Abstract Algebra I - Exercises

1. Sets

1) Use three different expressions to express the set of multiples of 3
2) Show that the power set of $\mathbb{N}$ and $\mathbb{R}$ have the same cardinality.
3) Show that $\mathbb{R}$ and $\mathbb{C}$ have the same cardinality.

2. Equivalence relations

1) In $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, consider a relation $\mathcal{R}$ so that for $\bar{a}, \bar{b} \in \mathbb{Z}_5$,
$$\bar{a}\mathcal{R}\bar{b} \quad \text{if} \quad \overline{a^k - b} = \bar{0}$$
for some integer k.
   a) Write down $\mathcal{R}$ as a set.
   b) Determine if $\mathcal{R}$ is an equivalence relation.
2) Let $v_1 = (3,1)$ and $v_2 = (1,3)$. For $x, y \in \mathbb{R}^2$, define
$$x \sim y \text{ if } \quad x - y = k_1 v_1 + k_2 v_2 \quad \text{for some } k_1, k_2 \in \mathbb{Z}.$$
   a) Show that "$\sim$" defines an equivalence relation.
   b) Sketch all points in the equivalence class $\overline{(1,1)}$ on $\mathbb{R}^2$.
   c) Find a fundamental domain (which is a set of representatives of all equivalence classes).
3) Let S be the collection of all subspaces in $\mathbb{R}^3$. For two subspaces V and W in $\mathbb{R}^3$, define
$$V \sim W \quad \text{if there exists some linear isomorphism } T : \mathbb{R}^3 \to \mathbb{R}^3 \text{ such that } T(V) = W.$$
   a) Show that "$\sim$" defines an equivalence relation on S.
   b) Find the number of equivalence classes.
4) For $A, B \in M_n(\mathbb{R})$, define
$$A \sim B \quad \text{if there exists an invertible matrix } P \text{ such that } B = PAP^{-1}.$$
Show that "$\sim$" defines an equivalence relation on $M_n(\mathbb{R})$. In this case, an equivalence class is called an conjugacy class.

3. Roots of unity and $\mathbb{Z}_n$

1) Let ρ be an injective map from $\mathbb{Z}_4$ to $U_4 = \{1, -1, i, -i\}$ so that $\rho(a+b) = \rho(a)\rho(b)$ for all $a, b \in \mathbb{Z}_4$.
   a) Show that $\rho(\bar{0}) = 1$.
   b) Show that $\rho(\bar{2}) = -1$.
   c) Find all possibilities of ρ.
2) Let $>, m$ be two positive integer. Let $\rho : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $\rho(\bar{a}) = \bar{a}$. Show that ρ is well-defined if and only if $m|n$.
3) For $\bar{a}, \bar{b} \in \mathbb{Z}_n$, define
$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$
Show that the above binary operator is well-defined.
4) Let S be the set of conjugacy classes of $M_n(\mathbb{R})$. Show that the trace and the determinant function are well-defined on S.

4. Binary operations

1) a) Show that the $\mathbb{Z}_6\backslash\{\bar{0}\}$ under multiplication is not closed.

   b) Show that the multiplication on $\mathbb{Z}_n\backslash\{\bar{0}\}$ is a not binary operator if n is not a prime number.

2) Determine if the following binary operators are commutative and associated.

   a) Average on $\mathbb{R}$: $a * b := \frac{1}{2}(a+b)$.

   b) Matrix addition

   c) Subspace addition $V + W := \{\vec{v} + \vec{w} | \vec{v} \in V, \vec{w} \in W\}$.

   d) Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ with $f(a, b) = a^b$.

5. Isomorphic binary structures

1) Consider the following four binary operators on $S = \{a, b\}$.

$*_1$	a	b
a	a	b
b	b	a

$*_2$	a	b
a	a	b
b	b	b

$*_3$	a	b
a	b	b
b	a	a

$*_4$	a	b
a	a	a
b	a	a

   a) Which of them are commute?

   b) Find the identity of each binary operator, if the identity exists.

   c) Is any of them isomorphic to $(\mathbb{Z}_2, +)$? If so, write down the map.

   d) Is any of them isomorphic to $(\mathbb{Z}_2, *)$? If so, write down the map.

