Math 206A: Algebra
Final Exam Solutions
Thursday, December 17, 2020.

Solutions

1. (a) Define a field.

   Solution: A field is a commutative ring with identity $1 \neq 0$ where every nonzero element is a unit.

   (b) Define an integral domain.

   Solution: An integral domain is a commutative ring with identity $1 \neq 0$ that has no zero divisors.

   (c) Prove that a finite integral domain is a field.

   Solution: Let R be a finite integral domain and let $x \in R$ be a nonzero element. We will show that x is a unit. This will show that every nonzero element of R is a unit. We conclude that R is a field.

   Consider the map $\varphi \colon R \to R$ defined by $\varphi(a) = a \cdot x$. We show that it is injective. An injective map between finite sets of the same size is automatically surjective. Once we know φ is surjective, there exists $y \in R$ such that $\varphi(y) = yx = 1$. Since R is commutative $xy = 1$ also. So x is a unit.

   We now need only prove that φ is injective. Suppose that $\varphi(a) = \varphi(b)$. This implies $ax = bx$. This means $ax - bx = (a - b)x = 0$. Since R is an integral domain, $a - b$ and x are not zero divisors. Therefore, $a - b = 0$ or $x = 0$. Since we assumed $x \neq 0$, we know that $a - b = 0$, so $a = b$. Therefore, φ is injective.

2. Decide which of the following are subrings of $\mathbb{Q}$. Give a brief justification for your answer.

   (a) The set of nonnegative rational numbers.

   Solution: This is not a subring of $\mathbb{Q}$ because it is not an additive subgroup of $\mathbb{Q}$. For example 1 does not have an additive inverse.

   (b) The set of all rational numbers with odd numerators (when written in lowest terms)

   Solution: This is not a subring of $\mathbb{Q}$ because it is not an additive subgroup of $\mathbb{Q}$. For example 1 is in this set, but $1 + 1 = 2$ is not in this set.

   (c) The set of all rational numbers with even numerators (when written in lowest terms)

   Solution: This is a subring of $\mathbb{Q}$. We first check that it is an additive subgroup of $\mathbb{Q}$. The set consists of all rational numbers $\frac{2a}{b}$ where a is any nonzero integer, b is a nonzero odd positive integer and $\gcd(a, b) = 1$, and also 0. We see that

$$\frac{2a_1}{b_1} - \frac{2a_2}{b_2} = \frac{2a_1b_2 - 2a_2b_1}{b_1b_2}.$$

This fraction may not be in lowest terms, but since b_1b_2 is odd, when we write it in lowest terms, the denominator is odd. By the subgroup criterion, this set is an additive subgroup of $\mathbb{Q}$.

We now show that this set is closed under multiplication. We have

$$\frac{2a_1}{b_1} \cdot \frac{2a_2}{b_2} = \frac{4a_1a_2}{b_1b_2}.$$

This fraction may not be in lowest terms, but since b_1b_2 is odd, when we write it in lowest terms, the denominator is odd.

Note: For this question we are using Dummit and Foote's definition of a subring. That is, a subring does not necessarily have to contain an identity.

3. Decide which of the following are ideals of $\mathbb{Z}[x]$:

   (a) The set of all polynomials whose coefficient of x^2 is a multiple of 3.

   Solution: This is not an ideal because it is not closed under left multiplication by elements of $\mathbb{Z}[x]$. For example, $1 + 0x^2$ is in this set, but $x^2 = x^2(1 + 0x^2)$ is not.

   (b) The set of all polynomials whose constant term, coefficient of x, and coefficient of x^2 are zero.

   Solution: This is an ideal of $\mathbb{Z}[x]$. The set described here is the set of all polynomials divisible by x^3. This is the ideal generated by x^3.

   (c) The set of all polynomials whose coefficients sum to zero.

   Solution: This is an ideal of $\mathbb{Z}[x]$. The set described here is the set of $p(x) \in \mathbb{Z}[x]$ such that $p(1) = 0$, since $p(1)$ is the sum of the coefficients of $p(x)$. This is the set of all polynomials divisible by $x - 1$, which is the ideal generated by $x - 1$.

4. Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. Explain how you know your list is complete.

   Note: For this question we are using Dummit and Foote's definition of a ring homomorphism. That is, a ring homomorphism $\varphi\colon R \to S$ between rings with identities does not necessarily have to take the identity of R to the identity of S.

   Solution: A group homomorphism from a cyclic group G to another group is determined by where it sends a generator of G. Therefore, we need only consider $\varphi\colon \mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$ defined by $\varphi(1) = x$. We check which of these group homomorphisms have the property that $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, and are therefore ring homomorphisms.

We first note that
$$x = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = x^2.$$
So we need only consider x for which $x^2 = x$ in $\mathbb{Z}/30\mathbb{Z}$, or equivalently $x^2 - x = x(x-1) \equiv 0 \pmod{30}$.

