Math 230A: Algebra

Final Exam: Solutions

Thursday, December 8, 2022.

Problems

1. Is the following statement True or False? Explain how you know that your answer is correct.

   Every element of the symmetric group S_6 has order at most 6.

   Solution: Let $\sigma \in S_n$ be a permutation. The order of σ is the least common multiple of the lengths of the cycles when you write σ as a product of disjoint cycles. Here are the possibilities for the cycle structure of a permutation $\sigma \in S_6$:

   $$(6), (5,1), (4,2), (4,1,1), (3,3), (3,2,1), (3,1,1,1), (2,2,2), (2,2,1,1), (1,1,1,1,1,1).$$

   We see that in every case the least common multiple is at most 6. So this is true.

2. Is the following statement True or False? Explain how you know that your answer is correct.

   For each $n \geq 3$, the automorphism group of the symmetric group S_n contains a subgroup isomorphic to S_n.

   Solution: This is true. We first recall that the subgroup of inner automorphisms of a group G, those automorphisms that come from $x \to gxg^{-1}$ where $g \in G$ is fixed, is isomorphic to $G/Z(G)$. Since $Z(S_n)$ is trivial for $n \geq 3$, we see that the subgroup of $\mathrm{Aut}(S_n)$ consisting of inner automorphisms is isomorphic to S_n.

3. Is the following statement True or False? Explain how you know that your answer is correct.

   Any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

   Solution: This is true. A subfield F of $\mathbb{R}$ must contain the multiplicative identity 1 of $\mathbb{R}$. (If $x \in F$ is nonzero, $y = 1$ is the unique element of $\mathbb{R}$ such that $x \cdot y = x$, so if F has any multiplicative identity, it must be 1.)

   Since F is a subgroup of $\mathbb{R}$, it contains $\mathbb{Z}$. Let $n \in \mathbb{Z}$. Since $n \in F$ we must have $1/n \in F$. Since F is closed under addition, we have $\frac{m}{n} \in F$ for any $m \in \mathbb{Z}$. Therefore, F contains $\mathbb{Q}$.

4. Consider the subset R of $M_2(\mathbb{R})$ consisting of matrices of the form

   $$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

(a) Prove that R is a subring of $M_2(\mathbb{R})$.

(For this problem we are using the definition of a subring from Dummit and Foote where a subring does not necessarily have to contain the multiplicative identity of $M_2(\mathbb{R})$. But, note that in this case R does contain I_2, so don't worry about it.)

Solution: We need only show that this set is a subgroup under addition and that it is closed under multiplication. Note that

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} + (-1) \cdot \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ b-d & a-c \end{pmatrix} \in R.$$

By the subgroup criterion, R is a subgroup.

We now check that

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{pmatrix} \in R.$$

So R is a subring.

(b) Prove that R is a commutative ring with 1, but is not an integral domain.

Solution: If we take the computation we just did and exchange a and c, and exchange b and d, then we see the product we computed is unchanged. That is, multiplication is commutative. Setting $a = 1$ and $b = 0$ we see that R contains a multiplicative identity, I_2. We see that R is not an integral domain because

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(c) Recall that an element x is an *idempotent* if $x^2 = x$. Find all idempotents in R.

Solution

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & 2ab \\ 2ab & a^2+b^2 \end{pmatrix}.$$

So we get an idempotent if and only if $a = a^2 + b^2$ and $2ab = b$. This second equation implies that $(2a-1)b = 0$.

Since $\mathbb{R}$ is an integral domain, there are two cases. If $b = 0$ then we need only have $a = a^2$, which holds if and only if $a \in \{0, 1\}$. If $b \neq 0$, then $2a = 1$ and $a = \frac{1}{2}$. In this case we get an idempotent if and only if $\frac{1}{4} = b^2$, which happens if and only if $b \in \{\pm\frac{1}{2}\}$.

(d) Define $\varphi\colon R \to \mathbb{R}$ by

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \to a - b.$$

Show that φ is a ring homomorphism.

(In this problem we use the Dummit and Foote definition of a ring homomorphism, so it is not required that φ takes the identity to the identity. In this case, the homomorphism does take the identity to the identity, so you don't need to worry about this distinction.)

Solution: Let

$$A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}, \; M = \begin{pmatrix} c & d \\ d & c \end{pmatrix}.$$

We have

$$\varphi(A + M) = (a + c) - (b + d) = (a - b) + (c - d) = \varphi(A) + \varphi(M).$$

By the computation above, we have

$$\varphi(A \cdot M) = (ac + bd) - (ad + bc) = (a - b)(c - d) = \varphi(A) \cdot \varphi(M).$$

(e) Determine the kernel of φ as well as $R/\ker(\varphi)$.

Solution: $A \in \ker(\varphi)$ if and only if $b = a$, which means

$$A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}.$$

(f) Is $\ker(\varphi)$ a prime ideal? Is $\ker(\varphi)$ a maximal ideal? Explain how you know.

Solution: By choosing $b = 0$ and $a \in \mathbb{R}$ is clear that this ring homomorphism is surjective. By the First Isomorphism Theorem for Rings, $R/\ker(\varphi) \cong \mathbb{R}$. Since $\mathbb{R}$ is both an integral domain and a field, we see that $\ker(\varphi)$ is prime and maximal.

5. Let G be a group and M, N be normal subgroups of G.
Prove that $G/(M \cap N)$ is isomorphic to a subgroup of $(G/M) \times (G/N)$.

