1 Groups

1. Prove or Disprove: If H is a characteristic subgroup of K and K is a characteristic subgroup of G then H is characteristic in G.

2. Fix an integer $n > 1$. Prove there are only finitely many isomorphism types of simple groups which have a subgroup of index n.

3. Show that a simple group of order 60 is isomorphic to A_5.

4. Call an invertible function $f : \mathbb{N} \to \mathbb{N}$ finite if $f(n) = n$ for all but finitely many n. Show the group of finite invertible functions contains a unique nontrivial proper normal subgroup.

5. Suppose G is a group of odd order. Show that if H is a normal subgroup of G of order 5, then H is central. Show this result is false if we replace the 5 with a 7.

6. Let D be the subgroup $\{m \cdot 2^n | m, n \in \mathbb{Z}\}$ of the additive group $\mathbb{Q}$. Show D is not isomorphic to the additive group $\mathbb{Q}$.

7. Show that a group with exactly 3 elements of order 2 is not simple.

8. Prove every group of order 105 has a subgroup of order 21.

9. Prove characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic. Prove the commutator subgroup of a group is normal.

10. Find the isomorphism type of each Sylow group and the number of Sylow groups of each order of S_5, S_6, A_5, and A_6.

11. Prove or disprove: If all proper subgroups of a group are cyclic then the group is abelian.

12. Let H be a subgroup of G, and let σ be an automorphism of H. Prove or disprove: There must be an automorphism τ of G such that $\tau(H) = H$ and $\tau|_H = \sigma$.

13. Prove or disprove: The set of squares in a group is a subgroup.

14. Find the automorphism group of the group G consisting of all functions from $C_{10} \to \mathbb{Q}$ (where here the operation is point wise addition of functions). Is there an automorphism of order 11?

15. Prove or Disprove: If every finitely generated subgroup of a group is cyclic, then the group is cyclic.

16. Prove or Disprove: If every finitely generated subgroup of a group is abelian, then the group is abelian.

17. Prove or Disprove: The center of a non-abelian group G is always properly contained in some abelian subgroup.

18. Does S_4 have a subgroup of every order dividing the order of the group? Does S_5?

19. Classify all finite groups whose automorphism group is trivial.

20. Show that if G is a p-group and H is a non-trivial normal subgroup of G then H intersects the center of G nontrivially.

21. Determine all groups with a proper subgroup that contains all proper subgroups of the original group.

22. Show that if $|G| = pm$ and G has a normal subgroup of order p then that subgroup must be central if $(p-1, m) = 1$. Show that last hypothesis was necessary.

23. Let G be a p-group, and let H be the intersection of all index p subgroups of G. Show that H is normal, and that G/H is abelian.

24. Let G be a group of order 72 whose center's order is divisible by 8. Show G is abelian.

25. Show that a group of order $5 \cdot 7 \cdot 11$ has a nontrivial center.

26. Show that any index 2 subgroup of a group contains the set of squares. Is this true for cubes in an index 3 subgroup?

27. How many conjugacy classes are in $\mathrm{GL}_3(\mathbb{F}_2)$?

28. Let G be a group of order 24 with no elements of order 6.
    (a) Prove no subgroup of order 2 is normal
    (b) Prove $C_G(P_3) = P_3$
    (c) Prove there are 4 distinct conjugates of P_3
    (d) Prove G acts faithfully/transitively on $\mathrm{Syl}_3(G)$

    Conclude that $G \cong S_4$.

29. How many elements of order 7 does a simple group of order 168 have?

30. Show that a nilpotent group has subgroups of every order dividing the order of the group.

31. Show that if $|G| = pm$ and G has a normal subgroup of order p, then that subgroup is central if $(p-1, m) = 1$. Show this is not necessarily the case if $(p-1, m) \neq 1$.

32. Is it possible for S_4 to act transitively on a set with 3 elements?

33. How many index 5 subgroups does $\mathbb{Z}^n$ have?

34. Show that if G has a unique element x of order 2, then $x \in Z(G)$.

35. Demonstrate a Sylow subgroup of each order of $\mathrm{GL}_2(\mathbb{F}_3)$.

36. True or False: A group none of whose Sylow subgroups are normal is simple.

37. Show any 2-generated group can have at most 3 index 2 subgroups. How many index 2 subgroups can a 3-generated group have?

