Let $\mathbb{Z}$ denote the ring of integers and $\mathbb{Q}, \mathbb{C}$ the fields of rational and complex numbers, respectively.

(20) 1. Let $\mathbb{Q}(x)$ denote the field of rational functions in an indeterminate $x$ with coefficients from $\mathbb{Q}$.

(i) Describe the group $\text{Aut}(\mathbb{Q}(x)/\mathbb{Q}(x^2))$ of automorphisms of $\mathbb{Q}(x)$ that fix the field $\mathbb{Q}(x^2)$. Is the field extension $\mathbb{Q}(x)/\mathbb{Q}(x^2)$ Galois?

(ii) Describe the group $\text{Aut}(\mathbb{Q}(x)/\mathbb{Q}(x^3))$ of automorphisms of $\mathbb{Q}(x)$ that fix the field $\mathbb{Q}(x^3)$. Is the field extension $\mathbb{Q}(x)/\mathbb{Q}(x^3)$ Galois?

(iii) Let $f = x^2 - x$. Describe the group $\text{Aut}(\mathbb{Q}(x)/\mathbb{Q}(f))$ of automorphism of $\mathbb{Q}(x)$ that fix the field $\mathbb{Q}(f)$. Is the field extension $\mathbb{Q}(x)/\mathbb{Q}(f)$ Galois?

(iv) Let $\phi : \mathbb{Q}(x) \to \mathbb{Q}(x)$ be the automorphism determined by defining $\phi(x) = x + 1$ and let $K = \{r \in \mathbb{Q}(x) \mid \phi(r) = r\}$ be the fixed field of $\phi$. What is $[\mathbb{Q}(x) : K]$? What is $[K : \mathbb{Q}]$?

(v) For $f = x^2 - x$, what is the field $\mathbb{Q}(x^2) \cap \mathbb{Q}(f)$?
Recall that if $R$ and $S$ are rings, then $R \times S = \{(r, s) \mid r \in R, s \in S\}$ is a ring where addition and multiplication in $R \times S$ are defined componentwise.

(6) 2. Describe all the prime ideals of $\mathbb{Z} \times \mathbb{Z}$.

(16) 3. Consider the polynomial ring $\mathbb{Z}[x]$.
   (i) Define $\phi_1 : \mathbb{Z}[x] \to \mathbb{Z}$, by $\phi_1(f(x)) = f(1)$ for every $f(x) \in \mathbb{Z}[x]$. Give generator(s) for the ideal ker $\phi_1$.

   (ii) Define $\phi_{-1} : \mathbb{Z}[x] \to \mathbb{Z}$, by $\phi_{-1}(f(x)) = f(-1)$ for every $f(x) \in \mathbb{Z}[x]$. Give generator(s) for the ideal ker $\phi_{-1}$.

   (iii) Define $\phi : \mathbb{Z}[x] \to \mathbb{Z} \times \mathbb{Z}$ by $\phi(f(x)) = (f(1), f(-1))$ for every $f(x) \in \mathbb{Z}[x]$. Give generator(s) for the ideal ker $\phi$.

   (iv) Prove or disprove that $\phi$ is surjective.
4. Let $K/F$ be a finite separable algebraic field extension and let $\alpha \in K$.

(i) Define the norm $N_{K/F}(\alpha)$ of $\alpha$ from $K$ to $F$.

(ii) Prove that $N_{K/F}(\alpha) \in F$.

(iii) Define the trace $Tr_{K/F}(\alpha)$ of $\alpha$ from $K$ to $F$.

(iv) Prove that $Tr_{K/F}(\alpha) \in F$.

(v) For $K = \mathbb{Q}(\sqrt[3]{2})$, compute $N_{K/\mathbb{Q}}(2\sqrt[3]{2})$ and $Tr_{K/\mathbb{Q}}(2\sqrt[3]{2})$.

(vi) For $K = \mathbb{Q}(\sqrt[3]{2})$, compute $N_{K/\mathbb{Q}}(2)$ and $Tr_{K/\mathbb{Q}}(2)$. 
5. Find all subgroups of the cyclic group $\mathbb{Z}_{45} = \langle x \rangle$, giving a generator for each. Diagram the lattice of subgroups.