It is not difficult to see that this holds if and only if each of $2, 3$ and 5 divide either x or $x - 1$. That is, x is either: a multiple of 5 or one more than a multiple of 5, a multiple of 3 or one more than a multiple of 3, and a multiple of 2 or one more than a multiple of 2. This last condition is always satisfied and the first two are easy to check.

We see that the only possibilities are $x \in \{0, 1, 6, 10, 15, 16, 21, 25\}$.

We claim that each of these values of x determines a ring homomorphism. We have
$$\varphi(a) = \varphi(1 + \cdots + 1) = a \cdot \varphi(1) = ax.$$
Similarly,
$$\varphi(b) = \varphi(1 + \cdots + 1) = b \cdot \varphi(1) = bx,$$
and
$$\varphi(ab) = \varphi(1 + \cdots + 1) = ab \cdot \varphi(1) = abx.$$
Now,
$$\varphi(a) \cdot \varphi(b) = (ax)(bx) = abx^2 = abx = \varphi(ab).$$

5. (a) State the Orbit-Stabilizer Theorem.

   Solution: $|\operatorname{Orb}_x| = [G\colon \operatorname{Stab}_x]$.

   (b) Let G be a finite p-group acting on a finite set X. Prove that
$$|X| \equiv \#\{\text{Fixed points of this action}\} \pmod{p}.$$

   Solution: Let $x_1, \ldots, x_r$ be representatives of the orbits of this action of size larger than 1. Since the orbits of a group action partition X, we have
$$|X| = \#\{\text{Fixed points of this action}\} + \sum_{i=1}^{r} |\operatorname{Orb}_{x_i}|.$$
   By the Orbit-Stabilizer Theorem, we have $|\operatorname{Orb}_{x_i}| = [G\colon \operatorname{Stab}_{x_i}]$ for each i. Since $|\operatorname{Orb}_{x_i}| > 1$, we know that $[G\colon \operatorname{Stab}_{x_i}] > 1$ for each i. The index of a proper subgroup of G divides $|G|$, so we see that for each i, $[G\colon \operatorname{Stab}_{x_i}] \equiv 0 \pmod{p}$. Therefore,
$$\begin{aligned} |X| &= \#\{\text{Fixed points of this action}\} + \sum_{i=1}^{r} |\operatorname{Orb}_{x_i}| \\ &\equiv \#\{\text{Fixed points of this action}\} + \sum_{i=1}^{r} |\operatorname{Orb}_{x_i}| \pmod{p} \\ &\equiv \#\{\text{Fixed points of this action}\} \pmod{p}. \end{aligned}$$

6. Does there exist a group G where $G \times G$ contains an element of order 15, but G does not contain an element of order 15?
   Either give an example of such a G or prove that such an example does not exist.

   Solution: Yes. Take $G = S_5$. The element $((1,2,3),(1,2,3,4,5))$ has order $15 = \mathrm{lcm}(3,5)$ in $S_5 \times S_5$. But, S_5 has no element of order 15. The order of an element in S_n is the least common multiple of its cycle lengths when written as a product of disjoint cycles. So the only elements of order divisible by 5 in S_5 are the 5-cycles, which all have order 5.

7. Let $p < q$ be odd primes. Let G be a group of order $2pq$.

   (a) Prove that G is not simple.

   Solution: We use the fact that for a prime r dividing $|G|$ a Sylow r-subgroup of G is normal if and only if $n_r = 1$.

   By Sylow III, we have $n_q \equiv 1 \pmod{q}$ and $n_q \mid 2p$. Since $q > 2$ and $q > p$, if G is simple we must have $n_q = 2p$. This means that G contains $2p(q-1)$ elements of order q. We also have $n_p \equiv 1 \pmod{p}$ and $n_p \mid 2q$. If G is simple, $n_p \neq 1$ and therefore $n_p \geq q$. So n_p has at least $q(p-1)$ elements of order p. But then, G contains at least $2p(q-1) + q(p-1) > 2pq$ elements (note that $q \geq 5$), which is a contradiction.

   (b) Define what it means for a group to be solvable.

   Solution: A group G is solvable if there exist a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G,$$

   where each G_i is a normal subgroup of G_{i+1} and each quotient G_{i+1}/G_i is abelian.

   (c) Prove that G is solvable.

   Solution: Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G. In the first part we proved that either $P \trianglelefteq G$ or $Q \trianglelefteq G$. Either way, PQ is a subgroup of G of order pq. Since this subgroup has index 2, it is normal in G. Now, $G/PQ \cong \mathbb{Z}/2\mathbb{Z}$ is abelian.

   Let H be either P or Q, whichever one is normal in G. Since H is normal in G it is also normal in PQ. Since PQ/H has prime order, it is cyclic, and therefore abelian.

