

MATH 113 – INTRODUCTION TO ABSTRACT ALGEBRA

SECTION 2 – INSTRUCTOR: ANA CANNAS DA SILVA

SOLUTIONS TO THE PRACTICE EXAM – BERKELEY, MAY, 1998

- Each of the following four groups of questions is worth 25 points.
- Points per question within a group: a) 9, b) 6, c) 5, d) 5.
- No materials (no books, calculators, notes, etc.) are allowed during the exam.
- Please write clearly and don't forget to write your name on all pages you submit.
- Justify your answers.

For grading:

1	
2	
3	
4	
total	

NAME: _____

ID: _____

1. GROUPS

a) For each of the following descriptions, either find an object which satisfies it, or explain why such object cannot exist.

- Two groups of order four which are not isomorphic.

Answer: The groups of order 4 $\mathbb{Z}_2 \times \mathbb{Z}_2$ and \mathbb{Z}_4 are not isomorphic because \mathbb{Z}_4 is cyclic and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not (any element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2). \square

- Three different generators of the group \mathbb{Z}_{12} .

Answer: $\underline{1}, \underline{5}, \underline{7}$. In general, \underline{a} generates \mathbb{Z}_{12} if and only if $\text{g.c.d.}(a, 12) = 1$. \square

- Two different group isomorphisms from \mathbb{Z} to \mathbb{Z} .

Answer: The identity isomorphism $\phi : \mathbb{Z} \rightarrow \mathbb{Z}, \phi(a) = a$, and the isomorphism taking each element to its symmetric $\psi : \mathbb{Z} \rightarrow \mathbb{Z}, \psi(a) = -a$. (ψ is a bijection and satisfies $\psi(a + b) = -(a + b) = (-a) + (-b) = \psi(a) + \psi(b)$.) \square

b) List all elements of the factor group

$$\left(\mathbb{Z} \times \mathbb{Z}_6\right) / \langle (2, \underline{3}) \rangle$$

and find the order of the element $(1, \underline{2}) + \langle (2, \underline{3}) \rangle$ in $(\mathbb{Z} \times \mathbb{Z}_6) / \langle (2, \underline{3}) \rangle$.

Answer: $\langle (2, \underline{3}) \rangle = \{(2n, \underline{3n}) \mid n \in \mathbb{Z}\}$.

List of elements of $(\mathbb{Z} \times \mathbb{Z}_6) / \langle (2, \underline{3}) \rangle$:

$$\begin{array}{ll} (0, \underline{0}) + \langle (2, \underline{3}) \rangle & (1, \underline{0}) + \langle (2, \underline{3}) \rangle \\ (0, \underline{1}) + \langle (2, \underline{3}) \rangle & (1, \underline{1}) + \langle (2, \underline{3}) \rangle \\ (0, \underline{2}) + \langle (2, \underline{3}) \rangle & (1, \underline{2}) + \langle (2, \underline{3}) \rangle \end{array}$$

Denoting by \equiv the equivalence relation given by belonging to the same coset, we have

$$\begin{array}{l} 2(1, \underline{2}) = (1, \underline{2}) + (1, \underline{2}) \equiv (0, \underline{1}) \\ 3(1, \underline{2}) = (0, \underline{1}) + (1, \underline{2}) \equiv (1, \underline{0}) \\ 4(1, \underline{2}) = (1, \underline{0}) + (1, \underline{2}) \equiv (0, \underline{2}) \\ 5(1, \underline{2}) = (0, \underline{2}) + (1, \underline{2}) \equiv (1, \underline{1}) \\ 6(1, \underline{2}) = (1, \underline{1}) + (1, \underline{2}) \equiv (0, \underline{0}) \end{array}$$

Hence, $(1, \underline{2}) + \langle (2, \underline{3}) \rangle$ has order 6 in $(\mathbb{Z} \times \mathbb{Z}_6) / \langle (2, \underline{3}) \rangle$ (so this is a generator). \square

- c) Use the properties $\det(AB) = \det A \cdot \det B$ and $\det \text{Id}_n = 1$ for $n \times n$ matrices (where Id_n is the $n \times n$ identity matrix) to show that the $n \times n$ matrices with determinant 1 form a normal subgroup of $\text{GL}(n; \mathbb{R})$.

