MA561
Sathaye **Old Problem Sets**

All rings will be commutative with 1 unless otherwise declared.

1 Group Theory

1. Define the center of a group and show that it is always a normal subgroup. Find the center of the quaternion group

$$Q = \{\pm 1, \pm i, \pm j, \pm k | ij = k = -ji, jk = i = -kj, ki = j = -ik\}$$

Find the center and show that $Q/C(Q)$ is abelian. (What is the name for such groups?).

2. Let H and K be normal subgroups of a group G, with $H \leq K$. Show that there is a natural homomorphism from G/H onto G/K. (Make sure that your function is well-defined.) What is the kernel of this homomorphism? Use the first isomorphism theorem to deduce a theorem that looks like a cancellation theorem.

3. Define a **simple group**. Is there a simple group of order 96? Justify your answer.

4. Let M be a finitely generated abelian group, written additively. Let T denote the torsion subgroup of M:

$$T = \{x \in M \mid nx = 0 \text{ for some } n \in Z, n \neq 0\}.$$

(a) Prove that M/T is torsion-free. That is, its torsion subgroup is trivial.

(b) It is a fact that if $T = \{0\}$, then M is a free Z-module. Prove this in the special case that M can be generated by 2 elements.

2 Rings

1. Prove that if M is a maximal ideal in a ring R, then M is prime and all powers M^n of M are primary.

2. If K is a field and $K[X_1, X_2, \cdots, X_n]$ is the polynomial ring in n variables over K (where n is at least 2), then prove that any principal ideal is prime iff it is generated by an irreducible polynomial.

Also prove that such an ideal is **never** maximal.

Deduce that any maximal ideal needs at least two generators. Give examples of maximal ideals for various values of n.

Try to prove that every maximal ideal can be generated by n elements.

3. Let K be a field and $K[X, Y]$ the polynomial ring in two variables over K. Take an ideal generated by two or three polynomials of degree at least two in $K[X, Y]$. Determine its primary decomposition, identifying all the primary and prime components. *Be sure to pick an ideal with at least two components.*

   Do a similar exercise in $\mathbf{Z}[X]$.

   Make sure that at least one of your examples has an embedded prime.

4. Prove that if R is a noetherian ring, then any localization of R and any homomorphic image of R are noetherian.

   Using suitable theorem(s) deduce that $R = \mathbf{Z}[\sqrt{(-5)}]$ is noetherian. Calculate the primary decompositions of various principal ideals generated by prime integers, say, 5 and 3. Deduce that there are prime ideals in R which are not principal.

5. Prove that every prime element in an integral domain is irreducible. Generally, when is primeness of an element equivalent to irreducibility? give an example of an integral domain and a nonprime irreducible element in it.

6. Given a ring homomorphism $f : R \longrightarrow S$, prove that there is a one-to-one correspondence between the ideals of S and ideals of R containing $\mathrm{Ker}(f)$. (Show that the image of a prime ideal containing the kernel is again a prime ideal. Show that the condition about the kernel is essential!)

7. Prove that every UFD is integrally closed (also termed normal).

8. Prove that $R = \mathbb{Z}[\sqrt{17}] = \mathbb{Z}[X]/(X^2 - 17)$. (What happens if 17 is replaced by another integer? What happens if square root is replaced by other roots? Is the ring R integrally closed? If not, what is the integral closure of $\mathbb{Z}$ in the quotient field of R? When is R an integral domain? Is it ever a field?)

9. Prove that in a commutative ring R with 1, the following are equivalent:

   (a) Every ideal is finitely generated.

   (b) Every strictly increasing sequence of ideals is finite.

   (c) Every set of ideals contains a maximal element.

   What are such rings called (noetherian, of course!)? Give an example of a nonnoetherian ring. (What ring operations preserve the noetherian property? Consider subring, residue class ring, localization, integral closure, polynomial ring extensions, power series ring extensions etc.)

10. Let P, Q, and A be ideals in the commutative ring R. Show that if A is contained in the union of P and Q then A is contained in one of P and Q. Give an example of a commutative ring and four ideals such

that one of them is contained in the union of the other three but is contained in no one of them.

11. Prove that a *finite* commutative ring with identity having 100 elements must have two non-zero elements a, b such that $ab = 0$.

12. Are $Z[\sqrt{-2}]$ and $Z[\sqrt{-5}]$ isomorphic rings? Why?

13. Let $f : K[X, Y] \to K[T]$be a homomorphism defined by $f(X) = T^3$ and $f(y) = T^4$. Determine the $Ker(f)$.

14. Define an **idempotent** element of a ring R to be an element satisfying $e^2 = e$.

    a If $e \in R$ is an idempotent, show that $1 - e$ is also an idempotent.

    b If R contains an idempotent e different from $0, 1$ then R is a direct sum of two subrings Re and $R(1 - e)$.