2) Let

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\} \quad \text{and} \quad S' = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R}, ad \neq 0 \right\}$$

   Then

   a) Show that matrix multiplication defines a binary operator on S.

   b) Consider $f : S \to S'$ given by $f(A) = A^T$. Verify whether f is an isomorphism or not. (You have to check three conditions of isomorphisms.)

   c) Construct an isomorphism from S to S'.

6. Structure properties

1) Prove that

   "There exists a non-identity element $x \in S$ such that $x * x$ is the identity."

   is a structural property of a binary structure.

2) Show that $(\mathbb{Z}, +)$ and $(\mathbb{Q}, \cdot)$ are not isomorphic.

3) Find a structure property to show that $(\mathbb{R}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

4) Find a structure property to show that $(M_2(\mathbb{R}), +)$ and $(M_2(\mathbb{R}), *)$ are not isomorphic.

5) Find a structure property to show that $(\mathbb{Z}^2, +)$ and $(\mathbb{Z}, +)$ are not isomorphic.

7. Groups

1) a) Show that $\mathbb{Z}_9^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ under multiplication is a group.
   b) Show that $(\mathbb{Z}_9^*, \cdot)$ is isomorphic to $(\mathbb{Z}_6, +)$.

2) Show that the cross product on $\mathbb{R}^3$ is a binary operator, but $(\mathbb{R}^3, \times)$ is not a group.

3) Show that the bijection from $\{1, \cdots, n\}$ forms a group under composition, denoted by S_n. How many elements does this group have?

4) List of all symmetries of an equilateral triangle. Suppose we have known these symmetries forms a group. Show that it is isomorphic to S_3.

8. Elementary properties of groups

1) Let G be a finite group. For all $g \in G$, show that there exists some positive integer n such that $g^n = e$.

2) If G is an infinite group, does 1) still hold?

9. Group of small cardinalities

1) Let $G = \{e, a_1, a_2, a_3, a_4\}$ be a group of order 5.
   a) Show that $(a_1)^2 \neq e$.
   b) Show that $(a_1)^3 \neq e$.
   c) Show that $(a_1)^4 \neq e$.
   d) Show that $G \cong \mathbb{Z}_5$.

2) Show that the additive groups $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, (\mathbb{Z}_2)^3$ are not isomorphic.

10. Multiplicative group $\mathbb{Z}_n^\times$

1) Let $(S, *)$ be an associative binary structure with identity e. Let S' be the subset of S consisting of all elements with inverse. Show that $*$ induces a binary operator on S' and S' is a group under the induced operator.

2) Find multiplicative inverses of elements in $\mathbb{Z}_{15}^\times = \{\bar{x} \in \mathbb{Z}_{15} : \gcd(x, 15) = 1\}$;

3) Find a structure property to show that $(\mathbb{Z}/12\mathbb{Z})^\times \ncong \mathbb{Z}/4\mathbb{Z}$ (You do not have to prove the property is structural.)

4) Find a group isomorphism from $(\mathbb{Z}/12\mathbb{Z})^\times$ to $(\mathbb{Z}/8\mathbb{Z})^\times$. (You have to verify the map you defined is indeed a group isomorphism.)

11. Subgroups

1) Let G be a group. Show that the center

$$Z_G = \{g \in G | xg = gx, \text{ for all x } \in G\}$$

is a subgroup of G.

2) Let x be an element in a group G, show that the centralizer

$$C_G(x) = \{g \in G | xg = gx\}$$

is a subgroup of G.

12. Subgroups

1) Let x be an element in a group G, show that the centralizer

$$C_G(x) = \{g \in G, xg = gx\}.$$

is a subgroup of G.

2) Draw the tree of subgroups of the additive group $\mathbb{Z}_6$.

3) Draw the tree of subgroups of $\mathbb{Z}_{40}$.

4) Given two subgroups H_1 and H_2 of a group G. Suppose $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$. Show that $H_1 \cup H_2$ is not a subgroup.
(Hint : Show that $H_1 \cup H_2$ is not closed under the group operation.)

13. Cyclic Subgroup

1) Find all cyclic subgroups of multiplicative group $(\mathbb{Z}_9)^\times$.

2) Show that every subgroup of $(\mathbb{Z}_9)^\times$ is cyclic.