Answer: Let $\text{SL}(n; \mathbb{R}) = \{A \in \text{GL}(n; \mathbb{R}) \mid \det A = 1\}$.

$\text{SL}(n; \mathbb{R})$ is closed for multiplication since, if $\det A = \det B = 1$, then $\det(AB) = \det A \cdot \det B = 1$.

$\text{Id}_n \in \text{SL}(n; \mathbb{R})$ since $\det \text{Id}_n = 1$.

If $A \in \text{SL}(n; \mathbb{R})$, then $\det A = 1 \neq 0$, so A is invertible and its inverse A^{-1} is also in $\text{SL}(n; \mathbb{R})$ because $\det A^{-1} = \det A^{-1} \cdot \det A = \det(A^{-1}A) = \det \text{Id}_n = 1$.

Hence, $\text{SL}(n; \mathbb{R})$ is a subgroup of $\text{GL}(n; \mathbb{R})$.

If $A \in \text{SL}(n; \mathbb{R})$ and $B \in \text{GL}(n; \mathbb{R})$, then

$$\det(BAB^{-1}) = \det B \cdot \underbrace{\det A}_1 \cdot \det B^{-1} = \det(BB^{-1}) = \det \text{Id}_n = 1.$$

Therefore, $BAB^{-1} \in \text{SL}(n; \mathbb{R})$, showing that $\text{SL}(n; \mathbb{R})$ is normal. \square

- d) Let G and G' be finite groups, and let $\phi : G \rightarrow G'$ be a homomorphism. Show that the order of the image of ϕ divides both the order of G and the order of G' .

Answer: $\text{im } \phi$ is a subgroup of G' . Thus, by Lagrange's theorem, $|\text{im } \phi|$ divides $|G'|$.

By the fundamental homomorphism theorem, $\text{im } \phi \simeq G/\ker \phi$, which implies $|G| = |\text{im } \phi| \cdot |\ker \phi|$. Thus, $|\text{im } \phi|$ divides $|G|$. \square

2. RINGS AND FIELDS

- a) Show that the fields \mathbb{C} and \mathbb{R} are not isomorphic.

Answer: Suppose $\phi : \mathbb{C} \rightarrow \mathbb{R}$ were a ring isomorphism. Then $\phi(1) = 1$ (because $(\phi(1))^2 = \phi(1)$ implies $\phi(1) = 1$ or $\phi(1) = 0$, and the second solution is impossible for an isomorphism ϕ), and $\phi(-1) = -\phi(1) = -1$.

Consider $x = \phi(i)$. Then $x^2 = (\phi(i))^2 = \phi(i^2) = \phi(-1) = -1$, which has no real solution x . Therefore, there cannot exist an isomorphism between \mathbb{C} and \mathbb{R} . \square

- b) Show that the unity element in a subfield of a field must be the unity of the whole field.

Answer: Let F be a field with unity 1, and let F' be a subfield of F with unity $1'$. By the property of a unity, $1 \cdot 1' = 1' = 1' \cdot 1'$. Since the field F has no divisors of zero, $(1 - 1') \cdot 1' = 0$ implies that $1 = 1'$. \square

c) Describe all ring homomorphisms $\phi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$.