38. Let G be a simple group and let p be a prime dividing $|G|$. Suppose that G has $p+1$ Sylow p-subgroups and that P is one of them. Show
    (a) G is isomorphic to a subgroup of S_{p+1}
    (b) p^2 does not divide $|G|$
    (c) The centralizer of P in G is equal to P
    (d) $|G| \big| p(p^2-1)$

39. Find $\#\mathrm{Aut}(C_2 \oplus C_{10})$

40. Which groups of order 8 are isomorphic to subgroups of S_5?

41. True or False: All subgroups are normal $\Rightarrow$ Abelian.

42. Classify all groups with exactly 3 conjugacy classes.

43. True or False: A group all of whose elements have finite order is finite.

44. Show any group of order p^n $(n > 1)$ has an automorphism of order p.

45. Suppose A_4 acts transitively on Ω. What are the possible orders of Ω?

46. Determine all groups with exactly 3 subgroups.

47. Let G be a group of odd order. Prove that if $g \in G$ is conjugate to g^{-1} then $g = 1$.

48. True or False: Every finite group G can be embedded in A_n for some n.

49. $\mathrm{PSL}_n(K)$ denotes the group of $n \times n$ matrices of determinant 1 over K, modulo scalar matrices. Compute the order of $\mathrm{PSL}_2(\mathbb{F}_3)$ and $\mathrm{PSL}_2(\mathbb{F}_5)$.

50. Suppose $\text{char}(F) \neq 2$. Show $\text{GL}_n(K)$ has exactly n conjugacy classes of elements of order 2. If $\text{char}(K) = 2$, show $\text{GL}_n(K)$ has $\lfloor \frac{n}{2} \rfloor$ such conjugacy classes.

51. How many conjugacy classes are there in $\text{GL}_2(\mathbb{F}_q)$?

52. Suppose H is a subgroup of G of index n. Show that G has a normal subgroup of index $\leq n!$. Use this to show there are no simple groups of order $2 \cdot 3^5 \cdot 5$.

2 Rings

1. Prove an Artinian integral domain is a field.

2. Prove or disprove: If R is a commutative ring and $\mathfrak{m}$ is a maximal ideal then $\cap_i \mathfrak{m}^i = (0)$.

3. Let $R = \mathbb{Q}[x]/(x^3 - x^2 - x + 1)$. Show R has exactly 6 ideals and draw a lattice of them.

4. Show the ideal (5) is not prime in the ring $\mathbb{Z}[i]$. What is the isomorphism type of the quotient?

5. Prove or Disprove: The intersection of two prime ideals of a ring is prime.

6. Determine the isomorphism type of the unit group of $k[x]/(x^2)$.

7. Does there exist a ring with 10 elements with no zero divisors?

8. Let R be a commutative ring such that $r^n = r$ for some n for every r. Show that every prime ideal of R is maximal.

9. Suppose R is a domain, and R is Noetherian. Show $R[\frac{1}{f}]$ is Noetherian for $f \neq 0$. Must all rings S satisfying $R \subseteq S \subseteq \text{Frac}(R)$ be Noetherian?

10. Suppose Ω generates $I \leq R$ a Noetherian ring. Then is it necessarily true that some finite subset of Ω generates I.

11. Show Nil $\iff$ Nilpotent for a Noetherian ring R. Is either implication true for a non-Noetherian ring?

12. True or False: A commutative ring with a unique prime ideal is a field.

13. True or False: The direct limit of Noetherian rings is Noetherian.

14. Show there is no unit ring whose additive group is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

15. Suppose R is a unit ring and
$$x \in \bigcap_{M \text{ maximal}} M.$$
Show that $1 + x$ is a unit.

16. If R is the subring of $\mathbb{Z}[x]$ consisting of the polynomials of the form $a_0 + a_1 x + \cdots + a_k x^k$ with $2|a_i$ for $i \geq 1$, show R is not Noetherian.

17. Show $\dim_K (Z(KG)) = \#$ of conjugacy classes of G.

18. Show if $|G| \neq 1$ but $|G| < \infty$ and R is a nonzero ring with 1 that RG is never a domain. Is this still true if G is infinite?

19. Give an example of a ring R and a nonzero prime ideal of R that is not maximal or minimal.

20. Find $\#\mathrm{GL}_3(\mathbb{Z}/6\mathbb{Z})$.

21. Find $\#\mathrm{GL}_3(\mathbb{Z}/4\mathbb{Z})$.

22. Find $\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/10\mathbb{Z}))$

23. For which p is there a nonzero homomorphism $\varphi\colon \mathbb{Z}[i] \to \mathbb{F}_p$?

24. Prove a finite subgroup of the group of units of an integral domain is cyclic. Is this true if the commutativity assumption is removed?