6. Diagram the lattice of ideals of the ring $R = \mathbb{Z}[x]/(15, x^2 + 1)$. What is the cardinality of $R$?
7. Suppose $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$.

(i) Define “$\alpha$ can be expressed by radicals” or the equivalent phrase “$\alpha$ can be solved for in terms of radicals.”

(ii) For a polynomial $f(x) \in \mathbb{Q}[x]$, define “$f(x)$ can be solved by radicals.”

8. For $n$ a positive integer, let $\mathbb{Z}_n$ denote a cyclic group of order $n$.

(i) What is the order of the group $\text{Aut}(\mathbb{Z}_n)$ of automorphism of $\mathbb{Z}_n$? Explain your answer.

(ii) Are the groups $\text{Aut}(\mathbb{Z}_7)$ and $\text{Aut}(\mathbb{Z}_9)$ isomorphic? Justify your answer.

(iii) Are the groups $\text{Aut}(\mathbb{Z}_8)$ and $\text{Aut}(\mathbb{Z}_{12})$ isomorphic? Justify your answer.
9. Let $\omega \in \mathbb{C}$ be a primitive 9-th root of unity.

(i) What is $[\mathbb{Q}(\omega) : \mathbb{Q}]$?

(ii) List the distinct conjugates of $\omega + \omega^{-1}$ over $\mathbb{Q}$.

(iii) What is the group $\text{Aut}(\mathbb{Q}(\omega + \omega^{-1})/\mathbb{Q})$? Is $\mathbb{Q}(\omega + \omega^{-1})$ Galois over $\mathbb{Q}$?

(iv) Diagram the lattice of subfields of $\mathbb{Q}(\omega)$ giving generators for each.
10. Let $F$ be a field. For each nonconstant monic polynomial $f = f(x) \in F[x]$, let $x_f$ be an indeterminate. Consider the polynomial ring $R = F[x_f]$, and let $I$ be the ideal of $R$ generated by the polynomials $f(x_f)$, where $f$ varies over all the nonconstant monic polynomials in $F[x]$.

(i) Prove that $I \neq R$.

(ii) Prove that there exists an extension field $K$ of $F$ in which each nonconstant monic polynomial $f \in F[x]$ has a root.

11. Let $K/F$ be an algebraic field extension. Suppose $R$ is a subring of $K$ such that $F \subseteq R$. Prove or disprove that $R$ is a field.
(18) 12. (i) Let $K/\mathbb{Q}$ be the splitting field of the polynomial $x^5 - 1 \in \mathbb{Q}[x]$. Diagram the lattice of subfields of $K/\mathbb{Q}$. For each subfield, give generators and list its degree over $\mathbb{Q}$.

(ii) Let $L/\mathbb{Q}$ be the splitting field of the polynomial $x^5 - 2 \in \mathbb{Q}[x]$. Diagram the lattice of subfields of $L/\mathbb{Q}$. For each subfield, give generators and list its degree over $\mathbb{Q}$.
(8) 13. Diagram the lattice of subgroups of the dihedral group $D_8$.

(10) 14. Let $G = \{ z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+ \}$. Define $\phi : G \to G$ by $\phi(z) = z^4$.

(i) What is the order of $\ker(\phi)$?

(ii) Prove or disprove that $\phi$ is surjective.
15. Let $\mathbb{F}_3$ denote the field with 3 elements. Prove or disprove that the polynomial ring $\mathbb{F}_3[x]$ has infinitely many nonassociate prime elements.

16. Let $R$ be a commutative ring with 1.
   
   (i) Define the characteristic of $R$.

   (ii) Does there exist a ring having characteristic 6? Justify your answer.
(8) 17. (i) Does there exist a field having 6 elements? If so, describe how to obtain such a field; if not, explain why not.

(ii) Does there exist a field having 25 elements? If so, describe how to obtain such a field; if not, explain why not.

(8) 18. Suppose $H$ and $K$ are normal subgroups of a group $G$ and that $H \cap K = 1$, where 1 denotes the identity subgroup. If $x \in H$ and $y \in K$ is it always true that $xy = yx$? Justify your answer.