3) Fix an element a of order n in a group G. Define an equivalent relation on G as follows

$$x \sim y \quad \text{if} \quad x = a^k y \quad \text{for some k } \in \mathbb{Z}.$$

   a) Show that every equivalence class has n elements.
   b) When G is a finite group, show that n divides $|G|$.
   c) Show that when $|G|$ is a prime p, $G \cong \mathbb{Z}_p$.

4) Let G be an abelian group. For $a, b \in G$, show that

$$\langle a, b\rangle = \{a^n b^m | n, m \in \mathbb{Z}\}.$$

14. Cyclic Group

1) Let $G = (\mathbb{Z}_{11}^\times, *)$.

   a) Show that G is a cyclic group (by finding a generator of G).
   b) Draw the subgroup diagram of G.

2) Let $G = (\mathbb{Z}_{15}^\times, *)$.

   a) Show that G is not cyclic group.
   b) Show that G can be generated by two elements.

15. Groups of Permutation

1) Suppose two sets A and B have the same cardinality. Show that the groups of permutations S_A and S_B are isomorphic.

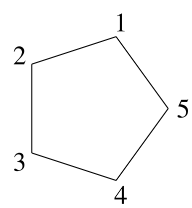
2) Examine a deck of cards and separate them into subsets that have the same kinds of symmetry.

16. Cycle Notation

1) Write $g = \binom{12345678}{43251876} \in S_8$ as in cycle notation.
2) Write $g = \binom{1234567}{4325176} \in S_7$ as in cycle notation.
3) Show that the order of any element in S_n divides $n!$.
4) Find the minimal number of n such that S_n contains an element of order 10.
5) 4 numbered players must find their own numbers in one of 4 drawers in order to win. The rules of the game is following: 1) Players can discuss their strategy before playing the game. 2) Each player may open only 2 drawers and only himself/herself can see the result. 3) Players cannot communicate with other players once the game has been started.
   a) Show that for each player, the probability of finding his/her own numbers using any strategy is 1/2.
   b) List all cycle structures of elements in S_4.
   c) Show that there exists a strategy for players that the probability of wining the game is at least 5/12.
6) Let $sigma$ be the perfect in-shuffle of $2n$ cards. Show that the order of σ equals the multiplicative order of 2 in $\mathbb{Z}_{2n-1}^{\times}$.

17. Symmetry group of n-gons

1) Let G be the symmetric group of a regular pentagon as shown in the below figure.

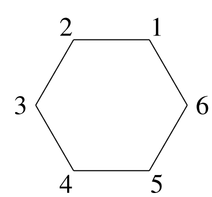


   Let σ be the counterclock-wise rotation of 72° and τ be the reflection in G which fixes vertex 1.

   a) Write down σ and τ using cycle notations.
   b) Show that $\sigma\tau = \tau\sigma^{-1}$.
   c) Show that G is not a cyclic group.
   d) Show that G contains exactly 10 elements.
   e) For a (linear) rotation σ' and a (linear) reflection τ' on $\mathbb{R}^2$, show that we always have

$$\sigma'\tau' = \tau'(\sigma')^{-1}.$$

2) Let $G = D_6$ be the group of symmetries of a regular hexagon as shown in the below figure.

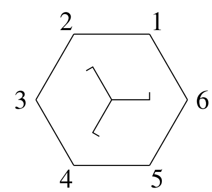


   a) Describe all elements of G in terms of symmetries.

b) Write all elements of G in cycle notations.

c) Show that G is not commutative.

d) Suppose the following figure is drawn in the hexagon.



Find the group of symmetries of the hexagon with the figure.

3) Let G be the group of rotational symmetries of a regular tetrahedron. Describes all elements in G.

4) Show that for $n \geq 3$, S_n can be generated by $(1 \cdots n)$ and (12).

18. Cayley Theorem

1) Let $G = S_3$, describe the group homomorphism from G to S_6 obtained in Cayley Theorem.

19. Transposition

1) Let G be a subgroup of S_n. Show that if G contains an odd permutation, then half of elements of G are odd and half of elements of G are even.

2) Identify D_6 as a subgroup of S_6. Let H be a subgroup of D_6 consisting of all even permutations. Find the group structure of H.