25. True or False: If R is a nonzero commutative ring, then $R^2 \not\cong R^3$ as rings.
How about as R-modules?

26. Prove or Disprove: If the square of a prime ideal is prime, then its square is itself.

27. Suppose A is a commutative ring with 1. Show $A[x]$ has infinitely many maximal ideals.

28. Determine all maximal ideals of $\mathbb{Z}[[x]]$.

29. If $R = \mathcal{C}[x, y]$
    (a) Find a maximal ideal that does not contain xy
    (b) Find a prime ideal that does not contain xy

30. Show that if R is a local ring with maximal ideal M then every element not in the ideal is a unit.

31. Show that if the order of the unit group of a ring R is odd, then the characteristic of R is equal to 2.

32. Show 5 is not the order of the unit group of any ring.

33. True or False: Every ideal of $\mathbb{Z}[x]$ can be generated by two elements.

34. Let α be a real number. Show the set of elements of $\mathbb{Z}[x]$ such that $f(\alpha) = 0$ is an ideal. Is it prime? Might it be maximal?

35. Show $(x-1)(x-2)...(x-n)-1$ is irreducible over $\mathbb{Z}[x]$.

3 Fields

1. Give a polynomial whose Galois Group over $\mathbb{Q}$ is C_3.

2. Show the polynomial $x^4 + 5x^2 + 3x + 2$ is irreducible in $\mathbb{Q}[x]]$.

3. Prove or Disprove: If K is a subfield of F and F is isomorphic to K then $F = K$.

4. Show that if K is a finite extension of $\mathbb{Q}$ then the torsion subgroup of $K^\times$ is finite.

5. Show that any element of a finite field is expressible as a sum of two squares of elements of that field.

6. Let K be a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to S_5. Prove that K is isomorphic to the splitting field of some polynomial of degree 5 over $\mathbb{Q}$.

7. Let $f(x)$ be a degree four irreducible polynomial in $\mathbb{Q}[x]$ with Galois group S_4 and roots $\alpha_1, ..., \alpha_4$. Let K be the splitting field of $f(x)$. Find the Galois group of K over $\mathbb{Q}(\alpha_1\alpha_2 + \alpha_3\alpha_4)$.

8. Prove or Disprove: If F is a field of characteristic p then the Frobenius map $x \mapsto x^p$ is an automorphism of F.

9. Does there exist a field K such that $K^+ \cong K^\times$?

10. List all quadratic subfields of $\mathbb{Q}(\zeta_5)$ in the form $\mathbb{Q}(\sqrt{d})$. Do the same for $\mathbb{Q}(\zeta_8)$ and the splitting field over $\mathbb{Q}$ of $x^4 - 2$.

11. Find all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{27})$ with explicit generators for each.

12. For what q does the polynomial $x^4 + x^3 + x^2 + x + 1$ factor completely over $\mathbb{F}_q$

13. Show $x^4 - x^2 + 1$ is reducible over $\mathbb{F}_p$ for every prime p. Note: $(x^2+1)(x^4-x^2+1) = x^6 + 1$.

14. Consider the extension $\mathbb{Q}(x)$ of $\mathbb{Q}(x^4)$. Find its degree. If it is Galois, find its Galois group, otherwise find its splitting field and its Galois group.

15. Let F be a field of order p^2. Show that $1+1+1+1+1$ is a square in F.

16. Prove or Disprove: The only example of a finite index proper subfield of an algebraically closed field is $\mathbb{R}$ inside of $\mathbb{C}$.

17. Give an example of a degree 3 extension of $\mathbb{Q}$ which is not of the form $\mathbb{Q}[\sqrt[3]{\beta}]$ for some $\beta \in \mathbb{Q}$.

18. Is there an infinite field K such that $|\overline{K}| > |K|$?

19. Show $\mathbb{Q}(\zeta_{35})$ has 3 quadratic subextensions.

20. Describe the action of the Galois group on the roots of $x^{24}+1$ over $\mathbb{Q}$.

21. Describe all q such that -1 is a square in $\mathbb{F}_q$.

22. How many primitive polynomials are there for the extension $\mathbb{F}_{2^{10}}$ of $\mathbb{F}_2$?

23. Prove or Disprove: If $\mathbb{Q}(\alpha) \bigcap \mathbb{Q}(\beta) = \mathbb{Q}$ then $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha+\beta)$.

