CHAPTER VII

Extensions of Rings

It is not always desirable to deal only with field extensions. Sometimes one wants to obtain a field extension by reducing a ring extension modulo a prime ideal. This procedure occurs in several contexts, and so we are led to give the basic theory of Galois automorphisms over rings, looking especially at how the Galois automorphisms operate on prime ideals or the residue class fields. The two examples given after Theorem 2.9 show the importance of working over rings, to get families of extensions in two very different contexts.

Throughout this chapter, A, B, C will denote commutative rings.

§1. INTEGRAL RING EXTENSIONS

In Chapters V and VI we have studied algebraic extensions of fields. For a number of reasons, it is desirable to study algebraic extensions of rings. For instance, given a polynomial with integer coefficients, say $X^5 - X - 1$, one can reduce this polynomial mod p for any prime p, and thus get a polynomial with coefficients in a finite field. As another example, consider the polynomial

$$X^n + s_{n-1}X^{n-1} + \cdots + s_0$$

where $s_{n-1}, \ldots, s_0$ are algebraically independent over a field k. This polynomial has coefficients in $k[s_0, \ldots, s_{n-1}]$ and by substituting elements of k for $s_0, \ldots, s_{n-1}$ one obtains a polynomial with coefficients in k. One can then get

S. Lang, *Algebra*

information about polynomials by taking a homomorphism of the ring in which they have their coefficients. This chapter is devoted to a brief description of the basic facts concerning polynomials over rings.

Let M be an A-module. We say that M is **faithful** if, whenever $a \in A$ is such that $aM = 0$, then $a = 0$. We note that A is a faithful module over itself since A contains a unit element. Furthermore, if $A \neq 0$, then a faithful module over A cannot be the 0-module.

Let A be a subring of B. Let $\alpha \in B$. The following conditions are equivalent:

INT 1. The element α is a root of a polynomial

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with coefficients $a_i \in A$, and degree $n \geqq 1$. (The essential thing here is that the leading coefficient is equal to 1.)

INT 2. The subring $A[\alpha]$ is a finitely generated A-module.

INT 3. There exists a faithful module over $A[\alpha]$ which is a finitely generated A-module.

We prove the equivalence. Assume **INT 1**. Let $g(X)$ be a polynomial in $A[X]$ of degree $\geqq 1$ with leading coefficient 1 such that $g(\alpha) = 0$. If $f(X) \in A[X]$ then

$$f(X) = q(X)g(X) + r(X)$$

with $q, r \in A[X]$ and $\deg r < \deg g$. Hence $f(\alpha) = r(\alpha)$, and we see that if $\deg g = n$, then $1, \alpha, \ldots, \alpha^{n-1}$ are generators of $A[\alpha]$ as a module over A.

An equation $g(X) = 0$ with g as above, such that $g(\alpha) = 0$ is called an **integral equation** for α over A.

Assume **INT 2.** We let the module be $A[\alpha]$ itself.

Assume **INT 3**, and let M be the faithful module over $A[\alpha]$ which is finitely generated over A, say by elements $w_1, \ldots, w_n$. Since $\alpha M \subset M$ there exist elements $a_{ij} \in A$ such that

$$\begin{aligned} \alpha w_1 &= a_{11}w_1 + \cdots + a_{1n}w_n, \\ &\cdots \\ \alpha w_n &= a_{n1}w_1 + \cdots + a_{nn}w_n. \end{aligned}$$

Transposing $\alpha w_1, \ldots, \alpha w_n$ to the right-hand side of these equations, we conclude that the determinant

$$d = \begin{vmatrix} \alpha - a_{11} & & & \\ & \alpha - a_{22} & & -a_{ij} \\ & & \ddots & \\ & -a_{ij} & & \\ & & & \alpha - a_{nn} \end{vmatrix}$$

is such that $dM = 0$. (This will be proved in the chapter when we deal with determinants.) Since M is faithful, we must have $d = 0$. Hence α is a root of the polynomial

$$\det(X\delta_{ij} - a_{ij}),$$

which gives an integral equation for α over A.

An element α satisfying the three conditions **INT 1, 2, 3** is called **integral** over A.

Proposition 1.1. *Let A be an entire ring and K its quotient field. Let α be algebraic over K. Then there exists an element $c \neq 0$ in A such that $c\alpha$ is integral over A.*

Proof. There exists an equation

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$ and $a_n \neq 0$. Multiply it by a_n^{n-1}. Then

$$(a_n\alpha)^n + \cdots + a_0 a_n^{n-1} = 0$$

is an integral equation for $a_n\alpha$ over A. This proves the proposition.

Let $A \subset B$ be subrings of a commutative ring C, and let $\alpha \in C$. If α is integral over A then α is a *fortiori* integral over B. Thus integrality is preserved under lifting. In particular, α is integral over any ring which is intermediate between A and B.

Let B contain A as a subring. We shall say that B is **integral** over A if every element of B is integral over A.

Proposition 1.2. *If B is integral over A and finitely generated as an A-algebra, then B is finitely generated as an A-module.*

Proof. We may prove this by induction on the number of ring generators, and thus we may assume that $B = A[\alpha]$ for some element α integral over A, by considering a tower

$$A \subset A[\alpha_1] \subset A[\alpha_1, \alpha_2] \subset \cdots \subset A[\alpha_1, \ldots, \alpha_n] = B.$$

But we have already seen that our assertion is true in that case, this being part of the definition of integrality.

Just as we did for extension fields, one may define a class $\mathcal{C}$ of extension rings $A \subset B$ to be **distinguished** if it satisfies the analogous properties, namely:

(1) Let $A \subset B \subset C$ be a tower of rings. The extension $A \subset C$ is in $\mathcal{C}$ if and only if $A \subset B$ is in $\mathcal{C}$ and $B \subset C$ is in $\mathcal{C}$.

(2) If $A \subset B$ is in $\mathcal{C}$, if C is any extension ring of A, and if B, C are both subrings of some ring, then $C \subset B[C]$ is in $\mathcal{C}$. (We note that $B[C] = C[B]$ is the smallest ring containing both B and C.)

As with fields, we find formally as a consequence of (1) and (2) that (3) holds, namely:

(3) If $A \subset B$ and $A \subset C$ are in $\mathfrak{C}$, and B, C are subrings of some ring, then $A \subset B[C]$ is in $\mathfrak{C}$.

Proposition 1.3. *Integral ring extensions form a distinguished class.*

Proof. Let $A \subset B \subset C$ be a tower of rings. If C is integral over A, then it is clear that B is integral over A and C is integral over B. Conversely, assume that each step in the tower is integral. Let $\alpha \in C$. Then α satisfies an integral equation

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0$$

with $b_i \in B$. Let $B_1 = A[b_0, \ldots, b_{n-1}]$. Then B_1 is a finitely generated A-module by Proposition 1.2, and is obviously faithful. Then $B_1[\alpha]$ is finite over B_1, hence over A, and hence α is integral over A. Hence C is integral over A. Finally let B, C be extension rings of A and assume B integral over A. Assume that B, C are subrings of some ring. Then $C[B]$ is generated by elements of B over C, and each element of B is integral over C. That $C[B]$ is integral over C will follow immediately from our next proposition.

Proposition 1.4. *Let A be a subring of C. Then the elements of C which are integral over A form a subring of C.*

Proof. Let $\alpha, \beta \in C$ be integral over A. Let $M = A[\alpha]$ and $N = A[\beta]$. Then MN contains 1, and is therefore faithful as an A-module. Furthermore, $\alpha M \subset M$ and $\beta N \subset N$. Hence MN is mapped into itself by multiplication with $\alpha \pm \beta$ and $\alpha\beta$. Furthermore MN is finitely generated over A (if $\{w_i\}$ are generators of M and $\{v_j\}$ are generators of N then $\{w_i v_j\}$ are generators of MN). This proves our proposition.