20. Cosets

1) Let $G = A_4$ be the alternating subgroup on 4 letters.

a) List all element of G.

b) Let $H = \langle (123) \rangle$. Find all left cosets of H.

2) Let $G = \langle \sigma, \tau | \sigma^6 = \tau^2 = e, \sigma\tau = \tau\sigma^{-1} \rangle$.

a) List all element of G.

b) Let $H = \langle \sigma^3 \rangle$. Find all left cosets of H.

3) Let $G = \mathbb{Z}^2$ and $H = \langle (2,0), (0,3) \rangle$. Find all left cosets of H.

4) Let G be a group with subgroups H and K. Suppose $K \subset H$ and two indexes $[G : H]$ and $[H : K]$ are all finite. Show that $[G : K] = [G : H][H : K]$.

22. Applications of Lagrange's Theorem

1) Suppose we have known that every group of order 6 is isomorphic $\mathbb{Z}_6$ or S_3. Find all subgroups of D_6.

2) Find all subgroups of A_4.

23. Direct Product

1) Show that S_4 and $\mathbb{Z}_4 \times S_3$ are not isomorphic.

2) Show that for any two positive n and m, S_{n+m} contains a subgroup isomorphic to $S_n \times S_m$.

24. Finitely Generated Abelian Groups

1) Find all possible structure of abelian groups of size 500.

2) Find the number of abelian groups of order 32 upto isomorphism.

3) Show that $\mathbb{Z}^n$ can not be generated by $n-1$ elements.

25. Structures of Finite Abelian Groups

1) Determine the group structure of $(\mathbb{Z}_{60})^\times$.

2) Determine the group structure of $(\mathbb{Z}_{32})^\times$.

3) Let G be an abelian group and p be a prime. Show that

$$G_p = \{a \in G | a^{p^k} = e, \text{for some } k \in \mathbb{N}\}$$

is a subgroup.

4) Let $G \cong \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_k}}$ where p is a prime. Show that

$$\log_p \left(\frac{|G^{(p^{i-1})}|}{|G^{(p^i)}|} \right) = |\{r_j | r_j \geq i\}|.$$

Use the above result to show that the structure of G can be determined by $|G^{(p)}|, |G^{(p^2)}|, \cdots$.

26. Homomorphism

1) Let ρ be a homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$.

   a) Show that the order of $\rho(a)$ divides the greatest common divisor of the order of a and m.
   b) Describe all homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_8$.
   c) Find the number of all possible homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$

2) Let Φ be a group homomorphism from S_3 to $\mathbb{Z}_n$.

   a) If $n = 2$, construct a nontrivial Φ.
   b) If $n = 3$, show that Φ is always trivial.
   (Recall Φ is trivial if Φ maps the whole S_3 to the identity.)

27. Kernels of Homomorphism

1) Consider the map $\Phi : \mathbb{Z} \to \mathbb{Z}_4 \times \mathbb{Z}_6$ given by $\Phi(x) = (x \mod 4, x \mod 6)$.

   a) Show that Φ is a group homomorphism.
   b) Find the kernel of Φ
   c) Is Φ surjective (onto)?

2) Let $G = D_6 = \langle \sigma, \tau | \sigma^6 = \tau^2 = e, \sigma\tau = \tau\sigma^{-1} \rangle$. Let $H_1 = \langle \sigma^2, \tau \rangle \cong D_3$. Find a group homomorphsim from G with kernel equal to H_1.

28. Normal Subgroups

1) Let H and N be two subgroups of G. Suppose N is a normal subgroup of G. Show that $N \cap H$ is a normal subgroup of H.
2) Let $H = \{e, (12)(34), (14)(23), (13)(24)\}$ be a subgroup of S_4. Show that H is a normal subgroup.
3) Let $G = \mathbb{Z} \times \mathbb{Z}$, $H = \langle (2,1), (1,2) \rangle$, and $N = \langle (3,0), (0,3) \rangle$.
   a) Show that $N \leq H$.
   b) Find $[G : H]$. (Hint: You may use that fact $[G : N] = [G : H][H : N]$.)
4) Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group where $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$. Let $H = \{\pm 1\}$, a subgroup of Q_8. Then
$$Q_8 = H \sqcup iH \sqcup jH \sqcup kH.$$
   Label the above cosets by 1,2,3, and 4 respectively and consider the map $\rho : Q_8 \to S_{Q_8/H} \cong S_4$ given by $\rho(g)(xH) = gxH$.
   a) Show that H is normal.
   b) Find the kernel of ϕ.
   c) Find $\phi(Q_8)$ as a subgroup of S_4.
   d) Determine the group structure of $\phi(Q_8)$.
   e) Show that Q_8 is not isomorphic to any subgroup of S_4.