24. Let $K \subseteq F$ be finite fields with $F = K[\alpha]$ with α satisfying $\alpha^{15} = 1$. Show $[F\colon K] \leq 4$.

25. Suppose $f\colon \mathbb{F}_p \to \mathbb{F}_p$ is a function. Prove it is a polynomial function.

26. Describe the orbits of the Galois group (over $\mathbb{Q}$) of $x^{24}-1$ on the roots.

27. Let $\zeta = e^{2\pi i/7}$. Find $\alpha \in \mathbb{Q}(\zeta)$ such that $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 3$. Show there does not exist $\beta \in \mathbb{Q}(\alpha)$ such that $\beta^3 \in \mathbb{Q}$ but $\beta \notin \mathbb{Q}$.

28. Determine the splitting field K and Galois group of the polynomial $x^4 - 2$ over $\mathbb{Q}$. Determine all quadratic subfields of K.

29. Prove any degree 5 irreducible polynomial with 3 real roots generates an extension with Galois group S_5.

30. Find the Galois group of $x^5 + 7x^3 + 6x^2 + x + 5$ over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ and $\mathbb{Q}$.

31. Let $F = \mathbb{F}_p$ and $E = \mathbb{F}_{p^n}$. Show that $\mathrm{Tr}(x)\colon = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ is a linear transformation from the F-vector space E to F.

32. Suppose $\mathbb{Q}$ has an extension of degree n, K. Show $K \hookrightarrow M_n(\mathbb{Q})$. Show $M_n(\mathbb{Q})$ does not contain isomorphic copies of any fields of degree $> n$.

33. Factor the polynomial $x^4 + x^3 + x^2 + x + 1$ into irreducible factors over $\mathbb{F}_{29}$.

34. Suppose F is a field and $f(x) \in F[x]$ is irreducible. Suppose E is a splitting field for $f(x)$, and that for some $\alpha \in E$, α and $\alpha + 1$ are both roots of $f(x)$. Show F is not characteristic 0.

35. Let F be a field extended by E. Call an element $a \in E$ abelian if $F[a]$ is a Galois extension of F with a Galois group which is abelian. Show that the set of abelian elements of E is a field.

36. Let $f(x) = x^8 + x^4 + 1$, and let $E = \mathrm{Spl}_{\mathbb{Q}}(f)$.
    (a) Compute $[E\colon \mathbb{Q}]$, and find the Galois group of $[E\colon \mathbb{Q}]$.
    (b) How many orbits are there in the action of G on the roots of $f(x)$?
    (c) Same question over $\mathbb{F}_5$ and $\mathbb{F}_7$.

37. Find an extension E of $\mathbb{Q}$ with Galois group $C_3 \times C_3$.

38. (a) Find $[E\colon \mathbb{Q}]$ where E is the splitting field of $x^6 - 4x^3 + 1$ over $\mathbb{Q}$.
    (b) Show $\mathrm{Gal}(E/\mathbb{Q})$ has an element of order 6.

4 Modules

1. Show that if I is injective then $0 \to I \to B \to C \to 0$ splits.

2. Tensor products are right exact. Show by example that they are not left exact.

3. Let T be the $\mathbb{Z}[i]$-module homomorphism from $\mathbb{Z}[i]^2$ to $\mathbb{Z}[i]$ defined by the matrix $\begin{pmatrix} 2i & 4i+2 \\ 2i-2 & i \end{pmatrix}$. Determine whether T is one-to-one and whether T is onto.

4. Describe $\mathbb{Q}[x]/(x^4 - 16)$ as a product of fields.

5. Let R be an integral domain, I injective. Show that for every nonzero $a \in R$, multiplication by a is surjective.

6. Show $\mathbb{Z}/2\mathbb{Z}$ is not a projective $\mathbb{Z}/4\mathbb{Z}$ module.

7. Show that $(A/I) \otimes_A I \cong I/I^2$. Use this to show if A/I is a flat A-module then $I = I^2$.

8. Show that the tensor product of projective modules is projective.

9. Show projective $\Rightarrow$ flat.

10. Give an example (or say why none exists) of a module which is

(a) projective but not injective.
(b) projective but not flat.
(c) injective but not projective.
(d) injective but not flat.
(e) flat but not projective.
(f) flat but not injective.