In Proposition 1.4, the set of elements of C which are integral over A is called the **integral closure of A in C**.

Example. Consider the integers $\mathbf{Z}$. Let K be a finite extension of $\mathbf{Q}$. We call K a **number field**. The integral closure of $\mathbf{Z}$ in K is called the ring of **algebraic integers** of K. This is the most classical example.

In algebraic geometry, one considers a finitely generated entire ring R over $\mathbf{Z}$ or over a field k. Let F be the quotient field of R. One then considers the integral closure of R in F, which is proved to be finite over R. If K is a finite extension of F, one also considers the integral closure of R in K.

Proposition 1.5. *Let $A \subset B$ be an extension ring, and let B be integral over A. Let σ be a homomorphism of B. Then $\sigma(B)$ is integral over $\sigma(A)$.*

Proof. Let $\alpha \in B$, and let

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

be an integral equation for α over A. Applying σ yields

$$\sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(a_0) = 0,$$

thereby proving our assertion.

Corollary 1.6. *Let A be an entire ring, k its quotient field, and E a finite extension of k. Let $\alpha \in E$ be integral over A. Then the norm and trace of α (from E to k) are integral over A, and so are the coefficients of the irreducible polynomial satisfied by α over k.*

Proof. For each embedding σ of E over k, $\sigma\alpha$ is integral over A. Since the norm is the product of $\sigma\alpha$ over all such σ (raised to a power of the characteristic), it follows that the norm is integral over A. Similarly for the trace, and similarly for the coefficients of $\mathrm{Irr}(\alpha, k, X)$, which are elementary symmetric functions of the roots.

Let A be an entire ring and k its quotient field. We say that A is **integrally closed** if it is equal to its integral closure in k.

Proposition 1.7. *Let A be entire and factorial. Then A is integrally closed.*

Proof. Suppose that there exists a quotient a/b with $a, b \in A$ which is integral over A, and a prime element p in A which divides b but not a. We have, for some integer $n \geqq 1$, and $a_i \in A$,

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0$$

whence

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0 b^n = 0.$$

Since p divides b, it must divide a^n, and hence must divide a, contradiction.

Let $f: A \to B$ be a ring-homomorphism (A, B being commutative rings). We recall that such a homomorphism is also called an ***A*-algebra**. We may view B as an A-module. We say that B is integral over A (for this ring-homomorphism f) if B is integral over $f(A)$. This extension of our definition of integrality is useful because there are applications when certain collapsings take place, and we still wish to speak of integrality. Strictly speaking we should not say that B is integral over A, but that f **is an integral ring-homomorphism**, or simply that f is **integral**. We shall use this terminology frequently.

Some of our preceding propositions have immediate consequences for integral ring-homomorphisms; for instance, if $f: A \to B$ and $g: B \to C$ are integral, then $g \circ f: A \to C$ is integral. However, it is not necessarily true that if $g \circ f$ is integral, so is f.

Let $f: A \to B$ be integral, and let S be a multiplicative subset of A. Then we get a homomorphism

$$S^{-1}f: S^{-1}A \to S^{-1}B,$$

where strictly speaking, $S^{-1}B = (f(S))^{-1}B$, and $S^{-1}f$ is defined by

$$(S^{-1}f)(x/s) = f(x)/f(s).$$

It is trivially verified that this is a homomorphism. We have a commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & S^{-1}B \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle S^{-1}f} \\ A & \longrightarrow & S^{-1}A \end{array}$$

the horizontal maps being the canonical ones: $x \to x/1$.

Proposition 1.8. *Let $f: A \to B$ be integral, and let S be a multiplicative subset of A. Then $S^{-1}f: S^{-1}A \to S^{-1}B$ is integral.*

Proof. If $\alpha \in B$ is integral over $f(A)$, then writing $\alpha\beta$ instead of $f(a)\beta$ for $a \in A$ and $\beta \in B$ we have

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$. Taking the canonical image in $S^{-1}A$ and $S^{-1}B$ respectively, we see that this relation proves the integrality of $\alpha/1$ over $S^{-1}A$, the coefficients being now $a_i/1$.

Proposition 1.9. *Let A be entire and integrally closed. Let S be a multiplicative subset of A, $0 \notin S$. Then $S^{-1}A$ is integrally closed.*

Proof. Let α be an element of the quotient field, integral over $S^{-1}A$. We have an equation

$$\alpha^n + \frac{a_{n-1}}{s_{n-1}}\alpha^{n-1} + \cdots + \frac{a_0}{s_0} = 0,$$

$a_i \in A$ and $s_i \in S$. Let s be the product $s_{n-1} \cdots s_0$. Then it is clear that $s\alpha$ is integral over A, whence in A. Hence α lies in $S^{-1}A$, and $S^{-1}A$ is integrally closed.

Let $\mathfrak{p}$ be a prime ideal of a ring A and let S be the complement of $\mathfrak{p}$ in A. We write $S = A - \mathfrak{p}$. If $f: A \to B$ is an A-algebra (i.e. a ring-homomorphism), we shall write $B_{\mathfrak{p}}$ instead of $S^{-1}B$. We can view $B_{\mathfrak{p}}$ as an $A_{\mathfrak{p}} = S^{-1}A$-module.

Let A be a subring of B. Let $\mathfrak{p}$ be a prime ideal of A and let $\mathfrak{P}$ be a prime ideal of B. We say that $\mathfrak{P}$ **lies above** $\mathfrak{p}$ if $\mathfrak{P} \cap A = \mathfrak{p}$. If that is the case, then the injection $A \to B$ induces an injection of the factor rings

$$A/\mathfrak{p} \to B/\mathfrak{P},$$

and in fact we have a commutative diagram:

$$\begin{array}{ccc} B & \longrightarrow & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A/\mathfrak{p} \end{array}$$

the horizontal arrows being the canonical homomorphisms, and the vertical arrows being injections.

If B is integral over A, then $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$ by Proposition 1.5.

Proposition 1.10. *Let A be a subring of B, let $\mathfrak{p}$ be a prime ideal of A, and assume B integral over A. Then $\mathfrak{p}B \neq B$ and there exists a prime ideal $\mathfrak{P}$ of B lying above $\mathfrak{p}$.*

Proof. We know that $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$ and that $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{m}_{\mathfrak{p}} = S^{-1}\mathfrak{p}$, where $S = A - \mathfrak{p}$. Since we obviously have

$$\mathfrak{p}B_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}B_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}},$$

it will suffice to prove our first assertion when A is a local ring. (Note that the existence of a prime ideal $\mathfrak{p}$ implies that $1 \neq 0$, and $\mathfrak{p}B = B$ if and only if $1 \in \mathfrak{p}B$.) In that case, if $\mathfrak{p}B = B$, then 1 has an expression as a finite linear combination of elements of B with coefficients in $\mathfrak{p}$,

$$1 = a_1b_1 + \cdots + a_nb_n$$

with $a_i \in \mathfrak{p}$ and $b_i \in B$. We shall now use notation as if $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$. We leave it to the reader as an exercise to verify that our arguments are valid when we deal only with a canonical homomorphism $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$. Let $B_0 = A[b_1, \ldots, b_n]$. Then $\mathfrak{p}B_0 = B_0$ and B_0 is a finite A-module by Proposition 1.2. Hence $B_0 = 0$ by Nakayama's lemma, contradiction. (See Lemma 4.1 of Chapter X.)

