holds for all elements of G and thus for all conjugacy classes, as required. $\square$

	Points Possible					
complete	0	1	2	3	4	5
mathematically valid	0	1	2	3	4	5
readable/fluent	0	1	2	3	4	5
Total:				(out of 15)		

Statement: Show that $2\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic as groups but not as rings.

Problem:	**9B**
No. stars:	**1**

Proof. We have that $2\mathbb{Z}$ is an infinite cyclic group with generator $\langle 2 \rangle$ and $3\mathbb{Z}$ is an infinite cyclic group with generator $\langle 3 \rangle$. Hence, any isomorphism from $2\mathbb{Z}$ to $3\mathbb{Z}$ must map ± 2 to ± 3. Without loss of generality, let us thus define $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ by $\varphi(2k) = 3k$. Let us show that this defines a group isomorphism. Fix $x, y \in 2\mathbb{Z}$ and suppose $\varphi(x) = \varphi(y)$. Then $x = 2n$ and $y = 2m$ for some $n, m \in \mathbb{Z}$ and we have,

$$\begin{aligned} &\varphi(x) = \varphi(y) \\ \implies &\varphi(2n) = \varphi(2m) \\ \implies &3n = 3m \\ \implies &n = m \\ \implies &x = y \end{aligned}$$

Hence, we have that φ is injective. Now let $z \in 3\mathbb{Z}$. Hence, $z = 3k$ for some $k \in \mathbb{Z}$. Then we have that $\varphi(2k) = 3k$, and so φ is surjective. Thus, φ is a bijective. Again consider $x = 2n$ and $y = 2m$. Then we have,

$$\begin{aligned} \varphi(x+y) &= \varphi(2n + 2m) \\ &= \varphi(2(n+m)) \\ &= 3(n+m) \\ &= 3n + 3m \\ &= \varphi(2n)\varphi(2m) \\ &= \varphi(x)\varphi(y) \end{aligned}$$

Now fix $2, 4 \in 2\mathbb{Z}$. We have $2 = 2 \cdot 1$ and $4 = 2 \cdot 2$. Thus, applying φ yields,

$$\begin{aligned} \varphi(2 \cdot 4) &= \varphi(8) \\ &= \varphi(2 \cdot 4) \\ &= 3 \cdot 4 \\ &= 12 \end{aligned}$$

However, $\varphi(2)\varphi(4) = (3 \cdot 1) \cdot (3 \cdot 2) = 18$. Hence, $\varphi(2 \cdot 4) \neq \varphi(2)\varphi(4)$ and so φ is not a ring isomorphism.

Thus, φ is a group isomorphism. $\square$

	Points Possible					
complete	0	1	2	3	4	5
mathematically valid	0	1	2	3	4	5
readable/fluent	0	1	2	3	4	5
Total:						(out of 15)

Problem:	**10A**
No. stars:	**1**

Statement: Prove that if M is an ideal such that R/M is a field then M is a maximal ideal (do not assume R is commutative).

Proof. Suppose M is an ideal such that R/M is a field. Recall that a field is a commutative ring with identity in which every nonzero element has an inverse. That is, for every $x + M \in R/M$ with $x \neq 0$, there exists a $y + M \in R/M$ such that $(x + M)(y + M) = 1 + M$. Now let N be an ideal such that $M \subset N$. Also let $x \in N$ such that $x \notin M$. As a result, we have that $x + M \neq 0 + M \in R/M$. Since R/M is a field, there is a $y + M \in R/M$ such that $(x + M)(y + M) = 1 + M$. Now, by Proposition 6 in Section 7.3 of DF, we can reformulate $(x + M)(y + M)$ as $xy + M$. Hence, we have,

$$xy + M = 1 + M$$

Since $xy = 1$ from the above, we know that $y = x^{-1}$. Since $x \in N$ and N is an ideal, we must have that $y = x^{-1} \in N$ as well.

Now, because R/M is a group under addition (as a consequence of being a field), we can apply Proposition 4 from Section 3.1 of DF and state,

$$xy - 1 \in M$$

That is, there exists an $m \in M$ such that $xy - 1 = m$. This implies that $1 = xy - m$. But note that $x, y, m \in N$. As a result, we have that $1 = xy - m \in N$. By Proposition 9(1) in Section 7.4 of DF, this gives us that $N = R$. Hence, the only ideal of R which contains M is R itself. We now need to show that $M \neq R$ in order to show that it is a maximal ideal. If $M = R$, then $R/M = R/R = 0$. Since a field must have two distinct identities, one additive and one multiplicative, R/R is not a field. Thus, we have a contradiction and so $M \neq R$, as required. As a result, M is a maximal ideal of R. □

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)

Problem:	3C
No. stars:	2

Statement: For which $n \in \mathbb{Z}_{\geqslant 1}$ is $(\mathbb{Z}/2^n\mathbb{Z})^\times$ cyclic? Prove your claim.

Proof. Let $n \geqslant 3$ and consider $2^{n-1}+1$ and $2^{n-1}-1$. We have,

$$(2^{n-1}+1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \mod 2^n$$
$$(2^n(n-1)-1)^2 = 2^{2n-2} - 2^n + 1 \equiv 1 \mod 2^n$$

Thus, we have that $2^{n-1}+1 \mod 2^n \neq 2^{n+1}-1 \mod 2^n$ (i.e. they are distinct elements), but both elements have order 2. Note that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ can be represented by a subset of the following equivalence classes: $\{\bar{1}, \ldots, \overline{2^n-1}\}$. That is, the group is finite with size at most 2^n-1. Let us assume that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic. Hence, there exists an $x \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ such that $2^{n-1}+1 = x^\ell$ and $2^{n-1}-1 = x^m$ for some $\ell, m \in \mathbb{Z}$. Since $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is a finite group, we can apply Proposition 2 from Section 2.3 in DF, which states that $x^{2^n-1} = 1$ and $1, x, x^2, \ldots, x^{2^n-2}$ are all distinct elements. Thus, we know $\ell, m \in \{1, 2, 3, \ldots, 2^n-1\}$ and $\ell \neq m$ since $2^{n-1}+1 \mod 2^n \neq 2^{n+1}-1 \mod 2^n$.

Now recall that we have $|x^\ell| = |x^m| = 2$. This implies that,

$$(2^n-1) \mid 2\ell \text{ and } (2^n-1) \mid 2m$$

But since $1 \leqslant \ell, m \leqslant 2^n-1$, we have that $2 \leqslant 2\ell, 2m \leqslant 2(2^n-1) < 2 \cdot 2^n$. Hence, the only way for $|x^\ell| = 2 = |x^m|$ is if $2\ell, 2m = 2^n-1$. But this implies that $\ell, m = 2^{n-1}-1/2$ and so $x^m = x^\ell$. This is a contradiction since $2^{n-1}+1 \mod 2^n \neq 2^{n+1}-1 \mod 2^n$, so $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic when $n \geqslant 3$.

Now let us examine $(\mathbb{Z}/2^2\mathbb{Z})^\times = (\mathbb{Z}/4\mathbb{Z})^\times$. This group has the following elements: $\{\bar{1}, \bar{3}\}$. We have that $\bar{3}^2 = \bar{9} = \bar{1}$ and $\bar{3}^1 = \bar{3}$, so this group is generated by $\langle \bar{3} \rangle$.

Finally, we will examine $(\mathbb{Z}/2^1\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^\times$. This group has the following elements: $\{\bar{1}\}$. We have that $\bar{1}^1 = \bar{1}$, so this group is generated by $\langle \bar{1} \rangle$. Hence, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic when $n = 1$ or $n = 2$. $\square$

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)