

Abstract Algebra, Final Exam Solutions

Name:

1. RING THEORY

a) Definitions:

- Ring: A set equipped with two binary operations $(+, *)$ such that the $+$ structure is an additive group, the $*$ structure is associative and has an identity, and $*$ is distributive over $+$.
- Integral Domain: A ring without zero divisors.
- Principal Ideal Domain: An integral domain in which every ideal is principal.
- Field: A ring in which every non-zero element is invertible.

$\mathbb{Z}[x]$ is an integral domain but not a principal ideal domain.

b)

- $\{f : f(1) = 0\}$ This is an ideal: if $f(1) = 0$ and $g(1) = 0$ then $(f+g)(1) = 0$, and if $f(1) = 0$ then $(fh)(1) = 0$ for any $h(x)$. It is a prime ideal: if $(fg)(1) = 0$ then $f(1) = 0$ or $g(1) = 0$. It is not a maximal ideal since it is the ideal $\langle x - 1 \rangle$ which is contained in the ideal $\langle x - 1, 3 \rangle$.
- $\{f : f(0) = 1\}$ This is not an ideal: if $f(0) = 1$ and $g(0) = 1$ then $(f+g)(0) = 2$.
- $\{f : 6|f\}$ This is the principal ideal $\langle 6 \rangle$. It is not prime since $2 * 3 \in I$ but $2 \notin I$ and $3 \notin I$.
- $\{f : f(x) = xg(x) + 2, g(x) \in \mathbb{Z}[x]\}$ This is not an ideal because it is not closed under $+$.
- $\{f : f(x) = xg(x) + 2n, g(x) \in \mathbb{Z}[x]; n \in \mathbb{Z}\}$ This is the maximal ideal $\langle x, 2 \rangle$.

c)

- $\mathbb{Z}[x]/\langle x - 1 \rangle \cong \mathbb{Z}$, by the Fundamental Homomorphism Theorem. It is an integral domain because $\langle x - 1 \rangle$ is prime.
- $\mathbb{Z}[x]/\langle 6 \rangle \cong \mathbb{Z}_6[x]$ by the Fundamental Homomorphism Theorem. It is not an integral domain because $\langle 6 \rangle$ is not prime.
- $\mathbb{Z}[x]/\langle x, 2 \rangle \cong \mathbb{Z}_2$ by the Fundamental Homomorphism Theorem. It is a field because $\langle x, 2 \rangle$ is a maximal ideal.

d) The kernel of $\phi: \mathbb{Z}[x] \rightarrow \mathbb{Z}_6[x, y]$ is the ideal $\langle 6 \rangle$ in $\mathbb{Z}[x]$. The image is the subring $\mathbb{Z}_6[x] \subset \mathbb{Z}_6[x, y]$.

EXTRA CREDIT) The quotient rings of $\mathbb{Z}[x]$ are all the images of homomorphisms from $\mathbb{Z}[x]$. They are commutative rings generated by 1 and one other element ($\phi(x)$). Conversely, any commutative ring R generated by 1 and an element r is the image of a homomorphism $\mathbb{Z}[x] \rightarrow R$ given by $x \mapsto r$.

Name:

2. PERMUTATION GROUPS

Let $G = A_4$ be the group of even permutations on 4 elements.

a) The conjugates of (123) in S_4 are the 8 3-cycles. But it is not possible to get from (123) to (132) by conjugation in A_4 , since the only elements of A_4 that fix 4 are (123) and (132) and conjugation by them preserves (123) . On the other hand, it is possible to change from a 3-cycle with fixed point 4 to a 3-cycle with any other given fixed point, by conjugating by a pair of disjoint transpositions. For instance to get from (123) to something that preserves 3, we conjugate by $(12)(34)$ and obtain (214) . So there are two conjugacy classes of 3-cycles, each of order 4. (123) has four conjugates in A_4 . Alternatively, we can use the orbit-stabilizer theorem. The stabilizer of (123) under the conjugation action is the set of elements that commute with it—only the identity, (123) and (132) . So since the order of A_4 is $24/2 = 12$, the orbit has order $12/3 = 4$. The product of disjoint transpositions $(12)(34)$ has 3 conjugates in S_4 , namely the 3 possible products of disjoint transpositions. Each of these is in fact conjugate in A_4 , since we can conjugate by a 3-cycle; for instance $(12)(34)$ conjugated by (123) gives $(23)(14)$. Alternatively, the stabilizer of $(12)(34)$ is the identity and the three products of transpositions, so it has order 4. Hence by the orbit-stabilizer theorem the conjugacy class has order 3.