To prove our second assertion, note the following commutative diagram:

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array}$$

We have just proved $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$. Hence $\mathfrak{m}_{\mathfrak{p}}B_{\mathfrak{p}}$ is contained in a maximal ideal $\mathfrak{M}$ of $B_{\mathfrak{p}}$. Taking inverse images, we see that the inverse image of $\mathfrak{M}$ in $A_{\mathfrak{p}}$ is an ideal containing $\mathfrak{m}_{\mathfrak{p}}$ (in the case of an inclusion $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ the inverse image is $\mathfrak{M} \cap A_{\mathfrak{p}}$). Since $\mathfrak{m}_{\mathfrak{p}}$ is maximal, we have $\mathfrak{M} \cap A_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$. Let $\mathfrak{P}$ be the inverse image of $\mathfrak{M}$ in B (in the case of inclusion, $\mathfrak{P} = \mathfrak{M} \cap B$). Then $\mathfrak{P}$ is a prime ideal of B. The inverse image of $\mathfrak{m}_{\mathfrak{p}}$ in A is simply $\mathfrak{p}$. Taking the inverse image of $\mathfrak{M}$ going around both ways in the diagram, we find that

$$\mathfrak{P} \cap A = \mathfrak{p},$$

as was to be shown.

Proposition 1.11. *Let A be a subring of B, and assume that B is integral over A. Let $\mathfrak{P}$ be a prime ideal of B lying over a prime ideal $\mathfrak{p}$ of A. Then $\mathfrak{P}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. Assume $\mathfrak{p}$ maximal in A. Then $A/\mathfrak{p}$ is a field, and $B/\mathfrak{P}$ is an entire ring, integral over $A/\mathfrak{p}$. If $\alpha \in B/\mathfrak{P}$, then α is algebraic over $A/\mathfrak{p}$, and we know that $A/\mathfrak{p}[\alpha]$ is a field. Hence every non-zero element of $B/\mathfrak{P}$ is invertible in $B/\mathfrak{P}$, which is therefore a field. Conversely, assume that $\mathfrak{P}$ is maximal in B. Then $B/\mathfrak{P}$ is a field, which is integral over the entire ring $A/\mathfrak{p}$. If $A/\mathfrak{p}$ is not a field, it has a non-zero maximal ideal $\mathfrak{m}$. By Proposition 1.10, there exists a prime ideal $\mathfrak{M}$ of $B/\mathfrak{P}$ lying above $\mathfrak{m}$, $\mathfrak{M} \neq 0$, contradiction.

§2. INTEGRAL GALOIS EXTENSIONS

We shall now investigate the relationship between the Galois theory of a polynomial, and the Galois theory of this same polynomial reduced modulo a prime ideal.

Proposition 2.1. *Let A be an entire ring, integrally closed in its quotient field K. Let L be a finite Galois extension of K with group G. Let $\mathfrak{p}$ be a maximal ideal of A, and let $\mathfrak{P}$, $\mathfrak{Q}$ be prime ideals of the integral closure B of A in L lying above $\mathfrak{p}$. Then there exists $\sigma \in G$ such that $\sigma\mathfrak{P} = \mathfrak{Q}$.*

Proof. Suppose that $\mathfrak{Q} \neq \sigma\mathfrak{P}$ for any $\sigma \in G$. Then $\tau\mathfrak{Q} \neq \sigma\mathfrak{P}$ for any pair of elements $\sigma, \tau \in G$. There exists an element $x \in B$ such that

$$x \equiv 0 \pmod{\sigma\mathfrak{P}}, \qquad \text{all } \sigma \in G$$

$$x \equiv 1 \pmod{\sigma\mathfrak{Q}}, \qquad \text{all } \sigma \in G$$

(use the Chinese remainder theorem). The norm

$$N_K^L(x) = \prod_{\sigma \in G} \sigma x$$

lies in $B \cap K = A$ (because A is integrally closed), and lies in $\mathfrak{P} \cap A = \mathfrak{p}$. But $x \notin \sigma\mathfrak{Q}$ for all $\sigma \in G$, so that $\sigma x \notin \mathfrak{Q}$ for all $\sigma \in G$. This contradicts the fact that the norm of x lies in $\mathfrak{p} = \mathfrak{Q} \cap A$.

If one localizes, one can eliminate the hypothesis that $\mathfrak{p}$ is maximal; just assume that $\mathfrak{p}$ is prime.

Corollary 2.2 *Let A be integrally closed in its quotient field K. Let E be a finite separable extension of K, and B the integral closure of A in E. Let $\mathfrak{p}$ be a maximal ideal of A. Then there exists only a finite number of prime ideals of B lying above $\mathfrak{p}$.*

Proof. Let L be the smallest Galois extension of K containing E. If $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ are two distinct prime ideals of B lying above $\mathfrak{p}$, and $\mathfrak{P}_1$, $\mathfrak{P}_2$ are two prime ideals of the integral closure of A in L lying above $\mathfrak{Q}_1$ and $\mathfrak{Q}_2$ respectively, then $\mathfrak{P}_1 \neq \mathfrak{P}_2$. This argument reduces our assertion to the case that E is Galois over K, and it then becomes an immediate consequence of the proposition.

Let A be integrally closed in its quotient field K, and let B be its integral closure in a finite Galois extension L, with group G. Then $\sigma B = B$ for every $\sigma \in G$. Let $\mathfrak{p}$ be a maximal ideal of A, and $\mathfrak{P}$ a maximal ideal of B lying above $\mathfrak{p}$. We denote by $G_{\mathfrak{P}}$ the subgroup of G consisting of those automorphisms such that $\sigma\mathfrak{P} = \mathfrak{P}$. Then $G_{\mathfrak{P}}$ operates in a natural way on the residue class field $B/\mathfrak{P}$, and leaves $A/\mathfrak{p}$ fixed. To each $\sigma \in G_{\mathfrak{P}}$ we can associate an automorphism $\bar{\sigma}$ of $B/\mathfrak{P}$ over $A/\mathfrak{p}$, and the map given by

$$\sigma \mapsto \bar{\sigma}$$

induces a homomorphism of $G_{\mathfrak{P}}$ into the group of automorphisms of $B/\mathfrak{P}$ over $A/\mathfrak{p}$.

The group $G_{\mathfrak{P}}$ will be called the **decomposition group** of $\mathfrak{P}$. Its fixed field will be denoted by L^{dec}, and will be called the **decomposition field** of $\mathfrak{P}$. Let B^{dec} be the integral closure of A in L^{dec}, and $\mathfrak{Q} = \mathfrak{P} \cap B^{\mathrm{dec}}$. By Proposition 2.1, we know that $\mathfrak{P}$ is the only prime of B lying above $\mathfrak{Q}$.

Let $G = \bigcup \sigma_j G_{\mathfrak{P}}$ be a coset decomposition of $G_{\mathfrak{P}}$ in G. Then the prime ideals $\sigma_j\mathfrak{P}$ are precisely the distinct primes of B lying above $\mathfrak{p}$. Indeed, for two elements $\sigma, \tau \in G$ we have $\sigma\mathfrak{P} = \tau\mathfrak{P}$ if and only if $\tau^{-1}\sigma\mathfrak{P} = \mathfrak{P}$, i.e. $\tau^{-1}\sigma$ lies in $G_{\mathfrak{P}}$. Thus τ, σ lie in the same coset mod $G_{\mathfrak{P}}$.

It is then immediately clear that the decomposition group of a prime $\sigma\mathfrak{P}$ is $\sigma G_{\mathfrak{P}} \sigma^{-1}$.

Proposition 2.3. *The field L^{dec} is the smallest subfield E of L containing K such that $\mathfrak{P}$ is the only prime of B lying above $\mathfrak{P} \cap E$ (which is prime in $B \cap E$).*

Proof. Let E be as above, and let H be the Galois group of L over E. Let $\mathfrak{q} = \mathfrak{P} \cap E$. By Proposition 2.1, all primes of B lying above $\mathfrak{q}$ are conjugate by elements of H. Since there is only one prime, namely $\mathfrak{P}$, it means that H leaves $\mathfrak{P}$ invariant. Hence $G \subset G_{\mathfrak{P}}$ and $E \supset L^{\mathrm{dec}}$. We have already observed that L^{dec} has the required property.

