# Math 206A: Algebra

## Midterm 1 Solutions

Friday, October 30, 2020.

### Problems

1. State the First Isomorphism Theorem.

   **Solution**: Let $\varphi\colon G \to H$ be a homomorphism between groups $G$ and $H$. Then $\ker(\varphi)$ is a normal subgroup of $G$ and
   $$G/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

2. What is the order of the automorphism group of $\mathbb{Z}/8\mathbb{Z}$?
   **No explanation is necessary, you can just write a number.**

   **Solution**: We know that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, the group of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ under multiplication. We know that $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$.
   Therefore, we see that $|\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})| = 4$.

3. For which integers $n \geq 2$ is the group $\{\mathrm{id}, (12)\}$ a normal subgroup of $S_n$?
   **Prove that your answer is correct.**

   **Solution**: When $n = 2$ this subgroup is all of $S_2$, so it is normal. For $n \geq 3$ we claim that this subgroup is not normal. A subgroup $H$ is normal in $G$ if and only if $gHg^{-1} = H$ for all $g \in G$. Let $H = \{\mathrm{id}, (12)\}$. We see that $(2,3)^{-1} = (2,3)$ and that
   $$(2,3)H(2,3) = \{\mathrm{id}, (2,3)(1,2)(2,3)\} = \{\mathrm{id}, (1,3)\} \neq H,$$
   so $H$ is not normal in $S_n$.

4. (a) **Either prove that the following statement is true or give a counterexample showing that it is false**: Suppose $G$ is a group. If $H$ is a normal subgroup of $G$ and $K$ is a normal subgroup of $H$, then $K$ is a normal subgroup of $G$.
   **Solution**: This is false. Let $G = S_4$, $H = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, and $K = \{\mathrm{id}, (1,2)(3,4)\}$. We see that $H$ is normal in $G$ because it is a union of two conjugacy classes (the identity and the set of all permutations of cycle type $(2,2)$). We see that $K$ is normal in $H$ because it has index 2. But, $K$ is not normal in $G$ because it is not a union of conjugacy classes.

   (b) **Either prove that the following statement is true or give a counterexample showing that it is false**: Suppose $G$ is a group and $H, K$ are subgroups of $G$ such that $K \leq H$. If $K$ is a normal subgroup of $G$, then $K$ is a normal subgroup of $H$.
   **Solution**: This is true. If $K$ is normal in $G$ then $gKg^{-1} = K$ for all $g \in G$. Since $H \leq G$, then clearly $hKh^{-1} = K$ for all $h \in H$, and $K$ is normal in $H$.

5. Show that for any $n \geq 3$, $A_n$ contains a subgroup isomorphic to $S_{n-2}$.

**Solution**: Consider the function $\varphi \colon S_{n-2} \to A_n$ defined by

$$\begin{array}{rcll} \varphi(\sigma) & = & \sigma & \text{if } \sigma \text{ is even.} \\ \varphi(\sigma) & = & \sigma(n-1, n-2) & \text{if } \sigma \text{ is odd.} \end{array}$$

Since the product of an odd permutation and a transposition is even, this function really does take $S_{n-2}$ to $A_n$. Clearly it is injective– since $\sigma \in S_{n-2}$ is a permutation of $\{1, 2, \ldots, n-2\}$, it is clear that $\sigma(n-1, n) \neq \text{id}$.

We check that $\varphi$ is a homomorphism.