   We see that

$$1 \trianglelefteq H \trianglelefteq PQ \trianglelefteq G,$$

   is a sequence of subgroups showing that G is solvable.

8. (a) Describe the conjugacy classes of S_4.

   (b) How many elements are in each conjugacy class?

Solution: The conjugacy classes of S_n correspond to cycle types. Therefore, in S_4 we have conjugacy classes consisting of all elements of cycle type: $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$. There are

$$\begin{aligned}
\binom{4}{4} \cdot (4-1)! &= 6 \quad \text{permutations of cycle type } (4), \\
\binom{4}{1} \cdot (3-1)! &= 8 \quad \text{permutations of cycle type } (3,1), \\
\binom{4}{2}/2 &= 3 \quad \text{permutations of cycle type } (2,2), \\
\binom{4}{2} \cdot 1! &= 6 \quad \text{permutations of cycle type } (2,1,1), \\
1 &= 1 \quad \text{permutation of cycle type } (1,1,1,1).
\end{aligned}$$

9. (a) Prove that a subgroup of a cyclic group is cyclic.

   Solution: Let $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ be a cyclic group. The trivial subgroup is cyclic: $\{1\} = \langle 1 \rangle$.

   Let H be a nontrivial subgroup of G. So H contains $x^n \neq 1$ for some $n \in \mathbb{Z}$. Since H is closed under taking inverses, H contains x^{-n} also. Since $x^n \neq 1$, we see that $x^{-n} \neq 1$ also. Therefore, H contains an element $x^m \neq 1$ for some positive integer m.

   Let m be the smallest positive integer for which $x^m \in H$. We claim that $H = \langle x^m \rangle$. Suppose that $y \in H$. Then $y = x^s$ for some integer s. By the division algorithm, $s = qm + r$ for some $0 \leq r < m$. Since $x^m \in H$, we have

   $$x^s \cdot (x^m)^{-q} = x^{qm+r} \cdot x^{-qm} = x^r \in H.$$

   Since we assumed that m was the smallest positive integer for which $x^m \in H$, we must have $r = 0$. Therefore $x^s = (x^m)^q \in \langle x^m \rangle$, completing the proof that $H = \langle x^m \rangle$.

   (b) Is the automorphism group of a cyclic group necessarily cyclic? Explain your answer.

   Solution: No. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, and $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not cyclic.

10. Let G be a group of order 42.

   (a) Prove that G has a subgroup of order 6.

   Solution: By Sylow III, $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 21$. So $n_2 \in \{1, 3, 7, 21\}$. Next, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 14$. So $n_3 = 1$ or $n_3 = 7$. Finally, $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 6$, so $n_7 = 1$.

   Let P be a Sylow 2-subgroup of G and Q be a Sylow 3-subgroup of G. If n_3 or n_2 is equal to 1, then PQ is a subgroup of G of order 6. If $n_3 \neq 1$, then $n_3 = 7 = [G : N_G(Q)]$, so $N_G(Q)$ is a subgroup of G of order 6.

   So, in any case G has a subgroup H of order 6.

(b) Prove that G has a subgroup of order 21.

Solution: Let N be the unique Sylow 7-subgroup of G. So $N \trianglelefteq G$. Then QN is a subgroup of G. We know that $|QN| = \frac{|Q||N|}{|Q| \cap |N|}$. By Lagrange's Theorem, $Q \cap N = 1$. So QN is a subgroup of G of order 21.

(c) Prove that G is isomorphic to a semidirect product of two nontrivial groups.

Solution: The Recognition Theorem for Semidirect Products states that if H, N are two subgroups of G such that $HN = G$, $H \cap N = 1$, and $H \trianglelefteq G$, then $G \cong H \rtimes_{\varphi} N$, where φ is the action of N on H by conjugation.

We can use either of the previous two parts to finish this problem. By Lagrange's Theorem, $H \cap N = 1$. So $HN = G$. Since $N \trianglelefteq G$, we see that $G \cong N \rtimes H$. Since QN is a subgroup of G of index 2, $QN \trianglelefteq G$. By Lagrange's Theorem, $P \cap QN = 1$. So $P(QN) = G$. We see that $G \cong QN \rtimes P$.

11. Either prove the following statement or give a counterexample.
For any group G, the map $\varphi\colon G \to G$ defined by $\varphi(g) = g^2$ is a homomorphism.

Solution: This is false in general for groups that are not abelian. Let $G = S_3$, $x = (1, 2)$, $y = (1, 3)$. Then $\varphi(x) = \varphi(y) = 1$, but

$$\varphi(xy) = \varphi(1, 3, 2) = (1, 2, 3).$$

Since $\varphi(x)\varphi(y) \neq \varphi(xy)$, we see that φ is not a homomorphism.