Proposition 2.4. *Notation being as above, we have $A/\mathfrak{p} = B^{\mathrm{dec}}/\mathfrak{Q}$ (under the canonical injection $A/\mathfrak{p} \to B^{\mathrm{dec}}/\mathfrak{Q}$).*

Proof. If σ is an element of G, not in $G_{\mathfrak{P}}$, then $\sigma\mathfrak{P} \neq \mathfrak{P}$ and $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$. Let

$$\mathfrak{Q}_\sigma = \sigma^{-1}\mathfrak{P} \cap B^{\mathrm{dec}}.$$

Then $\mathfrak{Q}_\sigma \neq \mathfrak{Q}$. Let x be an element of B^{dec}. There exists an element y of B^{dec} such that

$$y \equiv x \pmod{\mathfrak{Q}}$$

$$y \equiv 1 \pmod{\mathfrak{Q}_\sigma}$$

for each σ in G, but not in $G_{\mathfrak{P}}$. Hence in particular,

$$y \equiv x \pmod{\mathfrak{P}}$$
$$y \equiv 1 \pmod{\sigma^{-1}\mathfrak{P}}$$

for each σ not in $G_{\mathfrak{P}}$. This second congruence yields

$$\sigma y \equiv 1 \pmod{\mathfrak{P}}$$

for all $\sigma \notin G_{\mathfrak{P}}$. The norm of y from L^{dec} to K is a product of y and other factors σy with $\sigma \notin G_{\mathfrak{P}}$. Thus we obtain

$$N_K^{L^{\mathrm{dec}}}(y) \equiv x \pmod{\mathfrak{P}}.$$

But the norm lies in K, and even in A, since it is a product of elements integral over A. This last congruence holds mod $\mathfrak{Q}$, since both x and the norm lie in B^{dec}. This is precisely the meaning of the assertion in our proposition.

If x is an element of B, we shall denote by $\bar{x}$ its image under the homomorphism $B \to B/\mathfrak{P}$. Then $\bar{\sigma}$ is the automorphism of $B/\mathfrak{P}$ satisfying the relation

$$\bar{\sigma}\bar{x} = (\overline{\sigma x}).$$

If $f(X)$ is a polynomial with coefficients in B, we denote by $\bar{f}(X)$ its natural image under the above homomorphism. Thus, if

$$f(X) = b_n X^n + \cdots + b_0,$$

then

$$\bar{f}(X) = \bar{b}_n X^n + \cdots + \bar{b}_0.$$

Proposition 2.5. *Let A be integrally closed in its quotient field K, and let B be its integral closure in a finite Galois extension L of K, with group G. Let $\mathfrak{p}$ be a maximal ideal of A, and $\mathfrak{P}$ a maximal ideal of B lying above $\mathfrak{p}$. Then $B/\mathfrak{P}$ is a normal extension of $A/\mathfrak{p}$, and the map $\sigma \mapsto \bar{\sigma}$ induces a homomorphism of $G_{\mathfrak{P}}$ onto the Galois group of $B/\mathfrak{P}$ over $A/\mathfrak{p}$.*

Proof. Let $\bar{B} = B/\mathfrak{P}$ and $\bar{A} = A/\mathfrak{p}$. Any element of $\bar{B}$ can be written as $\bar{x}$ for some $x \in B$. Let $\bar{x}$ generate a separable subextension of $\bar{B}$ over $\bar{A}$, and let f be the irreducible polynomial for x over K. The coefficients of f lie in A because x is integral over A, and all the roots of f are integral over A. Thus

$$f(X) = \prod_{i=1}^{m} (X - x_i)$$

splits into linear factors in B. Since

$$\bar{f}(X) = \sum_{i=1}^{m} (X - \bar{x}_i)$$

and all the $\bar{x}_i$ lie in $\bar{B}$, it follows that $\bar{f}$ splits into linear factors in $\bar{B}$. We observe that $f(x) = 0$ implies $\bar{f}(\bar{x}) = 0$. Hence $\bar{B}$ is normal over $\bar{A}$, and

$$[\bar{A}(\bar{x}) : \bar{A}] \leqq [K(x) : K] \leqq [L : K].$$

This implies that the maximal separable subextension of $\bar{A}$ in $\bar{B}$ is of finite degree over $\bar{A}$ (using the primitive element theorem of elementary field theory). This degree is in fact bounded by $[L : K]$.

There remains to prove that the map $\sigma \mapsto \bar{\sigma}$ gives a surjective homomorphism of $G_{\mathfrak{P}}$ onto the Galois group of $\bar{B}$ over $\bar{A}$. To do this, we shall give an argument which reduces our problem to the case when $\mathfrak{P}$ is the only prime ideal of B lying above $\mathfrak{p}$. Indeed, by Proposition 2.4, the residue class fields of the ground ring and the ring B^{dec} in the decomposition field are the same. This means that to prove our surjectivity, we may take L^{dec} as ground field. This is the desired reduction, and we can assume $K = L^{\mathrm{dec}}$, $G = G_{\mathfrak{P}}$.

This being the case, take a generator of the maximal separable subextension of $\bar{B}$ over $\bar{A}$, and let it be $\bar{x}$, for some element x in B. Let f be the irreducible polynomial of x over K. Any automorphism of $\bar{B}$ is determined by its effect on $\bar{x}$, and maps $\bar{x}$ on some root of $\bar{f}$. Suppose that $x = x_1$. Given any root x_i of f, there exists an element σ of $G = G_{\mathfrak{P}}$ such that $\sigma x = x_i$. Hence $\bar{\sigma}\bar{x} = \bar{x}_i$. Hence the automorphisms of $\bar{B}$ over $\bar{A}$ induced by elements of G operate transitively on the roots of $\bar{f}$. Hence they give us all automorphisms of the residue class field, as was to be shown.

Corollary 2.6. *Let A be integrally closed in its quotient field K. Let L be a finite Galois extension of K, and B the integral closure of A in L. Let $\mathfrak{p}$ be a maximal ideal of A. Let $\varphi : A \to A/\mathfrak{p}$ be the canonical homomorphism, and let ψ_1, ψ_2 be two homomorphisms of B extending φ in a given algebraic closure of $A/\mathfrak{p}$. Then there exists an automorphism σ of L over K such that*

$$\psi_1 = \psi_2 \circ \sigma.$$

Proof. The kernels of ψ_1, ψ_2 are prime ideals of B which are conjugate by Proposition 2.1. Hence there exists an element τ of the Galois group G such that ψ_1, $\psi_2 \circ \tau$ have the same kernel. Without loss of generality, we may therefore assume that ψ_1, ψ_2 have the same kernel $\mathfrak{P}$. Hence there exists an automorphism ω of $\psi_1(B)$ onto $\psi_2(B)$ such that $\omega \circ \psi_1 = \psi_2$. There exists an element σ of $G_{\mathfrak{P}}$ such that $\omega \circ \psi_1 = \psi_1 \circ \sigma$, by the preceding proposition. This proves what we wanted.

Remark. In all the above propositions, we could assume $\mathfrak{p}$ prime instead of maximal. In that case, one has to localize at $\mathfrak{p}$ to be able to apply our proofs.

In the above discussions, the kernel of the map

$$G_{\mathfrak{P}} \to \bar{G}_{\mathfrak{P}}$$

is called the **inertia group** of $\mathfrak{P}$. It consists of those automorphisms of $G_{\mathfrak{P}}$ which induce the trivial automorphism on the residue class field. Its fixed field is called the **inertia field**, and is denoted by L^{in}.