29. Quotient Group Computation

1) Let
$$G = \left\{ \begin{pmatrix} a & b \\ \bar{0} & c \end{pmatrix}, a, c \in \mathbb{Z}_4^\times, b \in \mathbb{Z}_4 \right\}$$
   be a multiplicative group and $H = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{3} & \bar{0} \\ \bar{0} & \bar{3} \end{pmatrix} \right\}$ be its subgroup.
   a) List all left cosets of H in G.
   b) Show that H is a normal subgroup.
   c) Determine if G/H is abelian or not.
   d) Determine the structure G/H.
   e) Construct a group isomorphism from G/H to $\left\{ \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix}, a \in \mathbb{Z}_4^\times, b \in \mathbb{Z}_4 \right\}$
2) a) Consider a map $\rho : \mathbb{Z}^3 \to \mathbb{Z}^2$ given by $\rho(x, y, z) = (y - 2x, z - 3x)$. Using this map to show that $\mathbb{Z}^3/\langle (1,2,3) \rangle \cong \mathbb{Z}^2$.
   b) Show that if $\gcd(a, b, c) = 1$, then $\mathbb{Z}^3/\langle (a, b, c) \rangle \cong \mathbb{Z}^2$. (You may first try the case $(a, b, c) = (6, 10, 15)$)
3) Let $G = \mathbb{Z}^2$ and $H = \langle (2,1), (-1,2) \rangle$.
   a) Find the group structure of G/H.
   b) Find a surjective group homomorphism from G with kernel equal to H.
4) (Extra homework) Let H be a subgroup of $\mathbb{Z}^n$. Show that H is generated by at most n elements.
   (Hint: Consider $p : \mathbb{Z}^n \to \mathbb{Z}^{n-1}$ given by $p((a_1, a_2, \cdots, a_n)) = (a_1, a_2, \cdots, a_{n-1})$. Find a subgroup H' in H such that the restriction of p on H' is an isomorphism from H' to $p(H)$. Show that $H \cong H' \oplus (\ker(p) \cap H)$.

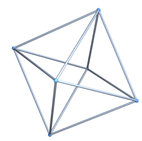
30. Normal Subgroups

31. Classification of Finite Groups

32. Cayley Graphs

1) Let $G = D_6 = \langle \sigma, \tau | \sigma^6 = \tau^2 = e, \sigma\tau = \tau\sigma^{-1} \rangle$ and $S = \{\sigma, \sigma^{-1}, \tau\}$. Draw the Cayley graph associated to (G, S).

2) Find a pair (G, S) such that the Cayley graph associated to (G, S) is the following graph.



33. Rings and Fields

1) Show that $R = \{a + bi | a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

2) Let $R = M_2(\mathbb{Z}_2)$ be the ring consisting of all 2 by 2 matrices with entries in $\mathbb{Z}_2$

   a) Find the number of units in R (which are elements with determinant not equal to zero).

   b) Find the structure of the group of units $R^\times$ (under matrix multiplication).

3) Let

$$R = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_p \right\}$$

   a) Show that R is a subring of $M_2(\mathbb{Z}_p)$.

   b) Show that R is commutative.

   c) Show that if $p = 2$, R is a not field.

   d) Show that if $p = 3$, R is a field.

   e) Show that R is a field if and only if $x^2 \equiv -1 \mod p$ has no solution.

4) Let R be a ring with unity. Show that

$$\langle 1_R \rangle = \{m 1_R | m \in \mathbb{Z}\}$$

   forms a subring of R. Moreover, $\langle 1_R \rangle \cong \mathbb{Z}$ or $\mathbb{Z}_n$ for some n as a ring.