11. True or False: The set of torsion elements of a module is a submodule.

12. (a) Show that any nontrivial idempotent in a ring R is not a unit.
    (b) Show eR is a projective R-module if $e^2 = e$.

13. True or False: $\prod_{i=1}^{\infty} \mathbb{Z}$ is a free $\mathbb{Z}$-module

14. Let $V = \mathbb{R}^2$. Show $e_1 \otimes e_2 + e_2 \otimes e_1$ is not a simple tensor in $V \otimes_{\mathbb{R}} V$.

15. Show $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$ if m and n are coprime.

16. Show that $K(\alpha) \otimes L \cong L[x]/(f(x))$ where $f(x)$ is the minimal polynomial of α and L is an extension of K. Under what conditions is this a field?

17. Prove that if M is a finitely generated module over a Noetherian ring R and $f\colon M \to M$ is surjective then it is also injective. Hint: consider $\ker(f^n)$. Is the converse true?

5 Linear Algebra

1. Let A and B be two complex matrices satisfying $AB = BA$. Show A and B share an eigenvector.

2. Show two 3×3 complex matrices are similar if they have the same minimal and characteristic polynomials. Is this true for 4×4 matrices?

3. Let $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$. Show there is a constant c such that the limit as n goes to infinity of $(cA)^n$ is a nonzero idempotent matrix E and compute c and E.

4. Show that if x, y, and $x + y$ are eigenvectors of a real matrix A then $x - y$ is also an eigenvector of A.

5. Suppose $A \in M_n(\mathbb{Q})$ and $A^2 = 2I$. Show n is even.

6. Let $V = P_2(\mathbb{R})$ the space of polynomials of degree at most 2. Define $T\colon V \to V$ by $T(f(x)) = f(0) + f(1)(x^2 + x)$. T is a linear transformation on V.

(a) Find the characteristic polynomial for T
(b) Find a basis of V consisting of eigenvectors
(c) Find $T^8(1+x)$

7. True or False: Two $n \times n$ matrices with the same minimal polynomial are conjugate.

8. Prove or Disprove: If $A \in M_n(k)$ with eigenvalues $\lambda_1, ..., \lambda_n$ when considered as an element of $M_n(\overline{k})$ then $\sum \lambda_i^2 \in k$.

9. Prove or Disprove: If $A \in M_n(k)$ with eigenvalues $\lambda_1, ..., \lambda_n$ when considered as an element of $M_n(\overline{k})$ then $\sum \lambda_i \lambda_j \in k$.

10. Under what circumstances is the Frobenius automorphism $\phi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} : x \mapsto x^p$ diagonalizable as a linear transformation over $\mathbb{F}_p$?

11. Find all positive integers that can occur as orders of elements of $\mathrm{GL}_2(\mathbb{R})$.

12. Find all positive integers that can occur as orders of elements of $\mathrm{GL}_4(\mathbb{Q})$. Exhibit an element of order 5.

13. What is the largest order an element of $GL_{10}(\mathbb{Q})$ can have is?

14. Suppose A is an $n \times n$ matrix over $\mathcal{C}$ with minimal polynomial $(x-\lambda)^n$ where $\lambda \neq 0$. Find the Jordan form of A^2. What if $\lambda = 0$?

15. Let X be a subspace of all $n \times n$ matrices over $\mathcal{C}$. Suppose all nonzero matrices in X are invertible. Conclude $\dim_{\mathcal{C}}(X) \leq 1$. Show explicitly this is false for $\mathbb{R}$.

16. (a) Show that the trace of a nilpotent matrix over a field is 0.
    (b) Is this true over an integral domain?
    (c) A commutative ring that is not a field?

17. Let K be an algebraically closed field. Let $K[A]$ denote the K-span of the matrices $A^0, A^1, \ldots$. Show that A is diagonalizable if and only if $K[A]$ contains no nilpotent elements.

18. Show the space of nxn matrices over a field k all of whose rows and columns sum to the same value is a k vector space and compute its dimension.

19. Let k be a field. Show that any $n+1$ dimensional subspace of $M_n(k)$ contains a non-zero matrix which is not invertible.

20. Give an example of a transformation from a finite dimensional vector space to itself which has no eigenvalues. Give an example of a transformation from a complex vector space to itself which has no eigenvalues.