Corollary 2.7. *Let the assumptions be as in Corollary* 2.6 *and assume that $\mathfrak{P}$ is the only prime of B lying above $\mathfrak{p}$. Let $f(X)$ be a polynomial in $A[X]$ with leading coefficient* 1. *Assume that f is irreducible in $K[X]$, and has a root α in B. Then the reduced polynomial $\bar{f}$ is a power of an irreducible polynomial in $\bar{A}[X]$.*

Proof. By Corollary 2.6, we know that any two roots of $\bar{f}$ are conjugate under some isomorphism of $\bar{B}$ over $\bar{A}$, and hence that $\bar{f}$ cannot split into relative prime polynomials. Therefore, $\bar{f}$ is a power of an irreducible polynomial.

Proposition 2.8. *Let A be an entire ring, integrally closed in its quotient field K. Let L be a finite Galois extension of K. Let $L = K(\alpha)$, where α is integral over A, and let*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

be the irreducible polynomial of α over k, with $a_i \in A$. Let $\mathfrak{p}$ be a maximal ideal in A, let $\mathfrak{P}$ be a prime ideal of the integral closure B of A in L, $\mathfrak{P}$ lying above $\mathfrak{p}$. Let $\bar{f}(X)$ be the reduced polynomial with coefficients in $A/\mathfrak{p}$. Let $G_{\mathfrak{P}}$ be the decomposition group. If $\bar{f}$ has no multiple roots, then the map $\sigma \mapsto \bar{\sigma}$ has trivial kernel, and is an isomorphism of $G_{\mathfrak{P}}$ on the Galois group of $\bar{f}$ over $A/\mathfrak{p}$.

Proof. Let

$$f(X) = \prod (X - x_i)$$

be the factorization of f in L. We know that all $x_i \in B$. If $\sigma \in G_{\mathfrak{P}}$, then we denote by $\bar{\sigma}$ the homomorphic image of σ in the group $\bar{G}_{\mathfrak{P}}$, as before. We have

$$\bar{f}(X) = \prod (X - \bar{x}_i).$$

Suppose that $\bar{\sigma}\bar{x}_i = \bar{x}_i$ for all i. Since $(\overline{\sigma x_i}) = \bar{\sigma}\bar{x}_i$, and since $\bar{f}$ has no multiple roots, it follows that σ is also the identity. Hence our map is injective, the inertia group is trivial. The field $\bar{A}[\bar{x}_1, \ldots, \bar{x}_n]$ is a subfield of $\bar{B}$ and any auto-

morphism of $\bar{B}$ over $\bar{A}$ which restricts to the identity on this subfield must be the identity, because the map $G_{\mathfrak{P}} \to \bar{G}_{\mathfrak{P}}$ is onto the Galois group of $\bar{B}$ over $\bar{A}$. Hence $\bar{B}$ is purely inseparable over $\bar{A}[\bar{x}_1, \ldots, \bar{x}_n]$ and therefore $G_{\mathfrak{P}}$ is isomorphic to the Galois group of $\bar{f}$ over $\bar{A}$.

Proposition 2.8 is only a special case of the more-general situation when the root of a polynomial does not necessarily generate a Galois extension. We state a version useful to compute Galois groups.

Theorem 2.9. *Let A be an entire ring, integrally closed in its quotient field K. Let $f(X) \in A[X]$ have leading coefficient 1 and be irreducible over K (or A, it's the same thing). Let $\mathfrak{p}$ be a maximal ideal of A and let $\bar{f} = f \bmod \mathfrak{p}$. Suppose that $\bar{f}$ has no multiple roots in an algebraic closure of $A/\mathfrak{p}$. Let L be a splitting field for f over K, and let B be the integral closure of A in L. Let $\mathfrak{P}$ be any prime of B above $\mathfrak{p}$ and let a bar denote reduction mod $\mathfrak{p}$. Then the map*

$$G_{\mathfrak{P}} \to \bar{G}_{\mathfrak{P}}$$

is an isomorphism of $G_{\mathfrak{P}}$ with the Galois group of $\bar{f}$ over $\bar{A}$.

Proof. Let $(\alpha_1, \ldots, \alpha_n)$ be the roots of f in B and let $(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ be their reductions mod $\mathfrak{P}$. Since

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i),$$

it follows that

$$\bar{f}(X) = \prod_{i=1}^{n} (X - \bar{\alpha}_i).$$

Any element of G is determined by its effect as a permutation of the roots, and for $\sigma \in G_{\mathfrak{P}}$, we have

$$\bar{\sigma}\, \bar{\alpha}_i = \overline{\sigma\alpha}_i.$$

Hence if $\bar{\sigma} = \mathrm{id}$ then $\sigma = \mathrm{id}$, so the map $G_{\mathfrak{P}} \to \bar{G}_{\mathfrak{P}}$ is injective. It is surjective by Proposition 2.5, so the theorem is proved.

This theorem justifies the statement used to compute Galois groups in Chapter VI, §2.

Theorem 2.9 gives a very efficient tool for analyzing polynomials over a ring.

Example. Consider the "generic" polynomial

$$f_w(X) = X^n + w_{n-1}X^{n-1} + \cdots + w_0$$

where $w_0, \ldots, w_{n-1}$ are algebraically independent over a field k. We know that the Galois group of this polynomial over the field $K = k(w_0, \ldots, w_{n-1})$ is the symmetric group. Let $t_1, \ldots, t_n$ be the roots. Let α be a generator of the splitting field L; that is, $L = K(\alpha)$. Without loss of generality, we can select α to be integral over the ring $k[w_0, \ldots, w_{n-1}]$(multiply any given generator by a suitably chosen polynomial and use Proposition 1.1). Let $g_w(X)$ be the irreducible polynomial of α over $k(w_0, \ldots, w_{n-1})$. The coefficients of g are polynomials in (w). If we can substitute values (a) for (w) with $a_0, \ldots, a_{n-1} \in k$ such that g_a remains irreducible, then by Proposition 2.8 we conclude at once that the Galois group of g_a is the symmetric group also. Similarly, if a finite Galois extension of $k(w_0, \ldots, w_{n-1})$ has Galois group G, then we can do a similar substitution to get a Galois extension of k having Galois group G, provided the special polynomial g_a remains irreducible.

Example. Let K be a number field; that is, a finite extension of $\mathbf{Q}$. Let $\mathfrak{o}$ be the ring of algebraic integers. Let L be a finite Galois extension of K and $\mathfrak{O}$ the algebraic integers in L. Let $\mathfrak{p}$ be a prime of $\mathfrak{o}$ and $\mathfrak{P}$ a prime of $\mathfrak{O}$ lying above $\mathfrak{p}$. Then $\mathfrak{o}/\mathfrak{p}$ is a finite field, say with q elements. Then $\mathfrak{O}/\mathfrak{P}$ is a finite extension of $\mathfrak{o}/\mathfrak{p}$, and by the theory of finite fields, there is a unique element in $\overline{G}_{\mathfrak{P}}$, called the **Frobenius element** $\overline{\mathrm{Fr}}_{\mathfrak{P}}$, such that $\overline{\mathrm{Fr}}_{\mathfrak{P}}(\bar{x}) = \bar{x}^q$ for $\bar{x} \in \mathfrak{O}/\mathfrak{P}$. The conditions of Theorem 2.9 are satisfied for all but a finite number of primes $\mathfrak{p}$, and for such primes, there is a unique element $\mathrm{Fr}_{\mathfrak{P}} \in G_{\mathfrak{P}}$ such that $\mathrm{Fr}_{\mathfrak{P}}(x) \equiv x^q \bmod \mathfrak{P}$ for all $x \in \mathfrak{O}$. We call $\mathrm{Fr}_{\mathfrak{P}}$ the **Frobenius element** in $G_{\mathfrak{P}}$. Cf. Chapter VI, §15, where some of the significance of the Frobenius element is explained.