15. Define a PID. Prove that $Z[X]$ is not a PID.

16. Let F be a field. Prove that the polynomial rings $F[X]$ and $F[X, Y]$ cannot be isomorphic.

17. Let R be a commutative ring with identity. Let P be an ideal in R and let $S = R/P$, the residue class ring. Prove that S is a field if and only if P is a maximal ideal.

    Give an example to show that the above is false when the ring R does not contain an identity.

18. Let p be a prime number and let $F = Z_p$ be the field with p elements. Let
    $$I = \{f(X) \in F[X] | f(a) = 0 \ \ \forall a \in F\}.$$
    (For example, $X^p - X \in I$).

    - Prove that I is an ideal.
    - Is I principal? If so, find a generator for I .

19. Let K be a field and $S = K[X, Y]$ the polynomial ring in two variables over K.

    Let

    $I = \{f(X, Y) \in S \mid f(1, 2) = 0\}\text{and}J = \{u(X-1)+v(Y-2) \mid u, v \in S\}$

    (a) Prove that $I = J$.

    (b) Prove that J is a maximal ideal of S.

20. How many units are there in the ring $Z/(999)Z$ the ring of integers modulo 999? Explain your calculation!

21. Let Z be the ring of integers and let S be the subring of real numbers defined by

$$S = \{a + b\sqrt{5} \mid a, b \in Z\}$$

(a) Prove that $S \cong Z[X]/(X^2 - 5)Z[X]$.

(b) Prove that S is noetherian.

(c) Prove that $S/(2)S \cong T[X]/((X-1)^2)T[X]$ where $T = Z/(2)Z$ the ring of integers modulo 2. Using this or otherwise determine all the prime ideals of S containing 2.

22. Let Z denote the ring of integers and $f(x) = X^2 - 2 \in Z[X]$. Show that $Z[X]/(f(X))$ is an integral domain but not a field.

23. Given that a *noetherian* ring is one in which every ideal is finitely generated, prove that every strictly increasing sequence of ideals in a noetherian ring must be finite.

24. Let k be a field and $\{X, Y, t\}$ indeterminates over k. Let ϕ denote the homomorphism from $k[X, Y]$ to $k[t]$ defined by

$$X \to t^2$$

$$Y \to t^5.$$

Calculate the kernel of ϕ.

25. If K is any field, prove that the polynomial rings $K[X, Y]$ and $K[Z]$ cannot be isomorphic.

26. Let

$$J = \{f(X, Y) \mid f(0,0) = f(1,1) = 0\} \in K[X, Y].$$

Prove that J is an ideal in the polynomial ring $K[X, Y]$ over a field K. Find a set of generators for J. Define a *maximal ideal* and a *prime ideal* and determine, with justification, if J has either of the two properties.

27. Let R be a ring and let $a \in R$ be a nilpotent element. Prove that the element $1 + a^2$ is an invertible element of R.

28. Prove that $Z/(8Z)$ is a principal ideal ring.

29. Let Z denote the integers and $Z[X]$ the polynomial ring in one indeterminate over Z. Let h be an *automorphism* of $Z[X]$. Then h is determined by its action on X:

$$h(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

Solve the following. *You may use the result of any part to do another, even if you have not solved the part you use.*

(a) Prove that $a_j = 0$ for $j = 2, ..., n$.

(b) Prove $a_1 = \pm 1$

(c) Prove (e.g. by exhibiting inverses) that σ and τ are automorphisms where $\sigma(X) = X + 1$ and $\tau(X) = -X$.

(d) Show that $\tau\sigma\tau^{-1} = \sigma^{-1}$

(e) Prove that $h = \sigma^b$ or $h = \tau\sigma^b$ for some integer b.

(f) Prove that the representation of h in part (e) is unique.

(g) Determine the orders of σ^b and $\tau\sigma^b$.

30. If R is a commutative ring with identity and A, and B are ideals in R, let ψ_A be the natural homomorphism from R to R/A and ψ_B the natural homomorphism from R to R/B. Let $\psi : R \to R/A \oplus R/B$ be defined by $\psi(r) = (\psi_A(r), \psi_B(r))$.

    (a) Prove that the kernel of ψ is $A \cap B$.

    (b) Prove that if ψ is surjective then there are $a \in A$ and $b \in B$ such that $1 = a + b$.

    Hint: Consider e_A and e_B such that $\psi(e_A) = (1, 0)$ and $\psi(e_B) = (0, 1)$

31. Let $f : R \longrightarrow S$ be a ring epimorphism. Prove that there is a one-to-one correspondence between the ideals in R that contain $Ker(f)$ and those of S.