Answer: Let $x = \phi(1)$. Then $x^2 = x$, whose only solutions in $\mathbb{Z} \times \mathbb{Z}$ are $(0, 0)$, $(1, 1)$, $(1, 0)$, or $(0, 1)$. These four solutions indeed correspond to the possible homomorphisms given, at any $a \in \mathbb{Z}$, by

$$\begin{aligned} \phi_0(a) &= (0, 0) , & \phi_1(a) &= (a, a) , \\ \phi_2(a) &= (a, 0) , & \phi_3(a) &= (0, a) . \end{aligned}$$

□

d) Let R be a ring. Show that, if $a^2 = a$ for all $a \in R$, then R is commutative. (Hint: consider $(a + b)^2$.)

Answer: For any $a, b \in R$,

$$a + b = (a + b)^2 = \underbrace{a^2}_a + ab + ba + \underbrace{b^2}_b \iff ab = -ba .$$

Moreover, $a = a^2 = (-a)^2 = -a$, so we conclude that $ab = ba$.

□

3. POLYNOMIALS AND FACTOR RINGS

a) For each of the following descriptions, either find an object which satisfies it, or explain why such object cannot exist.

- A nonzero polynomial in $\mathbb{R}[x]$ which is irreducible over \mathbb{R} and has a zero in \mathbb{R} .

Answer: Impossible. If $f(x) \in \mathbb{R}[x]$ has a zero $a \in \mathbb{R}$, then, by the division algorithm, $f(x) = (x - a)q(x)$ for some $q(x) \in \mathbb{R}[x]$. □

- An ideal H in $\mathbb{R}[x]$ such that $H \neq \{0\}$, $H \neq \mathbb{R}[x]$ and H is not maximal.

Answer: For example, $H = \langle x^2 \rangle$. H is not maximal because $H \subset \langle x \rangle \subset \mathbb{R}[x]$, $H \neq \langle x \rangle$ (because $x \notin H$) and $H \neq \mathbb{R}[x]$. □

- A ring R and a ring homomorphism $\phi : \mathbb{Q} \rightarrow R$ such that the kernel of ϕ is the subring $\{5n \mid n \in \mathbb{Z}\}$.

Answer: Impossible. The kernel of a ring homomorphism has to be an ideal, but $\{5n \mid n \in \mathbb{Z}\}$ is not an ideal in \mathbb{Q} (for instance, $5 \cdot \frac{1}{2} \notin \{5n \mid n \in \mathbb{Z}\}$). □

- b) Find a factorization of $x^4 + 5x^2 + 6 \in \mathbb{Q}[x]$ into irreducible factors in $\mathbb{Q}[x]$.

Answer: $x^4 + 5x^2 + 6 = 0 \iff (x^2)^2 + 5x^2 + 6 = 0 \iff x^2 = -2$ or $x^2 = -3$, so that $x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$. The factors $x^2 + 2$ and $x^2 + 3$ are irreducible over \mathbb{R} since they are polynomials of degree 2 and have no real zeros. \square

- c) Give the precise condition for a subring to be an ideal.

Answer: A subring H of a ring R is an *ideal* if, for any $h \in H$ and any $a \in R$, we have that $ha \in H$ and $ah \in H$. \square

- d) Show that $x^2 + 1$ is irreducible in $\mathbb{Z}_7[x]$. Give an example of a field having 49 elements.

Answer: Let $f(x) = x^2 + 1 \in \mathbb{Z}_7[x]$. Then

$$\begin{aligned} f(\underline{0}) &= \underline{1}, & f(\underline{1}) &= f(-\underline{1}) = \underline{2}, \\ f(\underline{2}) &= f(-\underline{2}) = \underline{5}, & f(\underline{3}) &= f(-\underline{3}) = \underline{3}. \end{aligned}$$

Since $f(x)$ is of degree 2, and $f(x)$ has no zeros in \mathbb{Z}_7 , $f(x)$ must be irreducible in $\mathbb{Z}_7[x]$. $\mathbb{Z}_7[x]/\langle x^2 + 1 \rangle$ is a field with 49 elements, because it is a 2-dimensional vector space over \mathbb{Z}_7 . \square

4. EXTENSION FIELDS

- a) Find the irreducible polynomial for $\alpha = \sqrt{1 + \sqrt{1 + \sqrt{2}}}$ over \mathbb{Q} .