§3. EXTENSION OF HOMOMORPHISMS

When we first discussed the process of localization, we considered very briefly the extension of a homomorphism to a local ring. In our discussion of field theory, we also described an extension theorem for embeddings of one field into another. We shall now treat the extension question in full generality.

First we recall the case of a local ring. Let A be a commutative ring and $\mathfrak{p}$ a prime ideal. We know that the local ring $A_{\mathfrak{p}}$ is the set of all fractions x/y, with $x, y \in A$ and $y \notin \mathfrak{p}$. Its maximal ideal consists of those fractions with $x \in \mathfrak{p}$. Let L be a field and let $\varphi\colon A \to L$ be a homomorphism whose kernel is $\mathfrak{p}$. Then we can extend φ to a homomorphism of $A_{\mathfrak{p}}$ into L by letting

$$\varphi(x/y) = \varphi(x)/\varphi(y)$$

if x/y is an element of $A_{\mathfrak{p}}$ as above.

Second, we have integral ring extensions. Let $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$, let B be integral over $\mathfrak{o}$, and let $\varphi : \mathfrak{o} \to L$ be a homomorphism of $\mathfrak{o}$

into an algebraically closed field L. We assume that the kernel of φ is $\mathfrak{m}$. By Proposition 1.10, we know that there exists a maximal ideal $\mathfrak{M}$ of B lying above $\mathfrak{m}$, i.e. such that $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. Then $B/\mathfrak{M}$ is a field, which is an algebraic extension of $\mathfrak{o}/\mathfrak{m}$, and $\mathfrak{o}/\mathfrak{m}$ is isomorphic to the subfield $\varphi(\mathfrak{o})$ of L because the kernel of φ is $\mathfrak{m}$.

We can find an isomorphism of $\mathfrak{o}/\mathfrak{m}$ onto $\varphi(\mathfrak{o})$ such that the composite homomorphism

$$\mathfrak{o} \to \mathfrak{o}/\mathfrak{m} \to L$$

is equal to φ. We now embed $B/\mathfrak{M}$ into L so as to make the following diagram commutative:

$$\begin{array}{ccccc} B & \longrightarrow & B/\mathfrak{M} & & \\ \uparrow & & \uparrow & \searrow & \\ \mathfrak{o} & \longrightarrow & \mathfrak{o}/\mathfrak{m} & \longrightarrow & L \end{array}$$

and in this way get a homomorphism of B into L which extends φ.

Proposition 3.1. *Let A be a subring of B and assume that B is integral over A. Let $\varphi : A \to L$ be a homomorphism into a field L which is algebraically closed. Then φ has an extension to a homomorphism of B into L.*

Proof. Let $\mathfrak{p}$ be the kernel of φ and let S be the complement of $\mathfrak{p}$ in A. Then we have a commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & S^{-1}B \\ \uparrow & & \uparrow \\ A & \longrightarrow & S^{-1}A = A_{\mathfrak{p}} \end{array}$$

and φ can be factored through the canonical homomorphism of A into $S^{-1}A$. Furthermore, $S^{-1}B$ is integral over $S^{-1}A$. This reduces the question to the case when we deal with a local ring, which has just been discussed above.

Theorem 3.2. *Let A be a subring of a field K and let $x \in K$, $x \neq 0$. Let $\varphi : A \to L$ be a homomorphism of A into an algebraically closed field L. Then φ has an extension to a homomorphism of $A[x]$ or $A[x^{-1}]$ into L.*

Proof. We may first extend φ to a homomorphism of the local ring $A_{\mathfrak{p}}$, where $\mathfrak{p}$ is the kernel of φ. Thus without loss of generality, we may assume that A is a local ring with maximal ideal $\mathfrak{m}$. Suppose that

$$\mathfrak{m}A[x^{-1}] = A[x^{-1}].$$

Then we can write

$$1 = a_0 + a_1x^{-1} + \cdots + a_nx^{-n}$$

with $a_i \in \mathfrak{m}$. Multiplying by x^n we obtain

$$(1 - a_0)x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$$

with suitable elements $b_i \in A$. Since $a_0 \in \mathfrak{m}$, it follows that $1 - a_0 \notin \mathfrak{m}$ and hence $1 - a_0$ is a unit in A because A is assumed to be a local ring. Dividing by $1 - a_0$ we see that x is integral over A, and hence that our homomorphism has an extension to $A[x]$ by Proposition 3.1.

If on the other hand we have

$$\mathfrak{m}A[x^{-1}] \neq A[x^{-1}]$$

then $\mathfrak{m}A[x^{-1}]$ is contained in some maximal ideal $\mathfrak{P}$ of $A[x^{-1}]$ and $\mathfrak{P} \cap A$ contains $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, we must have $\mathfrak{P} \cap A = \mathfrak{m}$. Since φ and the canonical map $A \to A/\mathfrak{m}$ have the same kernel, namely $\mathfrak{m}$, we can find an embedding ψ of $A/\mathfrak{m}$ into L such that the composite map

$$A \to A/\mathfrak{m} \xrightarrow{\psi} L$$

is equal to φ. We note that $A/\mathfrak{m}$ is canonically embedded in $B/\mathfrak{P}$ where $B = A[x^{-1}]$, and extend ψ to a homomorphism of $B/\mathfrak{P}$ into L, which we can do whether the image of x^{-1} in $B/\mathfrak{P}$ is transcendental or algebraic over $A/\mathfrak{m}$. The composite $B \to B/\mathfrak{P} \to L$ gives us what we want.

Corollary 3.3. *Let A be a subring of a field K and let L be an algebraically closed field. Let $\varphi : A \to L$ be a homomorphism. Let B be a maximal subring of K to which φ has an extension homomorphism into L. Then B is a local ring and if $x \in K$, $x \neq 0$, then $x \in B$ or $x^{-1} \in B$.*

Proof. Let S be the set of pairs (C, ψ) where C is a subring of K and $\psi : C \to L$ is a homomorphism extending φ. Then S is not empty (containing (A, φ)], and is partially ordered by ascending inclusion and restriction. In other words, $(C, \psi) \leqq (C', \psi')$ if $C \subset C'$ and the restriction of ψ' to C is equal to ψ. It is clear that S is inductively ordered, and by Zorn's lemma there exists a maximal element, say (B, ψ_0). Then first B is a local ring, otherwise ψ_0 extends to the local ring arising from the kernel, and second, B has the desired property according to Theorem 3.2.

Let B be a subring of a field K having the property that given $x \in K$, $x \neq 0$, then $x \in B$ or $x^{-1} \in B$. Then we call B a **valuation ring** in K. We shall study such rings in greater detail in Chapter XII. However, we shall also give some applications in the next chapter, so we make some more comments here.

Let F be a field. We let the symbol ∞ satisfy the usual algebraic rules. If $a \in F$, we define

$$a \pm \infty = \infty, \qquad a \cdot \infty = \infty \quad \text{if} \quad a \neq 0,$$

$$\infty \cdot \infty = \infty, \qquad \frac{1}{0} = \infty \quad \text{and} \quad \frac{1}{\infty} = 0.$$

The expressions $\infty \pm \infty$, $0 \cdot \infty$, $0/0$, and ∞/∞ are not defined.

A **place** φ of a field K into a field F is a mapping

$$\varphi : K \to \{F, \infty\}$$

of K into the set consisting of F and ∞ satisfying the usual rules for a homomorphism, namely

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

whenever the expressions on the right-hand side of these formulas are defined, and such that $\varphi(1) = 1$. We shall also say that the place is ***F*-valued**. The elements of K which are not mapped into ∞ will be called **finite** under the place, and the others will be called **infinite**.

