1. Let a be a nonzero nonunit of an integral domain R.

(a) Define "a is irreducible".

(b) Define "a is a prime element".

(c) Prove that if a is a prime element, then a is irreducible.

(d) Give an example of an integral domain R and a nonzero nonunit a of R that is irreducible but not a prime element. Explain why in your example a is irreducible but not a prime element.

2. Let $\mathbb{Z}$ denote the ring of integers. Diagram the lattice of ideals of the polynomial ring $\mathbb{Z}[x]$ that contain the ideal $(3, x^3 - 1)$. Give generators for each such ideal.

3. Let R be an integral domain.

(a) Define "$N : R \to \mathbb{Z}^+ \cup \{0\}$ is a Dedekind-Hasse norm."

(b) Prove that if R has a Dedekind-Hasse norm, then R is a principal ideal domain

(c) Prove that if R is a principal ideal domain, then R has a Dedekind-Hasse norm.

4. State Gauss' Lemma.

5. Let R be an integral domain with field of fractions F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$.

(a) If $a(x) \notin R[x]$, prove that R is not a UFD.

(b) Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

6. Assume that $f(x)$ and $g(x)$ are polynomials in $\mathbb{Q}[x]$ and that $f(x)g(x) \in \mathbb{Z}[x]$. Prove that the product of any coefficient of $f(x)$ with any coefficient of $g(x)$ is an integer.

7. Let R be a commutative ring with 1. Recall that $a \in R$ is called **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$, and a nonzero element $a \in R$ is said to be a **zero divisor** if there exists a nonzero $b \in R$ such that $ab = 0$.

(a) Give an example where R has a zero divisor that is not nilpotent.

(b) Give an example where every zero divisor of R is nilpotent and where R has a nonzero nilpotent element.

8. Consider the quadratic integer ring $R = \mathbb{Z}[\sqrt{-5}]$.

(a) Diagram the lattice of ideals of R that contain (2).

(b) Diagram the lattice of ideals of R that contain (3).

(c) Diagram the lattice of ideals of R that contain (6).

9. Let p be a prime integer and let $\mathbb{F}_p$ denote the field with p elements.

(a) Prove or disprove that every finite algebraic field extension of $\mathbb{F}_p$ is Galois.

(b) Let K and L be finite algebraic field extensions of $\mathbb{F}_p$. If $[K : \mathbb{F}_p] \leq [L : \mathbb{F}_p]$, does it follow that K is isomorphic to a subfield of L? Justify your answer.

10. Prove that the polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime integer p.

11. Let K/F be a finite separable algebraic field extension and let L/F be the Galois closure of K over F. Let $H \leq \mathrm{Gal}(L/F)$ be the subgroup corresponding to K.

(a) For $\alpha \in K$ define the **norm** $N_{K/F}(\alpha)$ of α from K to F.

(b) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F and let $n = [K : F]$. Prove that d divides n.

(c) State a relationship that holds between $N_{K/F}(\alpha)$ and one of the coefficients of $m_\alpha(x)$.

(d) For $\alpha \in K$ define the **trace** $Tr_{K/F}(\alpha)$ of α from K to F.

(e) With $m_\alpha(x)$ as in (b), state a relationship that holds between $Tr_{K/F}(\alpha)$ and one of the coefficients of $m_\alpha(x)$.

12. Let $\alpha_1, \ldots, \alpha_n$ be the roots of a polynomial $g(x)$ of degree n. Define the **discriminant** D of $g(x)$.

13. Let p be a prime integer. Prove that the image of at least one of $2, 3$ or 6 in the field $\mathbb{F}_p$ is a square.

14. True or false: If $f(x), g(x) \in \mathbb{Q}[x]$ are irreducible polynomials that have the same splitting field, then $\deg f = \deg g$. Justify your answer.

15. Let F be a field and let K_1/F and K_2/F be finite algebraic Galois extensions contained in an algebraic closure $\overline{F}$ of F. Prove or disprove that the composite field K_1K_2 is Galois over F.

16. Let $\zeta \in \mathbb{C}$ be a primitive 7th root of unity. Diagram the lattice of subfields of $\mathbb{Q}(\zeta)$ giving generators for each.

17. Let $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$.

(a) What is the minimal polynomial for α over $\mathbb{Q}$?

(b) List the conjugates of α over $\mathbb{Q}$.

(c) List the conjugates of α over $\mathbb{Q}(\sqrt{2})$.

(d) Prove that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois and determine its Galois group.

18. Let $\beta = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$.

(a) What is the minimal polynomial for β over $\mathbb{Q}$?

(b) List the conjugates of β over $\mathbb{Q}$.

(c) List the conjugates of β over $\mathbb{Q}(\sqrt{3})$.

(d) Is $\mathbb{Q}(\beta)/\mathbb{Q}$ Galois ? Justify your answer.

19. Let $L/\mathbb{Q}$ be the Galois closure of the simple algebraic field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. Let p be a prime that divides the order of $\mathrm{Gal}(L/\mathbb{Q})$. Prove that there exists a subfield F of L such that $[L : F] = p$ and $L = F(\alpha)$.

20. Suppose $L/\mathbb{Q}$ is a finite algebraic field extension with $[L : \mathbb{Q}] = 4$. Is it possible that there exist precisely two subfields K_1 and K_2 of L for which $[L : K_i] = 2$? Justify your answer.