Math 230A: Algebra
Midterm 1 Solutions
Wednesday, October 19, 2022.

Problems

1. State the **Second Isomorphism Theorem**.

   Solution: Let G be a group and $A, B \leq G$ satisfying $A \leq N_G(B)$. Then, $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $A/(A \cap B) \cong AB/B$.

2. Let G be a group and H, K be subgroups of G.
   Consider the set $HK = \{hk \colon h \in H,\ k \in K\}$. Does HK always have to be a subgroup of G?

   Solution: HK does not have to be a subgroup if H is not contained in the normalizer for K in G. So we should pick K not to be a normal subgroup of G. (In fact, we want both H and K not to be normal in G. Can you see why?) For example, we can take $K = \langle sr \rangle$ and $H = \langle s \rangle$ in $G = D_6$. In this case, we have $HK = \{1, s, sr, srs\} = \{1, s, sr, r^2\}$, since $rs = sr^2$. We see that HK is not a subgroup of G since it does not contain $s \cdot sr = r$.

3. Let G be a group and A be a nonempty subset of G.

   (a) Define the **centralizer** $C_G(A)$ of A in G.

   (b) Define the **normalizer** $N_G(A)$ of A in G.

   (c) Prove that $C_G(A)$ is a normal subgroup of $N_G(A)$.

   Note: You may use the fact that $C_G(A)$ and $N_G(A)$ are subgroups of G without proving it.

   Solution: $C_G(A) = \{g \in G \colon ga = ag \text{ for all } a \in A\}$. $N_G(A) = \{g \in G \colon gAg^{-1} = A\}$.

   We want to show that for all $g \in N_G(A)$ we have $gC_G(A)g^{-1} = C_G(A)$.

   It is enough to show that for all $x \in C_G(A)$ we have $gxg^{-1} \in C_G(A)$. That is, we need to show that for $x \in C_G(A)$ and $g \in N_G(A)$, we have $gxg^{-1}a = agxg^{-1}$ for all $a \in A$.

   Multiply each side of the equation

   $$gxg^{-1}a = agxg^{-1}$$

   by g^{-1} on the left and by g on the right to see that this is equivalent to

   $$x(g^{-1}ag) = (g^{-1}ag)x.$$

   Since $g \in N_G(A)$ and $N_G(A) \leq G$ we have $g^{-1} \in N_G(A)$. Therefore, $g^{-1}ag = a'$ for some $a' \in A$ by the definition of $N_G(A)$. Since $x \in C_G(A)$ we have $xa' = a'x$.

   This completes the proof.

4. Are $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ isomorphic?
Either give an isomorphism between them or prove that no isomorphism exists.

Solution: These groups are not isomorphic. The main idea is to show that no homomorphism from $\mathbb{Z}$ to $\mathbb{Q}$ can be surjective. We argue by contradiction.

Suppose $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ is a homomorphism. Since $\mathbb{Z} = \langle 1 \rangle$ we have $\varphi(n) = n \cdot \varphi(1)$ for any integer n. Let $\varphi(1) = a/b$. It is clear that multiplying a/b by n does not increase the denominator, so the image of this homomorphism does not contain rational numbers with arbitrarily large denominators. Therefore, φ cannot be surjective, so it cannot be an isomorphism.
(This proof is basically the same as showing that $(\mathbb{Q}, +)$ is not cyclic.)

5. Suppose G is a group acting on a set X. Prove that different orbits of this group action are disjoint and that these orbits partition the set X.

Solution: (This is Theorem 3.16(a) in Conrad's 'Group Actions' notes.)

Suppose that $z \in \mathrm{Orb}_x \cap \mathrm{Orb}_y$. We want to show that $\mathrm{Orb}_x = \mathrm{Orb}_y$. Since $z \in \mathrm{Orb}_x$, there exists $g \in G$ such that $g \cdot x = z$. Since we have a group action

$$g^{-1} \cdot z = g^{-1} \cdot (g \cdot x) = x.$$

Since $z \in \mathrm{Orb}_y$, there exists $g' \in G$ such that $g' \cdot y = z$. Therefore,

$$g^{-1} g' \cdot y = g^{-1} \cdot (g' \cdot y) = g^{-1} \cdot z = x.$$

We see that $x \in \mathrm{Orb}_y$. Similarly, for any $u = g^* \cdot x$ we have $g^* g^{-1} g' \cdot y = g^* \cdot x = u$, which means $u \in \mathrm{Orb}_y$. This shows that $\mathrm{Orb}_x \subseteq \mathrm{Orb}_y$. A totally parallel argument with x and y reversed shows that $\mathrm{Orb}_y \subseteq \mathrm{Orb}_x$.

We now need only note that the union of the different orbits includes all the elements of X. Every element $x \in X$ is in some orbit since clearly $x \in \mathrm{Orb}_x$.

6. (a) Let G be a group and define the set of squares in G to be $S = \{g^2 \colon g \in G\}$.
Suppose $H \leq G$ is a subgroup of index 2. Prove that $S \subseteq H$.
   (b) Define the set of cubes in G to be $C = \{g^3 \colon g \in G\}$. Suppose $K \leq G$ is a subgroup of index 3. Do we have to have $C \subseteq K$?
Explain how you know your answer is correct.