32. Let F be a field and let R be the ring $F \bigoplus F \bigoplus \cdots \bigoplus F$, n times, where both addition and multiplication are componentwise.

    (a) Describe all the ideals of R.

    (b) Describe all the prime ideals of R.

    (c) Describe all the maximal ideals of R.

33. Let R be a principal ideal domain. Prove that every non-zero prime ideal in R is a maximal ideal.

34. Let D be an integral domain (a commutative ring with identity in which there are no non-trivial divisors of zero) and K its quotient field. Clearly K is a *module* over D. If θ is a D-module homomorphism of D into K, show that there is $\alpha \in K$ such that $\theta(d) = \alpha d$ for every $d \in D$.

35. Let Z_2 be the field with 2 elements. For the following rings determine which are fields, and which, if any, are isomorphic to each other. (In case two rings are isomorphic, you are required to exhibit an explicit isomorphism between the two.)

$$Z_2[X]/(X^3 + X^2 + X + 1)$$

$$Z_2[X]/(X^3 + X^2 + 1)$$

$$Z_2[X]/(X^3 + X + 1)$$

36. Let $f : K[X,Y] \to K[T]$be a homomorphism defined by $f(X) = T^3$ and $f(y) = T^4$. Determine the $Ker(f)$.

37. Let F be a field and X an indeterminate. Let $S = F[X]$, the ring of polynomials in X over F. Let

$$R = \{f(X) \in S | f'(0) = 0\}.$$

(a) Show that R is an integral domain.

(b) Show that R is not factorial (i.e. UFD).

(c) Find an ideal of R that is not *principal.*

(d) Explain why every ideal in S is, however, principal.

38. **Define** a module, a simple module, a free module and a projective module.

Give example with proof of a module that is not free.

Give example with proof of a module M with a submodule N such that $M \neq N \oplus N'$ for any module N'.

39. Let F be a field. Prove that the polynomial rings $F[X]$ and $F[X,Y]$ cannot be isomorphic.

40. Define an artinian ring and give an example (with justification) of one. Is the ring of integers artinian and why?

41. Prove that $Z/(8Z)$ is a principal ideal ring.

42. Let R be a ring with 1.

(a) Define a **free** (left) R-module.

(b) Prove that every R-module is a homomorphic image of a free R-module.

(c) Let M be an R-module and let F be a free R-module. Prove that if there is an epimorphism $\phi : M \longrightarrow F$, then there are submodules N and F' of M such that $M \cong N \oplus F'$ and $F' \cong F$.

3 Vector Spaces

1. Let $T : V \to V$ be a linear transformation of a vector space V. Assume V has dimension 3 and basis v_1, v_2, v_3. Suppose that T is defined by

$$T(v_1) = 2v_2, T(v_2) = 2v_3, T(v_3) = v_1$$

Find the minimal polynomial of T.

2. If $A \subset B$ are *vector spaces* then B is isomorphic to $A \oplus C$ for some C. Is the same true for modules? In particular, since modules over the integers are just abelian groups, is it true that if $H \subset G$ are abelian groups, then there is an abelian group K such that $G \simeq H \oplus K$?

3. Let V be an $n-$dimensional vector space over a field F. Let W be a nonzero subspace of V.

   (a) Show that there is a linear transformation $f\ :\ V \to W$ which is identity on W.

   (b) Show that
   $$V = \text{ Ker } f \oplus W.$$

   (c) Show that Hom (V, W), the set of $F-$linear transformations from V to W, is a vector space and compute its dimension.

4. Let V be a $3-$dimensional vector space over the field C of complex numbers with basis v_1, v_2, v_3. Let $T : V \longrightarrow V$ be a linear transformation defined by
   $$Tv_1 = 2v_2\ ,\ T_2 = 4v_3\ ,\ Tv_3 = v_1$$

   - Calculate the minimum polynomial of T.
   - Calculate *all* eigenvalues of T.
   - Calculate an eigenvector for a real eigenvalue of T.

5. Let **V** be an n-dimensional vector space over the field F and let f be a linear transformation of V into V. Prove:

   (a) If f is surjective, then f is injective.

   (b) If $f \circ f = f$ then $V = ker(f) \oplus im(f)$.

   What, if anything, would change if V were assumed only to be a free module of rank n over the integers?

6. Let $\mathbf{Q}$ denote the rationals and $\mathbf{K}$ an algebraic extension of $\mathbf{Q}$. Let $\alpha \in \mathbf{K}$ and T_α the mapping of $\mathbf{Q}(\alpha)$ into itself defined by
   $$T_\alpha(x)\ =\ \alpha x.$$

   (a) Show that T_α is a linear transformation of the $\mathbf{Q}$-vector space $\mathbf{Q}(\alpha)$ into itself.