(a) Suppose $\sigma_1, \sigma_2 \in S_{n-2}$. If both are even, then so is $\sigma_1\sigma_2$. We have

$$\varphi(\sigma_1)\varphi(\sigma_2) = \sigma_1\sigma_2 = \varphi(\sigma_1\sigma_2).$$

(b) If $\sigma_1$ is odd and $\sigma_2$ is even, then $\sigma_1\sigma_2$ is odd and

$$\varphi(\sigma_1)\varphi(\sigma_2) = (\sigma_1(n-1, n))\sigma_2 = \sigma_1\sigma_2(n-1, n) = \varphi(\sigma_1\sigma_2).$$

(c) If $\sigma_1$ is even and $\sigma_2$ is odd, then $\sigma_1\sigma_2$ is odd and

$$\varphi(\sigma_1)\varphi(\sigma_2) = \sigma_1(\sigma_2(n-1, n)) = \varphi(\sigma_1\sigma_2).$$

(d) If both are odd, then $\sigma_1\sigma_2$ is even. We have

$$\varphi(\sigma_1)\varphi(\sigma_2) = (\sigma_1(n-1, n))(\sigma_2(n-1, n)) = \sigma_1\sigma_2(n-1, n)^2 = \sigma_1\sigma_2 = \varphi(\sigma_1\sigma_2).$$

By the First Isomorphism Theorem, $S_{n-2}/\ker(\varphi) = S_{n-2}$ is isomorphic to a subgroup of $A_n$.

6. Let $G$ be a finite group and $g \in G$. Let $\mathcal{K}$ be the conjugacy class of $g$.
Show that $|\mathcal{K}|$ divides $|G|$.

**Solution**: Let $G$ act on itself by conjugation. The orbit of $g$ is $\mathcal{K}$, so by the orbit-stabilizer theorem we have

$$|\mathcal{K}| = \frac{|G|}{|\operatorname{Stab}_g|}.$$

We have $\operatorname{Stab}_g$ is equal to the centralizer of $g$, which is a subgroup of $G$.

Since $|\mathcal{K}||C_G(g)| = |G|$, we see that $|\mathcal{K}|$ divides $|G|$.

7. **Either prove that the following statement is true or give a counterexample showing that it is false**: Suppose that $G_1$ and $G_2$ are finite groups such that for each positive

integer $n$, $G_1$ and $G_2$ have the same number of conjugacy classes of size $n$. Then $G_1$ and $G_2$ are isomorphic.

**Solution**: This is false. In an abelian group every conjugacy class has size 1. So, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ are two non-isomorphic groups that each have four conjugacy classes of size 1 and no other conjugacy classes.
(You can see that they are not isomorphic by noting that one is cyclic and the other is not.)

8. Let $G$ be a finite nontrivial $p$-group. Prove that $Z(G)$ is nontrivial.

   **Solution**: Let $g_1, \ldots, g_r$ be representatives of the conjugacy classes of $G$ of size larger than 1. By the class equation,
   $$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$
   Since $g_i$ is in a conjugacy class of size greater than 1, we see that $[G : C_G(g_i)] > 1$. Since $[G : C_G(g_i)]$ divides $|G|$, we see that $[G : C_G(g_i)] \equiv 0 \pmod{p}$. Also, $p$ divides $|G|$, so $p$ must also divide $|Z(G)|$. Since $1 \in Z(G)$, we see that $|Z(G)| \geq p$. Therefore $Z(G)$ is nontrivial.

9. State Sylow's Theorem.

   **Solution**: Let $G$ be a finite group and let $p$ be a prime dividing $|G|$. Let $|G| = p^\alpha m$ where $p \nmid m$. A Sylow $p$-subgroup of $G$ is a subgroup of order $p^\alpha$. Let $\mathrm{Syl}_p(G)$ denote the set of Sylow $p$-subgroups of $G$ and let $n_p = |\mathrm{Syl}_p(G)|$.

   (a) $\mathrm{Syl}_p(G) \neq \emptyset$. That is, $n_p \geq 1$.
   (b) All Sylow $p$-subgroups are conjugate to each other.
   (c) $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$.
   (d) $n_p = [G : N_G(P)]$ where $P$ is some Sylow $p$-subgroup and $N_G(P)$ is its normalizer.