Solution: Consider the homomorphism $\varphi \colon G \to (G/M) \times (G/N)$ defined by

$$\varphi(x) = (xM, xN).$$

(It is clear that this is a group homomorphism, but if you want to write the details, just note that by the definition of multiplication in a quotient group,

$$(xM, xN) \cdot (yM, yN) = (xyM, xyN),$$

so we have $\varphi(xy) = \varphi(x) \cdot \varphi(y)$.)

We see that $x \in \ker(\varphi)$ if and only if $xM = 1M$ and $xN = 1N$. The first condition is equivalent to $x \in M$ and the second is equivalent to $x \in N$. Taken together we conclude that $x \in \ker(\varphi)$ if and only if $x \in M \cap N$. By the First Isomorphism Theorem for Groups, $G/\ker(\varphi) \cong \varphi(G)$, which is a subgroup of $(G/M) \times (G/N)$, since the image of a group homomorphism is always a subgroup.

6. Assume that all rings in this question are commutative with a multiplicative identity $1 \neq 0$. For each of the following, either give an example (with an explanation) of such an ideal, or explain why such an example does not exist:

   (a) A prime ideal P in a finite ring R that is not a maximal ideal.

   Solution: In a commutative ring R with identity $1 \neq 0$, for any ideal I of R, we have I is prime if and only if R/I is an integral domain, and I is maximal if and only if R/I is a field. Therefore, we are looking for a finite ring R with an ideal I for which R/I is an integral domain, but not a field. But, since R is finite, R/I is finite. We proved that a finite integral domain is a field. Therefore, I is prime implies that I is maximal, so such an example does not exist.

   (b) A prime ideal P in an integral domain R that is nonzero but not a maximal ideal.

   Solution: Let $R = \mathbb{Z}[x]$. This is an integral domain since $\mathbb{Z}$ is an integral domain. Let $P = (x)$. We have $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is an integral domain that is not a field. (We can see this quotient by noting that (x) is the kernel of the ring homomorphism where we send $p(x)$ to $p(0)$.)

7. Let G be a finite group and let p be a prime dividing $|G|$. Prove that there is a unique Sylow p-subgroup of G if and only if any Sylow p-subgroup of G is normal in G.

   Solution: Suppose $P, Q \in \mathrm{Syl}_p(G)$. By Sylow II, P and Q are conjugate in G. That is, there exists $g \in G$ for which $gPg^{-1} = Q$. Therefore, if P is normal in G, then $Q = P$.

   Now suppose there is a unique Sylow p-subgroup P in G. We know that G acts on the set its subgroups of given size by conjugation. Therefore, for any $g \in G$, we have gPg^{-1} is a subgroup of G of order equal to $|P|$. Since P is the only subgroup of G of order equal to $|P|$, we must have gPg^{-1} for all g, which means that P is normal in G.

8. Let G be a group of order 12. Prove that G is isomorphic to a semidirect product $H \rtimes_\varphi K$ where $H, K \leq G$ are proper non-trivial subgroups of G.

   Solution: $12 = 2^2 \cdot 3$. By Sylow III, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4$. Therefore, $n_3 \in \{1, 4\}$.

   (a) Suppose that $n_3 = 1$. Let Q be the unique Sylow 3-subgroup of G. Since it is unique, it must be normal in G. Let $P \in \mathrm{Syl}_2(G)$. We see that $PQ \leq G$ since $Q \trianglelefteq G$. By Lagrange's theorem, $P \cap Q$ is trivial (its order must divide both 4 and 3). Therefore,

   $$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = 12,$$

   which means that $PQ = G$. By the Recognition Theorem for Semidirect Products, $G \cong Q \rtimes_\varphi P$, where $\varphi \colon P \to \mathrm{Aut}(Q)$ is defined by conjugation.

(b) Suppose $n_3 = 4$. Since G contains 4 subgroups of order 3, it contains 8 elements of order 3. There are only 4 elements of G that do not have order 3. A Sylow 2-subgroup of G has 4 elements, and does not have any elements of order 3, so it must consist of the 4 elements of G that do not have order 3. Since this is true of any Sylow 2-subgroup, there is a unique Sylow 2-subgroup P of G, so it is normal in G.

Using the same reasoning as above, $PQ \leq G$, $|P \cap Q| = 1$, $PQ = G$, and by the Recognition Theorem for Semidirect Products, $G \cong P \rtimes_\varphi Q$, where $\varphi\colon Q \to \mathrm{Aut}(P)$ is defined by conjugation.

9. Does there exist a group G and a subgroup $H \leq G$ such that G is a simple group and H is not a simple group? Either give an example or prove that no such example exists.

Solution: There are lots of examples like this. For example, A_9 is simple and A_9 contains a 9-cycle. This 9-cycle generates a subgroup isomorphic to $\mathbb{Z}/9\mathbb{Z}$, which is not simple because it has a proper normal subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

10. (a) State Cauchy's Theorem.

Solution: Let G be a finite group of order n and let p be a prime dividing $|G|$. Then G contains an element of order p.

(b) State Cayley's Theorem.

Solution: Let G be a group (not necessarily finite). Then G is isomorphic to a subgroup of S_G, the set of permutations of the elements of G.

(c) State the Third Isomorphism Theorem for Groups.

Solution: Let G be a group and H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$