   (b) Show that the characteristic polynomial of T_α is the monic irreducible polynomial of α over $\mathbf{Q}$.

7. Let $T\ :\ V \mapsto V$ be a linear transformation defined by $T(v_1) = 2v_2, T(v_2) = 3v_3$ and $T(v_3) = v_1$, where v_1, v_2, v_3 form a basis of the vector space V. Determine the minimum polynomial of T.

8. Let V_n be the vector space of polynomials of degree $\leq n$ over the complex numbers. Then the derivative, D, is a linear transformation from V_n into itself. Calculate its characteristic polynomial.

9. Let V and W be finite-dimensional subspaces of a vector space over a field F. Prove that dim(V) + dim(W) = dim(V+W) + dim(V$\cap$W).

4 Fields and Galois Theory

1. Suppose that D is an integral domain with the property that **any strictly decreasing sequence of ideals** $I_1 > I_2 > \cdots$ is **necessarily finite**.

   Prove that D must be a field.

2. Is $\cos(\pi/60)$ constructible? What is the Galois group over $\mathbb{Q}$ of the field obtained by adjoining it? What about $\cos(\pi/180)$?

3. Prove or provide a counterexample (with justification).

   (a) Every field has a nontrivial algebraic extension.

   (b) Every extension of a field is finite.

   (c) The field $k(t)$ has only finitely many k-automorphisms. (What is the meaning of the symbol $k(t)$ anyway?)

   (d) Every finite extension is normal.

4. Given fields K, L, there exists at least one monomorphism $K \longrightarrow L$.

5. Define splitting field and Galois group. (Recall other related terms from field theory too!) Compute the Galois group of the polynomial $f(x) = (x^3 - 8)(x^2 + 5)$ over $\mathbb{Q}$.

6. Show that a finite extension of a field is always algebraic. Show by an example that the extension is not necessarily separable.

7. Define a separable polynomial and prove that $x^4 - 2x^2 - 35$ is separable over $\mathbb{Q}$. (Show that any irreducible polynomial is separable over a field of characteristic zero. How should we define separability of a reducible polynomial? For polynomials over fields with characteristic p, define and illustrate the separable and the inseparable degree.)

8. Use Newton's identities to find $\sum \alpha_i^2$ where the α_i are roots of $x^4 - 2x^2 - 35 = 0$ in some fixed splitting field. (Where do you need to ask what the field is? What can go wrong in fields of positive characteristic?)

9. Find the Galois group of $x^3 - x + 2$ over $\mathbb{Q}$. (How does the answer change if you change the ground field?)

10. Prove that any finite integral domain is a field. What happens if we drop the finiteness condition?(Prove that the multiplicative group of a finite integral domain is cyclic. What about the additive group?)

11. Let $f(x)$ be the polynomial $(x^3 - 3)(x^2 - 7)$ and let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Is K a normal extension of $\mathbb{Q}$? Is it Galois? What is the degree $[K : \mathbb{Q}\ ]$?(What are the conclusions if K is obtained by adjoining **some** root of $f(x)$? Does it depend on which root? Do you know examples of fields with the property that adjunction of **any root of any irreducible polynomial** results in a Galois extension?)

12. List all the subfields of the field $Q(\omega, \theta)$, where $\omega = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ and $\theta = \sqrt[3]{5}$. Which of these subfields are Galois (normal) extensions of Q? In particular, is $Q(\omega, \theta)$ Galois? Give reasons why your list is complete.

13. Give an example of an irreducible polynomial over a field which has a multiple root.

14. Let $r_1, ..., r_5$ be the roots of $X^5 + X^4 + 7$. Calculate $r_1^3 + r_2^3 + ... + r_5^3$

15. If α_i , $i = 1, ..., 4$ are the four roots of

$$X^4 - 3X^2 + 1 = 0$$

calculate the $\sum_{i=1}^{4} {\alpha_i}^2$.

16. Let F_q be the finite field with q elements. Let $f(x) \in F_q[x]$, not necessarily irreducible. Let α be a root of $f(x)$ and let $g(x)$ be the minimal polynomial of α over F_q. Prove that the degree of $g(x)$ is the smallest positive integer n such that $\alpha^{q^n} = \alpha$.

17. Let F be a field of characteristic $p > 0$ and let K be an extension of F. If $\alpha \in K$ is a root of $x^p - a$, $a \in F$, show that $[F(\alpha) : F]$ is 1 or p.

18. Determine the Galois group of $x^4 - 3$ over $\mathbb{Q}$. Is the polynomial separable, why? The formula for the resolvent cubic of $x^4 + bx^3 + cx^2 + dx + e$ is $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$.