The reader will verify at once that the set $\mathfrak{o}$ of elements of K which are finite under a place is a valuation ring of K. The maximal ideal consists of those elements x such that $\varphi(x) = 0$. Conversely, if $\mathfrak{o}$ is a valuation ring of K with maximal ideal $\mathfrak{m}$, we let $\varphi : \mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ be the canonical homomorphism, and define $\varphi(x) = \infty$ for $x \in K$, $x \notin \mathfrak{o}$. Then it is trivially verified that φ is a place.

If $\varphi_1 : K \to \{F_1, \infty\}$ and $\varphi_2 : K \to \{F_2, \infty\}$ are places of K, we take their restrictions to their images. We may therefore assume that they are surjective. We shall say that they are **equivalent** if there exists an isomorphism $\lambda : F_1 \to F_2$ such that $\varphi_2 = \varphi_1 \circ \lambda$. (We put $\lambda(\infty) = \infty$.) One sees that two places are equivalent if and only if they have the same valuation ring. It is clear that there is a bijection between equivalence classes of places of K, and valuation rings of K. A place is called trivial if it is injective. The valuation ring of the trivial place is simply K itself.

As with homomorphisms, we observe that the composite of two places is also a place (trivial verification).

It is often convenient to deal with places instead of valuation rings, just as it is convenient to deal with homomorphisms and not always with canonical homomorphisms or a ring modulo an ideal.

The general theory of valuations and valuation rings is due to Krull, Allgemeine Bewertungstheorie, *J. reine angew. Math.* **167** (1932), pp. 169-196. However, the extension theory of homomorphisms as above was realized only around 1945 by Chevalley and Zariski.

We shall now give some examples of places and valuation rings.

Example 1. Let p be a prime number. Let $\mathbf{Z}_{(p)}$ be the ring of all rational numbers whose denominator is not divisible by p. Then $\mathbf{Z}_{(p)}$ is a valuation ring. The maximal ideal consists of those rational numbers whose numerator is divisible by p.

Example 2. Let k be a field and $R = k[X]$ the polynomial ring in one variable. Let $p = p(X)$ be an irreducible polynomial. Let $\mathfrak{o}$ be the ring of rational functions whose denominator is not divisible by p. Then $\mathfrak{o}$ is a valuation ring, similar to that of Example 1.

Example 3. Let R be the ring of power series $k[[X]]$ in one variable. Then R is a valuation ring, whose maximal ideal consists of those power series divisible by X. The residue class field is k itself.

Example 4. Let $R = k[[X_1, \ldots, X_n]]$ be the ring of power series in several variables. Then R is not a valuation ring, but R is imbedded in the field of repeated power series $k((X_1))((X_2)) \cdots ((X_n)) = K_n$. By Example 3, there is a place of K_n which is K_{n-1}-valued. By induction and composition, we can define a k-valued place of K_n. Since the field of rational functions $k(X_1, \ldots, X_n)$ is contained in K_n, the restriction of this place to $k(X_1, \ldots, X_n)$ gives a k-valued place of the field of rational functions in n variables.

Example 5. In Chapter XI we shall consider the notion of ordered field. Let k be an ordered subfield of an ordered field K. Let $\mathfrak{o}$ be the subset of elements of K which are not infinitely large with respect to k. Let $\mathfrak{m}$ be the subset of elements of $\mathfrak{o}$ which are infinitely small with respect to k. Then $\mathfrak{o}$ is a valuation ring in K and $\mathfrak{m}$ is its maximal ideal.

The following property of places will be used in connection with projective space in the next chapter.

Proposition 3.4. *Let $\varphi: K \to \{L, \infty\}$ be an L-valued place of K. Given a finite number of non-zero elements $x_1, \ldots, x_n \in K$ there exists an index j such that φ is finite on x_i/x_j for $i = 1, \ldots, n$.*

Proof. Let B be the valuation ring of the place. Define $x_i \leqq x_j$ to mean that $x_i/x_j \in B$. Then the relation $\leqq$ is transitive, that is if $x_i \leqq x_j$ and $x_j \leqq x_r$ then $x_i \leqq x_r$. Furthermore, by the property of a valuation ring, we always have $x_i \leqq x_j$ or $x_j \leqq x_i$ for all pairs of indices i, j. Hence we may order our elements, and we select the index j such that $x_i \leqq x_j$ for all i. This index j satisfies the requirement of the proposition.

We can obtain a characterization of integral elements by means of valuation rings. We shall use the following terminology. If $\mathfrak{o}$, $\mathfrak{O}$ are local rings with maximal ideals $\mathfrak{m}$, $\mathfrak{M}$ respectively, we shall say that $\mathfrak{O}$ **lies above** $\mathfrak{o}$ if $\mathfrak{o} \subset \mathfrak{O}$ and $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. We then have a canonical injection $\mathfrak{o}/\mathfrak{m} \to \mathfrak{O}/\mathfrak{M}$.

Proposition 3.5. *Let $\mathfrak{o}$ be a local ring contained in a field L. An element x of L is integral over $\mathfrak{o}$ if and only if x lies in every valuation ring $\mathfrak{O}$ of L lying above $\mathfrak{o}$.*

Proof. Assume that x is not integral over $\mathfrak{o}$. Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$. Then the ideal $(\mathfrak{m}, 1/x)$ of $\mathfrak{o}[1/x]$ cannot be the entire ring, otherwise we can write

$$-1 = a_n(1/x)^n + \cdots + a_1(1/x) + y$$

with $y \in \mathfrak{m}$ and $a_i \in \mathfrak{o}$. From this we get

$$(1 + y)x^n + \cdots + a_n = 0.$$

But $1 + y$ is not in $\mathfrak{m}$, hence is a unit of $\mathfrak{o}$. We divide the equation by $1 + y$ to conclude that x is integral over $\mathfrak{o}$, contrary to our hypothesis. Thus $(\mathfrak{m}, 1/x)$ is not the entire ring, and is contained in a maximal ideal $\mathfrak{P}$, whose intersection with $\mathfrak{o}$ contains $\mathfrak{m}$ and hence must be equal to $\mathfrak{m}$. Extending the canonical homomorphism $\mathfrak{o}[1/x] \to \mathfrak{o}[1/x]/\mathfrak{P}$ to a homomorphism of a valuation ring $\mathfrak{O}$ of L, we see that the image of $1/x$ is 0 and hence that x cannot be in this valuation ring.

Conversely, assume that x is integral over $\mathfrak{o}$, and let

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

be an integral equation for x with coefficients in $\mathfrak{o}$. Let $\mathfrak{O}$ be any valuation ring of L lying above $\mathfrak{o}$. Suppose $x \notin \mathfrak{O}$. Let φ be the place given by the canonical homomorphism of $\mathfrak{O}$ modulo its maximal ideal. Then $\varphi(x) = \infty$ so $\varphi(1/x) = 0$. Divide the above equation by x^n, and apply φ. Then each term except the first maps to 0 under φ, so we get $\varphi(1) = 0$, a contradiction which proves the proposition.

Proposition 3.6. *Let A be a ring contained in a field L. An element x of L is integral over A if and only if x lies in every valuation ring $\mathfrak{O}$ of L containing A. In terms of places, x is integral over A if and only if every place of L finite on A is finite on x.*

Proof. Assume that every place finite on A is finite on x. We may assume $x \neq 0$. If $1/x$ is a unit in $A[1/x]$ then we can write

$$x = c_0 + c_1(1/x) + \cdots + c_{n-1}(1/x)^{n-1}$$

with $c_i \in A$ and some n. Multiplying by x^{n-1} we conclude that x is integral over A. If $1/x$ is not a unit in $A[1/x]$, then $1/x$ generates a proper principal ideal. By Zorn's lemma this ideal is contained in a maximal ideal $\mathfrak{M}$. The homomorphism $A[1/x] \to A[1/x]/\mathfrak{M}$ can be extended to a place which is a finite on A but maps

$1/x$ on 0, so x on ∞, which contradicts the possibility that $1/x$ is not a unit in $A[1/x]$ and proves that x is integral over A. The converse implication is proved just as in the second part of Proposition 3.5.

