1. Let $\mathbb{F}_p$ be the field $\mathbb{Z}/p\mathbb{Z}$.
   (a) How many monic polynomials of degree 2 with coefficients in $\mathbb{F}_p$ are irreducible over $\mathbb{F}_p$?
   (b) How many monic polynomials of degree 3 with coefficients in $\mathbb{F}_p$ are irreducible over $\mathbb{F}_p$?
2. Let $G = \mathbb{F}_{17}^{\times}$ be the multiplicative group of the field $\mathbb{F}_{17}$. Does there exist a transitive group action of G
   (a) on a set with 8 elements?
   (b) on a set with an odd number of elements?
3. Let G be a group of order 12.
   (a) Must G be abelian?
   (b) List all possible abelian G of order 12 (up to isomorphism).
4. Is the ideal generated by $x^7 + 1$ and $x^5 + 1$ a principal ideal in $\mathbb{F}_2[x]$? If not, why? If so, find a generator.
5. How many elements in S_5 have order exactly 6?
6. Let d be the smallest index of a proper subgroup of S_8. What is d? Do there exist two distinct subgroups of S_8 of index d?
7. Let G be a finite group. Let H be a subgroup of G which is not normal. Can the index of H be 2? Can the index of H be 3?
8. Are the following rings UFDs? Are the rings PIDs?
   (a) $\mathbb{Z}[x]$
   (b) $(\mathbb{Z}/2\mathbb{Z})[[x]]$
   (c) $\mathbb{R}[x]/(x^2 - 1)$
   (d) $\mathbb{R}[x]/(x^2 + 1)$

   Explain why or why not.
9. Which of the following rings are fields?
   (a) $\mathbb{Z}[x]/(3, x^2 + x + 1)$
   (b) $\mathbb{Z}[x]/(4, x^2 + x + 1)$
   (c) $\mathbb{Z}[x]/(2, x^2 + x + 1)$

   Explain why or why not.

10. What is the automorphism group $\mathrm{Aut}(G)$ of the following groups G?
    (a) $\mathbb{Z}/2\mathbb{Z}$
    (b) $\mathbb{Z}/8\mathbb{Z}$
    (c) $\mathbb{Z}$
    (d) S_3
11. In the ring $\mathbb{C}[x, y]$, do the following inclusions of ideals hold?
    (a) $(x-1, y-2) \subset (y^2 - 4x)$
    (b) $(y^2 - 4x) \subset (x-1, y-2)$

    Prove your answer.
12. Let $a \in \mathbb{Z}$ be a number which satisfies

$$\bar{a} = \bar{3} \bmod 15,$$
$$\bar{a} = \bar{1} \bmod 17.$$

    Does this information suffice to compute $\bar{a}$ mod 255? If so, what is the answer?
13. Do all groups of order 4 occur as subgroups of S_4? Do all groups of order n occur as subgroups of S_n?
14. Let G be the group of rotational symmetries of a regular solid cube.
    (a) How many elements does G have?
    (b) Does there exist a surjective homomorphism from G to S_3?
15. Does the alternating group A_{17} have any subgroup of index 2 or of index 3? Does the alternating group A_{17} have any elements of order 12?
16. Describe all possible homomorphisms
    (a) $f : S_3 \to \mathbb{Z}/6\mathbb{Z}$,
    (b) $g : S_5 \to \mathbb{Z}/2\mathbb{Z}$.
17. Which of the following statements are true for all groups G of order 56?
    (a) They contain a subgroup of order 2.
    (b) They contain a subgroup of order 3.
    (c) The number of different subgroups of order 8 contained in G is exactly 2.
18. In the ring $R = \mathbb{R}[x]$, are the following subsets ideals of R? Prove your answer.
    (a) $\{f(x) \in R : f(\pi) = 0\}$
    (b) $\{f(x) \in R : f'(\pi) = 0\}$
    (c) $\{f(x) \in R : f(i) = 0\}$
    (*Note*: we can evaluate a real polynomial at the complex number $i \in \mathbb{C}$)
    (d) $\{f(x) \in R : f(0) = f(1)\}$
19. Compute the conjugate of the group element $a = (3\,5\,2\,4) \in S_5$ by the element $(2\,3)$. How many elements of S_5 are conjugate to a?