1) Let $R = \mathbb{Q}[\sqrt{3}] = \{f(\sqrt{3}) | f(x) \in \mathbb{Q}[x]\}$.

   a) Construct an injective ring homomorphism from R to $M_2(\mathbb{Q})$.

   b) Show that R is a field.

   c) For a nonzero element $a + b\sqrt{3}$, find its multiplicative inverse.

2) In $\mathbb{Q}[x]$, define an equivalence relation $\sim$ by

$$f(x) \sim g(x) \quad \text{if} \quad (x^2 - 3) \Big| \big(f(x) - g(x)\big).$$

   Let R be the set of equivalence classes which forms a ring under the following operations.

$$\overline{f(x)} + \overline{g(x)} := \overline{f(x) + g(x)} \quad \text{and} \quad \overline{f(x)} \cdot \overline{g(x)} := \overline{f(x) \cdot g(x)}.$$

   a) Show that every equivalence class can be represented by a unique element of the form $ax + b$.

   b) Show that R and $\mathbb{Q}[\sqrt{3}]$ are isomorphic.

3) Let $\phi : R \to R'$ be a ring homomorphism. Let $I = \ker(\phi)$. Show that $(a + I)(b + I) := (ab) + I$ defines a multiplication on R/I.

34. Integer Domains

1) Show that every subring with unity of an integral domain is also an integral domain.

2) Let R be an integral domain. Show that $R[x]$ is also an integral domain.

35. Fields and Integer Domains

36. Quotient Fields

1) Let D be an integral domain and $S = \{(a,b)|a,b \in D, b \neq 0\}$. Define an relation on S given by $(a,b) \sim (c,d)$ if $ad = bc$. Show that $\sim$ is an equivalence relation.

37. Polynomial Rings

1) Let R be a ring with unity. What are the units of $\mathbb{R}[x]$?

2) For a ring R, show that $\mathbb{R}$ has no-zero divisors if and only if for all non-zero $f(x), g(x) \in R[x]$, $\deg f(x) + \deg g(x) = \deg(f(x)g(x))$.

38. Division Algorithm of Polynomials

1) Let $f(x) = x^3 + x + 1$ and $g(x) = x^2 + 2x + 3$ are elements in $\mathbb{Z}_5[x]$. Find $q(x)$ and $r(x)$ in $\mathbb{Z}_5[x]$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg r(x) < \deg g(x)$.

2) Let $f(x) = x^4 + 1$ and $g(x) = 2x^2 + 3$ are elements in $\mathbb{Z}_7[x]$. Find $q(x)$ and $r(x)$ in $\mathbb{Z}_7[x]$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg r(x) < \deg g(x)$.

39. Zeros of Polynomials

1) Find the zeros of $x^p - x$ in $\mathbb{Z}_p$ where p is a prime.

2) Use the previous problem to show that $(p-1)! \equiv -1 \mod p$.

3) Show that there exists a polynomial in $\mathbb{Z}_p$ does not have any zeros.

4) Find all zeros of $x^{6664} + x^{362} + x^{21} + 3x + 1$ in $\mathbb{Z}_7$.

5) Let F be a field. For $a \in F$ and $f(x) \in F[x]$, define the multiplicity of a as the zero of $f(x)$ to be

$$m_{a,f} := \max\left\{ n \in \mathbb{Z}_{\geq 0} \middle| (x-a)^n | f(x) \right\}.$$

(Note that when a is not a zero of $f(x)$, we set $m_{a,f} = 0$.) Prove that when $f(x)$ is nonzero,

$$\deg f(x) \geq \sum_{a \in F} m_{a,f}.$$

40. Irreducible Polynomials

1) For $f(x) = x^4 + 1 \in F[x]$, factor $f(x)$ as a product of irreducible polynomials for the following cases

   a) $F = \mathbb{Q}$
   b) $F = \mathbb{Z}_2$.
   c) $F = \mathbb{Z}_3$.

d) $F = \mathbb{Z}_5$.

2) Show that $x^4 - x^2 + 1$ is irreducible over $\mathbb{Q}$.

3) Factor $x^4 - x^2 + 1$ as a product of irreducible polynomials over $\mathbb{Z}_3$.

41. Gauss's Lemma

42. Polynomial Factorization Modulo a Prime

1) Show that $x^3 + 202x + 2020$ is irreducible in $\mathbb{Q}[x]$.

