MT310.01: Introduction to Abstract Algebra
Final Examination
Answers

1. *(10 points)* The following sets are all commutative rings: **Z**, **Q**, **R**, **C**, **Z**/2**Z**, **Z**/3**Z**, **Z**/4**Z**, **Z**/5**Z**, and **Z**/6**Z**. Which of these rings are integral domains? Which are fields?

You do not need to justify your answers to this question.

Answer: The integral domains are **Z**, **Q**, **R**, **C**, **Z**/2**Z**, **Z**/3**Z**, and **Z**/5**Z**. The fields are **Q**, **R**, **C**, **Z**/2**Z**, **Z**/3**Z**, and **Z**/5**Z**.

2. *(10 points)* (a) State Eisenstein's Criterion.

(b) Let n be a positive integer, and let k be an integer which is bigger than 1. Prove that $\sqrt[k]{25n+15}$ is irrational.

Answer: (a) If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial in $\mathbf{Z}[x]$, and

(1) $p \nmid a_n$.
(2) $p|a_{n-1}$, …, $p|a_1$, $p|a_0$.
(3) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $\mathbf{Q}[x]$.

(b) Consider the polynomial $x^k - (25n+15)$, with k and n as above. Eisenstein's Criterion says that this polynomial is irreducible in $\mathbf{Q}[x]$, because

(1) $5 \nmid 1$.
(2) $5|25n+15$.
(3) $25 \nmid 25n+15$.

Because the polynomial is irreducible in $\mathbf{Q}[x]$, we know that it cannot have a factor of the form $x - \frac{p}{q}$. Therefore, the roots of the polynomial are irrational, so $\sqrt[k]{25n+15}$ is irrational.

3. *(10 points)* Suppose that F is a field, and $f(x)$ is an element of $F[x]$. Prove or give a counterexample to each of the following statements:

(a) If $f(x)$ is irreducible, then $f(x^2)$ is irreducible.
(b) If $f(x^2)$ is irreducible, then $f(x)$ is irreducible.

A counterexample means finding a specific field F and specific polynomial $f(x)$ that makes the statement false.

Answer: (a) This statement is false. One simple counterexample is given by $f(x) = x - 1$, which is irreducible, while $f(x^2) = x^2 - 1 = (x+1)(x-1)$.

(b) This statement is true. Suppose that $f(x)$ is reducible, so that $f(x) = g(x)h(x)$, with $\deg(g(x)) \geq 1$ and $\deg(h(x)) \geq 1$. We then have $f(x^2) = g(x^2)h(x^2)$, with $\deg(g(x^2)) \geq 2$ and $\deg(h(x^2)) \geq 2$. This shows that $f(x^2)$ is reducible.

4. *(10 points)* Suppose that $\phi : G_1 \to G_2$ is a homomorphism of groups. Prove or give a counterexample:

(a) If $H_1 \triangleleft G_1$, then $\phi(H_1) \triangleleft G_2$
(b) If $H_2 \triangleleft G_2$, then $\phi^{-1}(H_2) \triangleleft G_1$.

As usual, $\phi(H_1)$ is defined with the equation

$$\phi(H_1) = \{\phi(h_1) : h_1 \in H_1\}$$

and $\phi^{-1}(H_2)$ is defined with the equation

$$\phi^{-1}(H_2) = \{g_1 \in G_1 : \phi(g_1) \in H_2\}.$$

Finding a counterexample means finding specific groups G_1 and G_2, a specific homomorphism ϕ, and a specific normal subgroup which makes the statement false.

Be sure not to assume in your proofs that ϕ is either injective or surjective.

Answer: (a) This statement is *false*. The easiest way to find a counterexample is to let G_1 be an abelian group, so that every subgroup is normal, and to let G_2 be S_3, because we know from homework problems that $\{e, (12)\}$ is a subgroup of S_3 which is not normal.

One possibility is to let $G_1 = \mathbf{Z}$, and define $\phi(n) = (12)^n$. In other words,

$$\phi(n) = \begin{cases} (12) & n \text{ is odd} \\ e & n \text{ is even} \end{cases}$$

Now, let $H_1 = 3\mathbf{Z}$, the subgroup of all multiples of 3. We know that $3\mathbf{Z} \triangleleft \mathbf{Z}$, because $\mathbf{Z}$ is abelian, and $\phi(H_1) = \{e, (12)\}$, which is not a normal subgroup of S_3.