b) Consider the subgroup $A_3 \subset G$ of permutations that fix 4. What is its order? Prove that it is not normal. The subgroup A_3 has order 3; it is just the identity and the two 3-cycles (123) and (132) . It is not normal since (123) is conjugate to (214) which doesn't fix 4.

c) Consider the subgroup $H \subset G$ of all elements of order 2. What is its order? Prove that it is normal. The subgroup H is just the identity plus the conjugacy class of disjoint transpositions; as in part a), it has order 4. It is normal because it is a union of conjugacy classes.

d) Describe the quotient group G/H . Since G has order 12 and H has order 4, G/H has order 3, so it is the cyclic group \mathbb{Z}_3 .

EXTRA CREDIT) Since the order of a subgroup divides the order of the group, possible orders are 2, 3, 4 and 6, and the order of an element must divide the order of the subgroup. Any normal subgroup containing an element of order 2 must contain all three elements of order 2, so it contains H . If it is not H , then it must be all of G . Any normal subgroup containing an element of order 3 would have to contain the four 3-cycles conjugate to it, as well as the 4 3-cycles conjugate to its square. Already we have 8 elements, so the group must be G . There are no elements of order 4 or 6 in this group.

Name:

3. GROUP ACTIONS

Let S be the eight-sided star pictured below. In this problem we will calculate how many ways S can be painted with red, blue, yellow and green edges.

a) The group D_8 has order 16. There are 8 rotations (all the multiples of 45° , and 8 reflections. Four of the reflections are reflections over lines connecting two opposite vertices. The other four are obtained by rotating these by 45° . They are reflections over lines between two opposite concave vertices of S .

b) The orbit of an edge is the set of all edges, since any edge can be rotated onto any other. The stabilizer is the set containing the identity and reflection over the perpendicular bisector of E . $8 * 2 = 16$, so the order of the orbit times the order of the stabilizer is equal to the order of the group.

c) If E and F are adjacent, you can get from E to F by a 90° rotation or by a reflection over the axis through the vertex where they meet. If they are opposite, the rotation is 180° and the reflection is over the axis parallel to both vertices. If they lie in different squares and cross each other, then the rotation is 45° and the reflection is over the axis passing through the crossing point. If they lie in different squares and do not cross, then the rotation is by 135° and the reflection is over the axis between the crossing points equidistant from the two edges.

d) There are 8 edges, labeled 1, 2, 3, 4, 5, 6, 7, 8. Each edge has a choice of 4 colors, red, blue, yellow or green. So there are 4^8 possible colorings.

e) The orbit of an edge under the 45° rotation (or the 135° , the 225° , or the 315°) is all of S . For a coloring to be fixed under the rotation, all the elements in the orbit have to have the same color. So the only possible colorings are the four monochrome colorings. The orbit of an edge under the 90° rotation (or the 270°) is the square containing it. So each square must have the same color, but the two squares are independent of each other. So there are 4^2 possible colorings. Under the 180° rotation, the orbit of any edge is itself and its opposite edge. There are four pairs of opposite edges, each of which are independent. So there are 4^4 possible colorings. Under a reflection, the orbit of any edge is itself and its image. If the axis is the perpendicular bisector of one of the 4 pairs of opposite edges, then those two edges are preserved, while the other 6 trade places. So there are 3 fixed pairs of edges and 2 fixed edges, so there are 4^5 possible colorings that are fixed. If the axis joins two of the crossings between edges, then no edge is preserved and every edge changes places with its opposite. So there are 4 independent orbits, each consisting of a pair of edges, so there are 4^4 colorings that are fixed. Every coloring is preserved by the identity, so there are 4^8 of them.