2) Write down a monic irreducible polynomial of degree 2020 over $\mathbb{Q}$ which is not irreducible over $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

3) Does there exist an irreducible polynomial over $\mathbb{Q}$ so that it is irreducible over $\mathbb{Z}_p$ for all p? (Write down a reason to support your answer.)

4) Let $f(x) = x^4 - x + 1$ and $g(x) = x^3 + 1$.

   a) Factor $f(x)$ into a product of irreducible polynomials over $\mathbb{Z}_3[x]$.
   b) Factor $g(x)$ into a product of irreducible polynomials over $\mathbb{Z}_3[x]$.
   c) Find a GCD of $f(x)$ and $g(x)$ over $\mathbb{Z}_3[x]$.

43. Unique Factorization Theorem of $\mathbb{F}$[x]

1) Let $f(x), g(x)$ be two non-constant polynomials in $\mathrm{F}[x]$. Show the gcd of $f(x)$ and $g(x)$ is unique upto units.

2) Show that $h(x) = x^2 - x$ has two different factorizations over $\mathbb{Z}_{15}[x]$ (as a product of two linear factors)

3) For an odd prime p, show that there exists some $a \in \mathbb{Z}_p$, such that $x^2 - a$ is irreducible.

4) Find the number of irreducible polynomials of degree two over $\mathbb{Z}_p$.
   (Hint: Using unique factorization theorem to count the number of reducible polynomials.)

44. Fields Extensions

1) Let E be a field and K_1 and K_2 be two subfields of E. Show that $F := K_1 \cap K_2$ is also as a subfield of E.

2) Let $f(x)$ be an irreducible polynomial over $F[x]$ and α is a zero of $f(x)$ in a larger field E. Let $g(x)$ be another polynomial in $F[x]$ with $g(\alpha) = 0$. Show that $f(x)|g(x)$.

3) Let $F_1 \subset F_2 \subset F_3$ be three fields. Suppose $\alpha \in F_3$ is algebraic over F_1. Show that $\mathrm{Irr}(\alpha, F_2)|\mathrm{Irr}(\alpha, F_1)$.

4) Suppose we have known that e is a transcendental number. Show that $\mathrm{Irr}(\sqrt{e}, \mathbb{Q}(e))(x) = x^2 - e$.

45. Elements of Extension Fields

1) Let α be a zero of $x^2 + 1$ over $\mathbb{Z}_3[x]$ in some field extension of $\mathbb{Z}_3$.

   a) Find the multiplicative inverse of $\alpha + 1$ of the form of $a_0 + a_1\alpha$.
   b) Find an element of the form $a_0 + a_1\alpha$ which is a generator of $\mathbb{Z}_3[\alpha]^\times$

2) Let α be a zero of $x^3 + 1$ over $\mathbb{Q}[x]$ in $\mathbb{C}$.

   a) Find the multiplicative inverse of $\alpha + 1$ of the form of $a_0 + a_1\alpha + a_2\alpha^2$.
   b) Is $\mathbb{Q}[\alpha]^\times$ a cyclic group?

46. Algebraic Extension

1) Let $f(x)$ be a polynomial of degree n over $\mathbb{Q}$ with zeros $\alpha_1, \cdots, \alpha_n$ in $\mathbb{C}$.
   a) Show that $[\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}] \leq n!$.
   b) Show that $[\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}] \big| n!$.

47. Example of Algebraic Extensions

1) Let α be a zero of $x^2 + x + 1$ and β be a zero of $x^3 - x - 2$. Find the degree $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$.

2) Let α be a zero of $x^2 + x + 1$ and β be a zero of $x^2 - x - 1$. Find the degree $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$.

3) In 2), show that $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$.

4) Find the irreducible polynomial of $\gamma = \sqrt{2} + 2\sqrt{3} - 3\sqrt{6}$ over $\mathbb{Q}(\sqrt{2})$.

5) Let α be a zero of $x^4 + 1$ in $\mathbb{C}$ and let $\gamma = \alpha + \alpha^2$.