(b) This statement is *true*. Let $h_1 \in \phi^{-1}(H_2)$, and $g_1 \in G_1$. We need to show that $g_1 h_1 g_1^{-1} \in \phi^{-1}(H_2)$.

Because $h_1 \in \phi^{-1}(H_2)$, we have $\phi(h_1) \in H_2$, and therefore if g_2 is any element of G_2, we know that $g_2 \phi(h_1) g_2^{-1} \in H_2$. In particular, if $g_2 = \phi(g_1)$, we have $\phi(g_1 h_1 g_1^{-1}) = \phi(g_1)\phi(h_1)\phi(g_1)^{-1} \in H_2$. This shows that $g_1 h_1 g_1^{-1} \in H_2$.

5. *(10 points)* Suppose that $\phi : R_1 \to R_2$ is a homomorphism of rings. Prove or give a counterexample:

(a) If I_1 is an ideal of R_1, then $\phi(I_1)$ is an ideal in R_2

(b) If I_2 is an ideal of R_2, then $\phi^{-1}(I_2)$ is an ideal in R_1.

Finding a counterexample means finding specific rings R_1 and R_2, a specific homomorphism ϕ, and a specific ideal which makes the statement false.

Be sure not to assume in your proofs that ϕ is either injective or surjective.

Answer: (a) This statement is *false*. A simple counterexample is to take $R_1 = \mathbf{Z}$, and $R_2 = \mathbf{Q}$, with the homomorphism $\phi(n) = n$. Let $I_1 = 2\mathbf{Z}$, the ideal of even integers. Then $\phi(I_1)$ is also the set of even integers, but inside the ring $\mathbf{Q}$, the set of even integers is not an ideal. For example, 2 is an even integer, and $\frac{1}{2} \in \mathbf{Q}$, and their product is not an even integer.

(b) This statement is true. Suppose that $i, j \in \phi^{-1}(I_2)$. Then we know that $\phi(i), \phi(j) \in I_2$, and because I_2 is an ideal, we know that $\phi(i) + \phi(j) \in I_2$. That shows that $\phi(i + j) \in I_2$, or $i + j \in \phi^{-1}(I_2)$.

Now let $r \in R_1$. We need to show that ir and $ri \in \phi^{-1}(I_2)$. We know that $\phi(i) \in I_2$, and therefore $r_2\phi(i)$ and $\phi(i)r_2 \in I_2$ for any $r_2 \in R_2$, because I_2 is an ideal. In particular, we let $r_2 = \phi(r)$, and then $\phi(r)\phi(i)$ and $\phi(i)\phi(r) \in I_2$. That shows that $\phi(ri)$ and $\phi(ir) \in I_2$, or $ri, ir \in \phi^{-1}(I_2)$.

6. *(5 points)* Suppose that R is a commutative ring, and the only ideals of R are $\{0\}$ and R. Prove that R is a field.

Answer: We need to show that any non-zero element of R has an inverse in R. Let r be such an element. The ideal (r) cannot be the zero ideal, because $r \neq 0$. Therefore $(r) = R$. Because $1 \in R$, we know that there is some element $s \in R$ so that $rs = 1$. This shows that r has an inverse.

7. *(10 points)* Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 5 & 2 & 3 & 7 & 6 & 9 & 8 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 8 & 9 & 5 & 7 & 2 & 1 & 3 & 4 \end{pmatrix}$$

(a) Write $\sigma \circ \tau$ in cycle notation.
(b) What is the order of σ?
(c) What is the order of τ?
(d) Is σ even or odd?
(e) Is τ even or odd?

Be sure to justify your answers.

Answer: We have $\sigma = (142)(35)(67)(89)$ and $\tau = (162839457)$.

(a) Therefore, $\sigma \circ \tau = (1743856)(29)$.

(b) $o(\sigma) = 6$.

(c) $o(\tau) = 9$.

(d) $\sigma = (142)(35)(67)(89) = (12)(14)(35)(67)(89)$, the product of an odd number of transpositions, and therefore σ is *odd*.