Answer: By squaring we obtain

$$\begin{aligned} \alpha^2 &= 1 + \sqrt{1 + \sqrt{2}} \\ \alpha^4 - 2\alpha^2 + 1 &= 1 + \sqrt{2} \\ \alpha^8 - 4\alpha^6 + 4\alpha^2 &= 2. \end{aligned}$$

The monic polynomial $x^8 - 4x^6 + 4x^2 - 2$ is irreducible over \mathbb{Q} since it satisfies the Eisenstein condition with $p = 2$. Hence, $\text{irr}(\alpha, \mathbb{Q}) = x^8 - 4x^6 + 4x^2 - 2$. \square

- b) Let F, E, K be fields such that E is a finite extension over F and K is a finite extension over E . Show that if $\{\alpha_1, \dots, \alpha_n\}$ is a basis for E as a vector space over F , and $\{\beta_1, \dots, \beta_m\}$ is a basis for K as a vector space over E , then $\{\alpha_i \beta_j \mid i = 1, \dots, n, j = 1, \dots, m\}$ is a basis for K as a vector space over F .

Answer:

– The $\{\alpha_i\beta_j\}$ span K over F :

Any $\gamma \in K$ is of the form $\gamma = \sum_j b_j \beta_j$ for some $b_j \in E$, since the $\{\beta_j\}$ span K over E . Any $b_j \in E$ is of the form $b_j = \sum_i a_{ij} \alpha_i$ for some $a_{ij} \in F$, since the $\{\alpha_i\}$ span E over F . Therefore,

$$\gamma = \sum_j \left(\sum_i a_{ij} \alpha_i \right) \beta_j = \sum_{i,j} a_{ij} (\alpha_i \beta_j)$$

– The $\{\alpha_i\beta_j\}$ are linearly independent over F :

Suppose $\sum_{i,j} a_{ij} (\alpha_i \beta_j) = 0$, i.e., $\sum_j \left(\sum_i a_{ij} \alpha_i \right) \beta_j = 0$. Since the $\{\beta_j\}$ are linearly independent over E , we must have $\sum_i a_{ij} \alpha_i = 0$, for all j . But since the $\{\alpha_i\}$ are linearly independent over f , we must have $a_{ij} = 0$, for all i, j . □

c) Give an intermediate field F between \mathbb{Q} and $\mathbb{Q}(\sqrt[4]{3})$, i.e., give a field F such that $F \neq \mathbb{Q}$, $F \neq \mathbb{Q}(\sqrt[4]{3})$ and $\mathbb{Q} \subset F \subset \mathbb{Q}(\sqrt[4]{3})$.

Answer: Let $F = \mathbb{Q}(\sqrt{3})$. We have $\mathbb{Q} \subset F$, but $\mathbb{Q} \neq F$ because $\sqrt{3} \notin \mathbb{Q}$. We also have $F \subset \mathbb{Q}(\sqrt[4]{3})$ because $\sqrt{3} = (\sqrt[4]{3})^2$, but $F \neq \mathbb{Q}(\sqrt[4]{3})$ because $\sqrt[4]{3} \notin F$. □

d) Give an explicit isomorphism from the field $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ to \mathbb{C} .

Answer: Define $\phi : \mathbb{R}[x]/\langle x^2 + 1 \rangle \rightarrow \mathbb{C}$ by

$$\phi(1 + \langle x^2 + 1 \rangle) = 1 \quad \text{and} \quad \phi(x + \langle x^2 + 1 \rangle) = i.$$

ϕ is a homomorphism (note that $(x + \langle x^2 + 1 \rangle)^2 = -1 + \langle x^2 + 1 \rangle$ agrees with $i^2 = -1$), injective and surjective. □