(b) Prove that K is not a normal extension of F. [If it were, conjugate β over F to show that K would contain a p^{th} root of s and then also a p^{th} root of t, so $[K : F] \geq p^2$, a contradiction.]

(c) Prove that there is no field K_0 such that $F \subseteq K_0 \subseteq K$ with K_0/F purely inseparable and K/K_0 separable. [If there were such a field, use Exercise 1 and the fact that the composite of two normal extensions is again normal to show that K would be a normal extension of F.]

4. Under the notation of the previous exercise prove that α, s is a separating transcendence base for K over $\mathbb{F}_p$.

5. Let p be a prime, let t be transcendental over $\mathbb{F}_p$ and let K be obtained by adjoining to $\mathbb{F}_p(t)$ all p-power roots of t. Prove that K has transcendence degree 1 over $\mathbb{F}_p$ and has no separating transcendence base.

6. Show that if t is transcendental over $\mathbb{Q}$ then $\mathbb{Q}(t, \sqrt{t^3 - t})$ is not a purely transcendental extension of $\mathbb{Q}$. (This is an example of what is called an *elliptic* function field.)

7. Let k be the field with 4 elements, t a transcendental over k, $F = k(t^4 + t)$ and $K = k(t)$.

(a) Show that $[K : F] = 4$.

(b) Show that K is separable over F.

(c) Show that K is Galois over F.

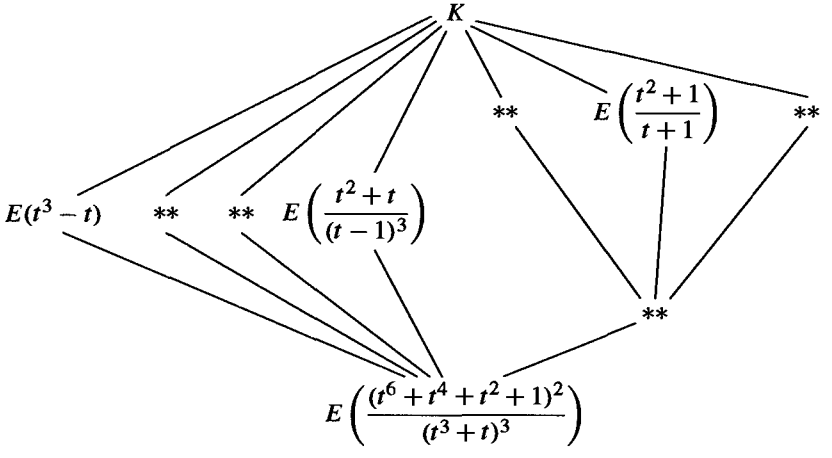
(d) Describe the lattice of subgroups of the Galois group and the corresponding lattice of subfields of K, giving each subfield in the form $k(r)$, for some rational function r.

8. Let p be an odd prime, k an algebraically closed field of characteristic p and let t be transcendental over k. Suppose F is a degree 2 field extension of $k(t)$. Show that F can be written in the form $k(t, y)$, for some $y \in F$ with $y^2 \in k(t)$ and y transcendental over k. If $y^2 = 4t^3 - t - 1$, find $[F : k(y)]$ and describe $k(t) \cap k(y)$ as $k(r)$, for some $r \in k(t)$.

9. Let t be transcendental over $\mathbb{F}_3$, let $K = \mathbb{F}_3(t)$, let $G = \text{Aut}(K/\mathbb{F}_3)$ and let F be the fixed field of G.

(a) Prove $G \cong S_4$ and deduce that there is a unique field E with $F \subseteq E \subseteq K$ and $[E : F] = 2$. [Recall that $G \cong PGL_2(\mathbb{F}_3)$; show that $GL_2(\mathbb{F}_3)$ permutes the 4 lines in a 2-dimensional vector space over $\mathbb{F}_3$ and the kernel of this permutation representation is the scalar matrices.]

(b) Complete the description of the lattice of subfields of K containing E:



Give each subfield in the form $E(r)$ for some rational function r. (The lattice of

subgroups of A_4 appears in Section 3.5).

10. Prove that a purely transcendental proper extension of a field is never algebraically closed.

11. Let S be a set of independent transcendentals over a field F and let Ω be an algebraic closure of $F(S)$. Prove that any permutation on S extends to an element of $\text{Aut}(F(S)/F)$. Prove that any such automorphism of $F(S)$ extends to an automorphism of Ω. Deduce that $\mathbb{C}$ has infinitely many automorphisms.

12. Let K be a subfield of $\mathbb{C}$ maximal with respect to the property "$\sqrt{2} \notin K$."
- **(a)** Show such a field K exists.
- **(b)** Show that $\mathbb{C}$ is algebraic over K.
- **(c)** Prove that every finite extension of K in $\mathbb{C}$ is Galois with Galois group a cyclic 2-group.
- **(d)** Deduce that $[\mathbb{C} : K]$ is countable (and not finite).

13. Let K be the fixed field in $\mathbb{C}$ of an automorphism of $\mathbb{C}$. Prove that every finite extension of K in $\mathbb{C}$ is cyclic.

14. Let K_n be the splitting field of $(x^2 - p_1)(x^2 - p_2) \cdots (x^2 - p_n)$ over $\mathbb{Q}$, where $p_1, \ldots, p_n$ are the first n primes. Prove that the Galois group of $K_n/\mathbb{Q}$ is an elementary abelian 2-group of order 2^n.