20. Let $\mathbb{F}_2$ be the field with two elements.
    (a) Show that, for every degree $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}_2[x]$.
    (b) Let $\overline{\mathbb{F}}_2$ be the algebraic closure of $\mathbb{F}_2$. Show that $\overline{\mathbb{F}}_2$ is infinite.

21. Let A be a module over the ring $\mathbb{C}[x]$. Since $\mathbb{C} \subset \mathbb{C}[x]$, A is a $\mathbb{C}$-vector space.
    (a) List all $\mathbb{C}[x]$-modules A with $\dim_{\mathbb{C}} A = 1$, up to isomorphism.
    (b) List all $\mathbb{C}[x]$-modules A with $\dim_{\mathbb{C}} A = 2$, up to isomorphism.
    (c) List all $\mathbb{C}[x]$-modules A with $\dim_{\mathbb{C}} A = 3$, up to isomorphism.

22. What is the degree over $\mathbb{Q}$ of the splitting field over $\mathbb{Q}$ of the polynomial $x^3 - 2$?

23. Is the field $\mathbb{Q}[1+i] \subset \mathbb{C}$ the splitting field in $\mathbb{C}$ over $\mathbb{Q}$ of some polynomial $f \in \mathbb{Q}[x]$? If so, give an example of such a polynomial f.

24. Let R be a commutative ring with unit, and let $R^\times \subset R$ be the group of units. Consider elements $X \in R^\times$ satisfying $X = X^{-1}$.
    (a) Show that if R is a field $R = k$, there are at most two such elements. When is there exactly one such element?
    (b) What if R is a domain? Are there still only at most two elements $X \in R^\times$ with $X = X^{-1}$? If so, give a proof, if not, give a counterexample.
    (c) What if we let R be a noncommutative ring with unit? Are there still at most two such elements X?

25. Let $G = \mathrm{GL}_2(\mathbb{F}_2)$ be the group of invertible 2×2-matrices with coefficients in $\mathbb{F}_2$. Let G act on the set of nonzero vectors in $(\mathbb{F}_2)^2$ in the usual way. Is the induced homomorphism $G \to S_3$ an isomorphism?

26. Let G be a group of order p^n (where p is prime) acting on a finite set X. Let $X^G \subset X$ be the set of fixed points. Is it true that $|X| = |X^G| \bmod p$? Answer with proof.

27. Give an example (with proof) of a group G which is not abelian and not isomorphic to any of the groups S_n (for $n \geq 1$).

28. Determine $\gcd(k^2 + k + 1, 3k^2 + 4k + 5)$ for each $k \in \mathbb{Z}$.

29. Let $\xi = 1.7099759466\ldots$ be the real cube root of 5. Is the field
$$\mathbb{Q}(i, \sqrt{3}, \xi) \subset \mathbb{C}$$
the splitting field in $\mathbb{C}$ over $\mathbb{Q}$ of some polynomial $f \in \mathbb{Q}[x]$? If so, give an example of such a polynomial f.

30. Is $\sqrt{2} - \sqrt{3}$ algebraic over $\mathbb{Q}$? If so, find the minimal polynomial over $\mathbb{Q}$.

31. Let $\mathbb{F}_q$ be the field with $q = p^n$ elements where p is an odd prime. For how many elements $\alpha \in \mathbb{F}_q$ does there exist a solution in $\mathbb{F}_q$ of the quadratic equation
$$x^2 - \alpha = 0\,?$$

32. Let R be an integral domain with finitely many elements. Must R be a field? Answer with proof.

33. Let $\mathbb{F}_q$ be the field with $q = 2^n$ elements. For how many elements $\alpha \in \mathbb{F}_q$ does there exist a solution in $\mathbb{F}_q$ of the quadratic equation
$$x^2 - \alpha = 0\,?$$

34. Let $\varphi : R \to S$ be a homomorphism of commutative rings.
    (a) If $I \subset R$ is an ideal, must $\varphi(I)$ be an ideal?
    (b) If $J \subset S$ is an ideal, must $\varphi^{-1}(J)$ be an ideal?