10. (a) Let $G$ be a group and $x \in G$ have order $k$. Prove that $x^n = 1$ if and only if $k \mid n$.
    **Solution**: By the division algorithm, there exist unique integers $q, r$ with $0 \leq r < k$ with $n = qk + r$. We have
    $$x^n = x^{qk+r} = x^{qn} \cdot x^r = (x^k)^q \cdot x^r = 1^q \cdot x^r = x^r.$$
    Since the order of $x$ is $k$ we see that $x^n = 1$ if and only if $r = 0$. This occurs if and only if $k \mid n$.

    (b) Suppose $G$ is a group and $x, y \in G$ satisfy $xy = yx$. Suppose that the order of $x$ is $n$ and the order of $y$ is $m$ where $\gcd(n, m) = 1$. Prove that the order of $xy$ is $nm$.
    **Solution**: We show that $n$ divides the order of $xy$ and that $m$ divides order of $xy$. Because $\gcd(n, m) = 1$, this implies that $nm$ divides the order of $xy$. Note that because $xy = yx$, we see that
    $$(xy)^{nm} = x^{nm} y^{nm} = (x^n)^m (y^m)^n = 1.$$

So $nm$ is some positive integer $k$ for which $(xy)^k = 1$, so since $nm$ divides the order of $xy$, we see that $nm$ **is** the order of $xy$.
Let $k$ denote the order of $xy$. Then

$$(xy)^k = x^k y^k = 1.$$

We see that

$$(xy)^{nk} = x^{nk} y^{nk} = (x^n)^k y^{nk} = y^{nk}.$$

By the first part of this problem, $m$ divides $nk$. Since $\gcd(n,m) = 1$, we must have $m$ divides $k$.
We see that

$$(xy)^{mk} = x^{mk} y^{mk} = x^{mk} (y^m)^k = x^{mk}.$$

By the first part of this problem, $n$ divides $mk$. Since $\gcd(n,m) = 1$, we must have $m$ divides $k$.
**Note**: A lot of people tried to argue like this. Let $k$ be the order of $xy$. Then $(xy)^k = x^k y^k = 1$. This is only possible if $x^k = 1$ and $y^k = 1$. So by part (a) we have $m \mid k$ and $n \mid k$ and therefore $\operatorname{lcm}(m,n) \mid k$. Since $\gcd(m,n) = 1$ we have $\operatorname{lcm}(m,n) = mn$. So $mn \leq k$. Since $(xy)^{mn} = 1$ we see that $k = mn$.
The problem with this argument is the assertion that $x^k y^k = 1$ implies $x^k = 1$ and $y^k = 1$. This needs to be justified. Here's one way: Suppose $x^k y^k = 1$ but $x^k \neq 1$ or $y^k \neq 1$. It is clear that both $x^k \neq 1$ and $y^k \neq 1$. We see that $y^k$ is a nontrivial element of $\langle x \rangle$ and clearly $y^k \in \langle y \rangle$, so $\langle y^k \rangle$ is a nontrivial subgroup of $\langle x \rangle \cap \langle y \rangle$. But, by Lagrange's theorem, $|\langle y^k \rangle|$ divides $m$ and also divides $n$. Since $\gcd(m,n) = 1$, we see that $|\langle y^k \rangle| = 1$, which contradicts the assumptions that $y^k \neq 1$.
Here's another way to justify this: Suppose $x^k y^k = 1$. So $x^k = y^{-k}$. Proposition 5 in Section 2.3 of Dummit and Foote says that the order of $x^k$ is $\frac{n}{\gcd(n,k)}$ and that the order of $y^k$ is $\frac{m}{\gcd(m,k)}$. So $\frac{n}{\gcd(n,k)} = \frac{m}{\gcd(m,k)}$. Since $\frac{n}{\gcd(n,k)} \mid n$ and $\frac{m}{\gcd(m,k)} \mid m$, the condition that $\gcd(m,n) = 1$ implies that $\frac{n}{\gcd(n,k)} = \frac{m}{\gcd(m,k)} = 1$. Therefore, $n \mid k$ and $m \mid k$, and again since $\gcd(n,m) = 1$ we have $mn \mid k$. Since $(xy)^{mn} = 1$ we have $k \mid mn$ also, so $k = mn$.