15. Let $K_0 = \mathbb{Q}$ and for $n \geq 0$ define the field K_{n+1} as the extension of K_n obtained by adjoining to K_n all roots of all cubic polynomials over K_n. Let K be the union of the subfields K_n, $n \geq 0$. Prove that K is a Galois extension of $\mathbb{Q}$. Prove that every cubic polynomial over K splits completely over K. Prove that there are nontrivial algebraic extensions of K.

16. Let F be the composite of all the splitting fields of irreducible cubics over $\mathbb{Q}$. Prove that F does not contain all quadratic extensions of $\mathbb{Q}$.

17. Let $K_0 = \mathbb{Q}$ and for $n \geq 0$ define the field K_{n+1} as the extension of K_n obtained by adjoining to K_n all radicals of elements in K_n. Let K be the union of the subfields K_n, $n \geq 0$. Prove that K is a Galois extension of $\mathbb{Q}$. Prove that there are no nontrivial solvable Galois extensions of K. Prove that there are nontrivial Galois extensions of K.

18. Let $F_0 = \mathbb{Q}$ and for $n \geq 0$ define the field F_{n+1} as the extension of F_n obtained by adjoining to F_n all real radicals of elements in F_n. Let F be the union of the subfields F_n, $n \geq 0$. Let K^+ be the fixed field of complex conjugation restricted to the field K in the previous exercise (the maximal real subfield of K). Prove that $F \neq K^+$.

19. This exercise proves that if K/F is a Galois extension of fields, then $\text{Gal}(K/F)$ is isomorphic to $\varprojlim \text{Gal}(L/F)$, where the inverse limit is taken over all the finite Galois extensions L of F contained in K.
- **(a)** Show that K is the union of the fields L.
- **(b)** Prove that the map $\varphi : \text{Gal}(K/F) \to \varprojlim \text{Gal}(L/F)$ defined by mapping σ in $\text{Gal}(K/F)$ to $(\ldots, \sigma|_L, \ldots)$, where $\sigma|_L$ is the restriction of σ to L, is a homomorphism.
- **(c)** Show that φ is injective.
- **(d)** If $(\ldots, \sigma_L, \ldots) \in \varprojlim \text{Gal}(L/F)$, define $\sigma \in \text{Gal}(K/F)$ by $\sigma(\alpha) = \sigma_L(\alpha)$ if $\alpha \in L$. Prove that σ is a well defined automorphism and deduce that φ is surjective.

Part V

INTRODUCTION TO COMMUTATIVE RINGS, ALGEBRAIC GEOMETRY, AND HOMOLOGICAL ALGEBRA

In this part of the book we continue the study of rings and modules, concentrating first on commutative rings. The topic of commutative algebra, which is of interest in its own right, is also a basic foundation for other areas of algebra. To indicate some of the importance of the algebraic topics introduced, we parallel the development of the ring theory in Chapter 15 with an introduction to affine algebraic geometry. Each section first presents the basic algebraic theory and then follows with an application of those ideas to geometry together with an indication of computational methods using the theory of Gröbner bases from Chapter 9. The purpose here is twofold: the first is to present an application of algebraic techniques in the important branch of mathematics called Algebraic Geometry, and the second is to indicate some of the motivations for the algebraic concepts introduced from their origins in geometric questions.

This connection of geometry and algebra shows a rich interplay between these two areas of mathematics and demonstrates again how results and structures in one circle of mathematical ideas provide insights into another.

In Chapter 16 we continue with some of the fundamental structures involving commutative rings, culminating with Dedekind Domains and a structure theorem for modules over such rings which is a generalization of the structure theorem for modules over P.I.D.s in Chapter 12.

In Chapter 17 we describe some of the basic techniques of "homological algebra," which continues with some of the questions raised by the failure of exactness of some of the sequences considered in Chapter 10. The cohomology of groups in this chapter is intended to serve both as a more in-depth application of homological algebra to see its uses in practice, and as a relatively self contained exposition of this important topic.

CHAPTER 15

Commutative Rings and Algebraic Geometry

Throughout this chapter R will denote a commutative ring with $1 \neq 0$.

15.1 NOETHERIAN RINGS AND AFFINE ALGEBRAIC SETS

In this section we study Noetherian rings in greater detail. These are a natural generalization of Principal Ideal Domains and were introduced briefly in Chapter 12. Note that when R is considered as a left module over itself, its R-submodules are precisely its ideals, so the definition in Section 1 of Chapter 12 may be phrased in the following form:

Definition. A commutative ring R is said to be *Noetherian* or to satisfy the *ascending chain condition on ideals* (or *A.C.C. on ideals*) if there is no infinite increasing chain of ideals in R, i.e., whenever $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an increasing chain of ideals of R, then there is a positive integer m such that $I_k = I_m$ for all $k \geq m$.

Proposition 1. If I is an ideal of the Noetherian ring R, then the quotient R/I is a Noetherian ring. Any homomorphic image of a Noetherian ring is Noetherian.

Proof: If R is a ring and I is an ideal in R, then any infinite ascending chain of ideals in the quotient R/I would correspond by the Lattice Isomorphism Theorem to an infinite ascending chain of ideals in R. This gives the first statement, and the second follows by the first Isomorphism Theorem.

Theorem 2. The following are equivalent:

(1) R is a Noetherian ring.

(2) Every nonempty set of ideals of R contains a maximal element under inclusion.

(3) Every ideal of R is finitely generated.

Proof: The proof is identical to that of Theorem 1 in Section 12.1 in the special case where the R-module M is R itself (and submodules are ideals).