35. Let $R \neq 0$ be a commutative ring whose only ideals are $\{0\}$ and R. Show that R is a field.

36. (a) Consider the polynomials $p, q \in \mathbb{Q}[x]$ defined by
$$p = x^3 - \frac{5}{2}x^2 + \frac{3}{2}x \text{ and } q = 2x^2 - x - 3.$$
    Compute the Euclidean division of p by q.
    (b) Find a single generator of the principal ideal $(p, q)\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$.

37. Let R be a UFD. Let $a, b \in R$ be coprime elements (that is, $\gcd(a, b) \in R^\times$) and $c \in R$. Suppose that $a|c$ and $b|c$. Prove that $ab|c$.

38. Find the order (if finite) of the following elements:
    (a) i, $e^{i\sqrt{3}\pi}$ and $e^{\frac{2\pi i}{17}}$ in the group $\mathbb{C}^\times$,
    (b) $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ and $\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ in the group $\mathrm{GL}_2(\mathbb{C})$,
    (c) $1, 2$ and 3 in $\mathbb{F}_{17}^\times$.

39. Let p be a prime number. For every integer $k \geq 1$, define
$$A_k = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \;\middle|\; \det(A)^k = 1 \right\} \subset \mathrm{GL}_2(\mathbb{F}_p).$$
    (a) Show that A_k is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.
    (b) Is A_k a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$?
    (c) What is the index of A_{p-1} in $\mathrm{GL}_2(\mathbb{F}_p)$?

40. Let G be a group of order 3^{17}, and let $H \subset G$ be a subgroup of index 3. Must H be normal?

41. Show that the center of S_{17} is trivial. What is $[S_{17}, S_{17}]$? Recall: for a group G, the commutator $[G, G]$ is defined as the subgroup of G generated by $\{aba^{-1}b^{-1} : a, b \in G\}$.

42. Let S_n act on $\{1,\ldots,n\}$ via the standard action. Define an action of S_n on
$$\{1,\ldots,n\}\times\{1,\ldots,n\}$$
by
$$g\cdot(i,j)=(g(i),g(j))\,.$$
Find and describe all the orbits of this action.

43. Is there a transitive action of S_5 on a set with 10 elements? Is there a transitive action of S_5 on a set with 20 elements?

44. Let $a\in\mathbb{Z}\setminus\{0,\pm1\}$ be a *square-free* integer, that is, an integer which is not divisible by any perfect square except 1. Prove that, for each $n\in\mathbb{Z}_{>0}$, the polynomial $x^n-a\in\mathbb{Q}[x]$ is irreducible.

45. Let K be a field of characteristic $\neq 2$ and L/K a field extension of degree 2. Show that there exists $\alpha\in L$ such that $\alpha^2\in K$ and $L=K(\alpha)$.

46. Let $L=K(\alpha)/K$ be a field extension such that $[L:K]$ is odd. Prove that $L=K(\alpha^2)$.

47. Is the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ countable? Are there real numbers which are not algebraic over $\mathbb{Q}$?

48. Let M be an $n\times n$ matrix with complex coefficients. Let
$$J=\{f\in\mathbb{C}[x]\,|\,f(M)=0\}\,.$$
In other words, J is the set of polynomials which vanish when evaluated at M.

    (a) Is J an ideal of $\mathbb{C}[x]$?

    (b) Let $g\in J$ be a nonzero polynomial of minimal degree. Can the degree of g be equal to $n+1$?

49. Let $R=\mathbb{Z}[x,y]$. Can you find a tower of ideals
$$I_0\subset I_1\subset I_2\subset I_3\subset R$$
where each $I_i\subset R$ is a prime ideal?

50. Consider the cubic polynomial $f(x)=(x^2+17x+1)(x-17)\in\mathbb{Z}[x]$. For each prime p, let
$$\overline{f}(x)\in\mathbb{F}_p[x]$$
be the polynomial defined by taking the coefficients of f mod p. For which primes does $\overline{f}(x)$ have repeated roots in the algebraic closure of $\mathbb{F}_p$?