f) Burnside's Theorem:

$$N = \frac{1}{|G|} \sum_{g \in G} \#(\text{Fix}(g)).$$

$$N = \frac{1}{16} (4(4) + 2(4^2) + 1(4^4) + 4(4^5) + 4(4^4) + 1(4^8)) = 1 + 2 + 16 + 256 + 64 + 4096 = 4435.$$

EXTRA CREDIT) The origin is the center of the star. As isometries of \mathbb{C} , the group is generated by the conjugation map $z \mapsto \bar{z}$ and multiplication by powers of $\zeta_8 = e^{i\pi/4}$. The proper isometries are the rotations $z \mapsto \zeta^n z$ and the improper isometries are the reflections $z \mapsto \zeta^n \bar{z}$. As linear maps on \mathbb{R}^2 , the group is the

subgroup of $GL_2(\mathbb{R})$ of rotation and reflection matrices by multiples of $\pi/4$

Name:

4. FIELD THEORY

Let F and G be fields.

a) Let $\phi: F \rightarrow G$ be a homomorphism. The kernel of a ring homomorphism is a proper ideal. But F is a field, so the only proper ideal is $\langle 0 \rangle$. Hence the kernel is 0 , so ϕ is injective. Alternatively, if $x \in \ker \phi$, then $\phi(x) = 0$. If $x \neq 0$, then x has a multiplicative inverse, and $\phi(x)\phi(x^{-1}) = \phi(1) = 1$, which is a contradiction. So the kernel of ϕ can only contain 0 , so ϕ is injective.

b) Assume $\text{char } F \neq 0$. If there exists a homomorphism from F to G , then $(\text{char } F)(1_F) = 0_F$, so $\phi(0_F) = (\text{char } F)(\phi(1_F)) = (\text{char } F)(1_G) = 0_G$. So $\text{char } F$ is the prime number of times that 1_G must be added to itself to get 0_G , so $\text{char } F = \text{char } G$. Assume $\text{char } F = 0$. Then $(\text{char } G)(1_G) = 0_G$, so $\text{char } G(1_F) \in \ker \phi$. But $\ker \phi = 0_F$. So $\text{char } G = 0$.

c) A homomorphism must preserve 0 and 1 , so it must preserve all of \mathbb{Z}_3 . So possible homomorphisms from the vector space to itself are the identity (which is the trivial linear transformation) and σ , which permutes the roots and acts as a rotation of the vector space around the fixed axis \mathbb{Z}_3 .

d) If F is a finite field with q elements, then all the elements of F satisfy $x^q = x$. So if ϕ is a homomorphism, then $\phi(x)^q = \phi(x^q) = \phi(x)$. So any element in the image $\phi(F)$ satisfies $x^q = x$. Since $x^q - x$ is a polynomial of degree q , it has at most q roots in the field G . But since ϕ is injective, the elements of F all have distinct images in G . So the image field $\phi(F)$ is precisely the set of roots of the polynomial $x^q - x$ in G .

e) EXTRA CREDIT: If F is allowed to be infinite, let F be the field $k(t)$ of rational functions in one variable t . Let G be the field $k(x, y)$ of rational functions in two variables x and y . Let $\phi_1: F \rightarrow G$ be given by $t \mapsto x$, and $\phi_2: F \rightarrow G$ by $t \mapsto y$. Then the image fields $\phi_1(F)$ and $\phi_2(F)$ are obviously isomorphic, but they are not the same subfield of G , since $x \in G$ is in $\phi_1(F)$ but not $\phi_2(F)$, and conversely for y .