Solution: Since H has index 2 in G it is normal in G. Since G/H has order 2 every $x \in G/H$ satisfies $x^2 = 1H$. Consider the natural projection homomorphism $\pi\colon G \to G/H$. We have $\pi(g^2) = \pi(g)^2 = 1H$. Since $\pi(g^2) = g^2 H = 1H$, we have $g^2 \in H$.

For the second part, C does not have to be in every subgroup of index 3.
For example, consider the subgroup $\langle s \rangle \subseteq D_6$. We have that $(sr)^3 = sr \in C$, but $sr \notin \langle s \rangle$.

7. For each part of this problem, **explain how you know your answer is correct**.

   (a) For which positive integers n does S_n contain a subgroup isomorphic to $\mathbb{Z}/7\mathbb{Z}$?

   (b) For which positive integers n does S_n contain a subgroup isomorphic to $\mathbb{Z}/10\mathbb{Z}$?

   Solution: Every $\sigma \in S_n$ has a decomposition into a product of disjoint cycles. The important thing to remember is that these disjoint cycles partition $\{1, 2, \ldots, n\}$, and the order of σ is the least common multiple of the lengths of the cycles. So for the first part, we need a bunch of cycles whose lengths add up to n and have least common multiple equal to 7. If the lcm of a set of numbers is 7 then at least one of these numbers must be equal to 7. Therefore, we must have $n \geq 7$. We can think of the 7-cycle $\sigma = (1234567)$ as being an element of S_n for any $n \geq 7$ by just saying that σ fixes $\{8, 9, \ldots, n\}$.

   For the second part, if the lcm of a bunch of numbers is 10, then at least one of the numbers has to be divisible by 5 and at least one of the numbers must be divisible by 2. The smallest n for which we can do this is $n = 7$ where we can have the product of a 5-cycle and a disjoint 2-cycle, something like $\sigma = (12345)(67)$. As above, we can think of this as an element of S_n for any $n \geq 7$.

8. Suppose G is a cyclic group. Prove that every subgroup H of G is cyclic.

   Solution: (This is Theorem 2.1 in Conrad's notes 'Subgroups of Cyclic Groups'.)

   Suppose $G = \langle x \rangle$. If H is trivial, it is $\langle 1 \rangle$. Suppose H is not trivial. There is a minimum positive integer d such that $x^d \in H$.

   To see this, it is enough to note that H contains x^m for some positive integer m. We know that H contains some nonidentity element $y \in G$. Since $G = \langle x \rangle$, we have $y = x^m$ for some m. If m is negative, we know that H is a subgroup, which implies that $y^{-1} = x^{-m} \in H$. (You did not have to justify this part to get full credit on this problem.)

   We claim that $H = \langle x^d \rangle$. Since $x^d \in H$, it is clear that $\langle x^d \rangle \subseteq H$. We show inclusion the other way. Suppose $y \in H$. Since $y \in G = \langle x \rangle$ we have $y = x^m$ for some m. We apply the division algorithm to write $m = qd + r$ for some $r \in \{0, 1, 2 \ldots, d-1\}$. Since $x^d \in H$ we see that $x^{-qd} \in H$, and $y \cdot x^{-qd} = x^r \in H$. Since d was chosen to be the minimum positive integer for which $x^d \in H$, we must have $r = 0$. Therefore $y = x^{qd} \in \langle x^d \rangle$.

9. (a) Suppose G is a group acting on a set X. (You may assume this is a left group action.) Define the stabilizer of x.

   Solution: $\text{Stab}_x = \{g \in G \colon g \cdot x = x\}$.

   (b) Let G be a group and $H \leq G$. We know that G acts on the set of left cosets of H in G by left multiplication. What is the stabilizer of the element $aH \in G/H$?
   Solution:

$$\text{Stab}_{aH} = \{g \in G \colon g \cdot aH = aH\} = \{g \in G \colon gaH = aH\}.$$

We recall that $xH = yH$ if and only if $y^{-1}x \in H$. Therefore,

$$\text{Stab}_{aH} = \{g \in G \colon a^{-1}ga \in H\}.$$

We see that $a^{-1}ga \in H$ if and only if $g \in aHa^{-1}$.

10. Let G be a finite simple group having a subgroup H of prime index p.
    Show that p is the largest prime divisor of $|G|$.

    Solution: G acts on the set of left cosets of H in G. We have $|G/H| = p$. This group action gives a homomorphism $\psi \colon G \to S_{G/H} \cong S_p$. We see that $\ker(\psi) \trianglelefteq G$. Since G is simple $\ker(\psi)$ is either trivial or is all of G. We note that $g \in \ker(\psi)$ implies $g \cdot 1H = gH = 1H$, so $g \in H$. Since $H \neq G$, we see that $\ker(\psi) \neq G$. Therefore, $\ker(\psi)$ is trivial. By the First Isomorphism Theorem, $G \cong \psi(G) \leq S_{G/H}$. By Lagrange's theorem, we must have $|G|$ divides $|S_{G/H}| = p!$. We conclude that G cannot have a prime factor larger than p. So p must be the **largest** prime dividing $|G|$.