(e) $\tau = (17)(15)(14)(19)(13)(18)(12)(16)$, the product of an even number of transpositions, and therefore τ is *even*.

8. *(15 points)* Remember that A_4 consists of the 12 elements in S_4 which are even permutations. Let $H = \{e, (12)(34), (13)(24), (14)(23)\}$. You may assume without proof that H is a subgroup of A_4.

(a) Show that H is group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
(b) List the left and right cosets of H in A_4.
(c) Is H a normal subgroup of A_4?

Answer: Here are the group operation tables for both H and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$:

$\cdot$	e	$(12)(34)$	$(13)(24)$	$(14)(23)$
e	e	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	e	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	e	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	e

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

(a) You can see from the group operation tables that any bijection between A_4 and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is a group isomorphism.

(b) We have

$$H = \{e, (12)(34), (13)(24), (14)(23)\} \qquad H = \{e, (12)(34), (13)(24), (14)(23)\}$$
$$H(123) = \{(123), (243), (142), (134)\} \qquad (123)H = \{(123), (134), (324), (142)\}$$
$$H(132) = \{(132), (143), (342), (124)\} \qquad (132)H = \{(132), (234), (124), (143)\}$$

(c) A bit of inspection shows that left and right cosets are equal (remember that, for example, $(342) = (234)$). Therefore, H is a normal subgroup of A_4.

9. *(10 points)* Suppose that G is an abelian group with 6 elements. Show that G is isomorphic to $\mathbf{Z}/6\mathbf{Z}$.

Answer: By Cauchy's Theorem, G contains an element a with $o(a) = 2$ and an element b with $o(b) = 3$. Because a and b commute, we can cite a homework problem to conclude that $o(ab) = 6$. Let $c = ab$, and we know that G is a cyclic group generated by c, so $G = \{e, c, c^2, c^3, c^4, c^5\}$. Now the function $\phi : G \to \mathbf{Z}/6\mathbf{Z}$ given by $\phi(c^n) = [n]_6$ is an isomorphism.

10. *(10 points)* Suppose that G is a nonabelian group with 6 elements. Show that G is isomorphic to S_3.

Answer: By Cauchy's Theorem, G contains an element a with $o(a) = 2$ and an element b with $o(b) = 3$. We can list the 6 elements of G as $\{e, b, b^2, a, ab, ab^2\}$.

We need to compute ba. We cannot have $ba = e$, or else $b = a^{-1}$. We cannot have $ba = b$, or else $a = e$. We cannot have $ba = b^2$, or else $a = b$. We cannot have $ba = a$, or else $b = e$. If $ba = ab$, then a and b commute, $o(ab) = 6$, G is cyclic, and therefore G is abelian.

The only possibility is that $ba = ab^2$. We can now compute for example that $b^2a = b(ba) = b(ab^2) = (ba)b^2 = ab^4 = ab$. Similar computations allow us to write out the complete group operation table for G:

$\cdot$	e	b	b^2	a	ab	ab^2
e	e	b	b^2	a	ab	ab^2
b	b	b^2	e	ab^2	a	ab
b^2	b^2	e	b	ab	ab^2	a
a	a	ab	ab^2	e	b	b^2
ab	ab	ab^2	a	b^2	e	b
ab^2	ab^2	a	ab	b	b^2	e

Here is the operation table for S_3:

$\cdot$	e	(123)	(132)	(12)	(23)	(13)
e	e	(123)	(132)	(12)	(23)	(13)
(123)	(123)	(132)	e	(13)	(12)	(23)
(132)	(132)	e	(123)	(23)	(13)	(12)
(12)	(12)	(23)	(13)	e	(123)	(132)
(23)	(23)	(13)	(12)	(132)	e	(123)
(13)	(13)	(12)	(23)	(123)	(132)	e

Now inspection shows that these are the same group operation tables with the mapping $\phi(e) = e$, $\phi(b) = (123)$, $\phi(b^2) = (132)$, $\phi(a) = (12)$, $\phi(ab) = (23)$, and $\phi(ab^2) = (13)$.

Grade	Number of people
70	1
52	1
51	1
48	1
38	1
37	1
36	1
24	1

Mean: 44.50
Standard deviation: 13.00