   (1) Show that $\mathrm{Irr}(\alpha, \mathbb{Q})$ is equal to $x^4 + 1$ and find a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.
   (2) Write $1/(\alpha + 1)$ as a linear combination of the basis in (1).
   (3) Find $\mathrm{Irr}(\gamma, \mathbb{Q})$.
   (4) Find $\mathrm{Irr}(\gamma, \mathbb{Q}(\alpha^2))$.
   (5) Find all possible quadratic sub-extensions of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

6) Let F be a subfield of $\mathbb{C}$. For $a, b \in \mathbb{C}$, if $\sqrt{a}$, $\sqrt{b}$, $\sqrt{ab}$ are all not contained in F, show that $[F(\sqrt{a}, \sqrt{b}) : F] = 4$.

7) Use the result in the previous problem to show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ is equal to 8.

8) (**) Let $p_1, \cdots, p_k$ be distinct primes. Show that the degree of $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_k})$ over $\mathbb{Q}$ is 2^k.

48. Algebraic Closure

1) Suppose E/F and K/E are both algebraic extensions. Show that K/F is also an algebraic extension.

2) Show that every finite field can not be algebraic closed.

49. Matrix representations of field extensions

1) Let α be a zero of the irreducible polynomial $x^3 + 2x + 2$ over $\mathbb{Z}_3[x]$ in $\bar{\mathbb{Z}}_3$. Let $F = \mathbb{Z}_3(\alpha)$.

   a) Find an injective ring homomorphism ρ from F to $M_3(\mathbb{Z}_3)$.
   b) Find the inverse map of ρ, which is a map from $\rho(F)$ to F.
   c) Using ρ and its inverse to rewrite $1/(1 + \alpha + \alpha^2)$ into the form $a_0 + a_1\alpha + a_2\alpha^2$.

50. Finite fields

1) Construct a field of 8 elements.

2) Let α be a zero of $x^2 + 2$ and β be zero of $x^2 + x + 2$ in $\overline{\mathbb{Z}}_5$.

   a) Show that $x^2 + x + 2$ has a zero in $\mathbb{Z}_5(\alpha)$.
   b) Construct a field isomorphism from $\mathbb{Z}_5(\alpha)$ to $\mathbb{Z}_5(\beta)$.

c) Find all zeros of all monic irreducible polynomials of degree two over $\mathbb{Z}_5$ in terms of α.

3) Show that if α is a zero of $f(x) \in \mathbb{Z}_p[x]$ in $\overline{\mathbb{Z}}_p$, then α^p is also a zero of $f(x)$.

4) For $\alpha \in \mathbb{F}_{p^6}$, show that $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^6}$ if $\alpha^{p^2-1} \neq 1$ and $\alpha^{p^3-1} \neq 1$.

5) Find the number of monic irreducible polynomials of degree 6 over $\mathbb{Z}_p$.

6) For $\alpha \in \mathbb{F}_{p^6}$, show that $\alpha \in \mathbb{Z}_p$ if and only if $\alpha^p = \alpha$.

7) Consider the map $\rho : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $\rho(x) = x^p$. Show that ρ is an ring isomorphism.

8) Let α be a zero of $x^2 + x + 1$ in $\overline{\mathbb{Z}}_2$.

   a) Show that $x^2 + \alpha$ is irreducible over $\mathbb{Z}_2(\alpha)$.

   b) Let β be zero of $x^2 + x + \alpha$ in $\overline{\mathbb{Z}}_2$. Find the irreducible polynomial of β over $\mathbb{Z}_2$

51. Structure of Finite Fields

52. Cyclomotic Polynomials over Finite Fields

1) Find the number of monic irreducible polynomials of degree four over $\mathbb{Z}_3$.

2) Find the product of monic irreducible polynomials of degree four over $\mathbb{Z}_3$.

3) Show that $\Phi_{11}(x)$ is irreducible over $\mathbb{Z}_2$.

4) Show that $\Phi_7(x)$ is irreducible over $\mathbb{Z}_3$.

5) Find an irreducible polynomial of degree 6 over $\mathbb{Z}_5$.

6) Find an irreducible polynomial of degree 12 over $\mathbb{Z}_2$.

   Remark. In general, $\Phi_n(x)$ is irreducible over $\mathbb{Z}_p$ if and only if p is a generator $\mathbb{Z}_n^\times$. The proof will be given in the next semester.