Remark. Let K be a subfield of L and let $x \in L$. Then x is integral over K if and only if x is algebraic over K. So if a place φ of L is finite on K, and x is algebraic over K, then φ is finite on $K(x)$. Of course this is a trivial case of the integrality criterion which can be seen directly. Let

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

be the irreducible equation for x over K. Suppose $x \neq 0$. Then $a_0 \neq 0$. Hence $\varphi(x) \neq 0$ immediately from the equation, so φ is an isomorphism of $K(x)$ on its image.

The next result is a generalization whose technique of proof can also be used in Exercise 1 of Chapter IX (the Hilbert-Zariski theorem).

Theorem 3.7. General Integrality Criterion. *Let A be an entire ring. Let $z_1, \ldots, z_m$ be elements of some extension field of its quotient field K. Assume that each z_s ($s = 1, \ldots, m$) satisfies a polynomial relation*

$$z_s^{d_s} + g_s(z_1, \ldots, z_m) = 0$$

where $g_s(Z_1, \ldots, Z_m) \in A[Z_1, \ldots, Z_m]$ is a polynomial of total degree $< d_s$, and that any pure power of Z_s occuring with non-zero coefficient in g_s occurs with a power strictly less than d_s. Then $z_1, \ldots, z_m$ are integral over A.

Proof. We apply Proposition 3.6. Suppose some z_s is not integral over A. There exists a place φ of K, finite on A, such that $\varphi(z_s) = \infty$ for some s. By Proposition 3.4 we can pick an index s such that $\varphi(z_j/z_s) \neq \infty$ for all j. We divide the polynomial relation of the hypothesis in the lemma by $z_s^{d_s}$ and apply the place. By the hypothesis on g_s, it follows that $\varphi(g_s(z)/z_s^{d_s}) = 0$, whence we get $1 = 0$, a contradiction which proves the theorem.

EXERCISES

1. Let K be a Galois extension of the rationals $\mathbf{Q}$, with group G. Let B be the integral closure of $\mathbf{Z}$ in K, and let $\alpha \in B$ be such that $K = \mathbf{Q}(\alpha)$. Let $f(X) = \mathrm{Irr}(\alpha, \mathbf{Q}, X)$. Let p be a prime number, and assume that f remains irreducible mod p over $\mathbf{Z}/p\mathbf{Z}$. What can you say about the Galois group G? (Artin asked this question to Tate on his qualifying exam.)
2. Let A be an entire ring and K its quotient field. Let t be transcendental over K. If A is integrally closed, show that $A[t]$ is integrally closed.

For the following exercises, you can use §1 of Chapter X.

3. Let A be an entire ring, integrally closed in its quotient field K. Let L be a finite separable extension of K, and let B be the integral closure of A in L. If A is Noetherian, show that B is a finite A-module. [*Hint*: Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of L over K. Multiplying all elements of this basis by a suitable element of A, we may assume without loss of generality that all ω_i are integral over A. Let $\{\omega_1', \ldots, \omega_n'\}$ be the dual basis relative to the trace, so that $\mathrm{Tr}(\omega_i\omega_j') = \delta_{ij}$. Write an element α of L integral over A in the form

$$\alpha = b_1\omega_1' + \cdots + b_n\omega_n'$$

with $b_j \in K$. Taking the trace $\mathrm{Tr}(\alpha\omega_i)$, for $i = 1, \ldots, n$, conclude that B is contained in the finite module $A\omega_1' + \cdots + A\omega_n'$.] Hence B is Noetherian.

4. The preceding exercise applies to the case when $A = \mathbf{Z}$ and $k = \mathbf{Q}$. Let L be a finite extension of $\mathbf{Q}$ and let $\mathfrak{o}_L$ be the ring of algebraic integers in L. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of L into the complex numbers. Embedded $\mathfrak{o}_L$ into a Euclidean space by the map

$$\alpha \mapsto (\sigma_1\alpha, \ldots, \sigma_n\alpha).$$

Show that in any bounded region of space, there is only a finite number of elements of $\mathfrak{o}_L$. [*Hint*: The coefficients in an integral equation for α are elementary symmetric functions of the conjugates of α and thus are bounded integers.] Use Exercise 5 of Chapter III to conclude that $\mathfrak{o}_L$ is a free $\mathbf{Z}$-module of dimension $\leqq n$. In fact, show that the dimension is n, a basis of $\mathfrak{o}_L$ over $\mathbf{Z}$ also being a basis of L over $\mathbf{Q}$.

5. Let E be a finite extension of $\mathbf{Q}$, and let $\mathfrak{o}_E$ be the ring of algebraic integers of E. Let U be the group of units of $\mathfrak{o}_E$. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of E into $\mathbf{C}$. Map U into a Euclidean space, by the map

$$l: \alpha \mapsto (\log|\sigma_1\alpha|, \ldots, \log|\sigma_n\alpha|).$$

Show that $l(U)$ is a free abelian group, finitely generated, by showing that in any finite region of space, there is only a finite number of elements of $l(U)$. Show that the kernel of l is a finite group, and is therefore the group of roots of unity in E. Thus U itself is a finitely generated abelian group.

6. Generalize the results of §2 to infinite Galois extensions, especially Propositions 2.1 and 2.5, using Zorn's lemma.

7. **Dedekind rings.** Let $\mathfrak{o}$ be an entire ring which is Noetherian, integrally closed, and such that every non-zero prime ideal is maximal. Define a fractional ideal $\mathfrak{a}$ to be an $\mathfrak{o}$-submodule $\neq 0$ of the quotient field K such that there exists $c \in \mathfrak{o}$, $c \neq 0$ for which $c\mathfrak{a} \subset \mathfrak{o}$. Prove that the fractional ideals form a group under multiplication. Hint following van der Waerden: Prove the following statements in order:
   (a) Given an ideal $\mathfrak{a} \neq 0$ in $\mathfrak{o}$, there exists a product of prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}$.
   (b) Every maximal ideal $\mathfrak{p}$ is invertible, i.e. if we let $\mathfrak{p}^{-1}$ be the set of elements $x \in K$ such that $x\mathfrak{p} \subset \mathfrak{o}$, then $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}$.
   (c) Every non-zero ideal is invertible, by a fractional ideal. (Use the Noetherian property that if this is not true, there exists a maximal non-invertible ideal $\mathfrak{a}$, and get a contradiction.)

8. Using prime ideals instead of prime numbers for a Dedekind ring A, define the notion of content as in the Gauss lemma, and prove that if $f(X)$, $g(X) \in A[X]$ are polynomials of degree $\geqq 0$ with coefficients in A, then $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$. Also if K is the quotient field of A, prove the same statement for f, $g \in K[X]$.

9. Let A be an entire ring, integrally closed. Let B be entire, integral over A. Let Q_1, Q_2 be prime ideals of B with $Q_1 \supset Q_2$ but $Q_1 \neq Q_2$. Let $P_i = Q_i \cap A$. Show that $P_1 \neq P_2$.

10. Let n be a positive integer and let ζ, ζ' be primitive n-th roots of unity.
    (a) Show that $(1 - \zeta)/(1 - \zeta')$ is an algebraic integer.
    (b) If $n \geqq 6$ is divisible by at least two primes, show that $1 - \zeta$ is a unit in the ring $\mathbf{Z}[\zeta]$.

11. Let p be a prime and ζ a primitive p-th root of unity. Show that there is a principal ideal J in $\mathbf{Z}[\zeta]$ such that $J^{p-1} = (p)$ (the principal ideal generated by p).

Symmetric Polynomials

12. Let F be a field of characteristic 0. Let $t_1, \ldots, t_n$ be algebraically independent over F. Let $s_1, \ldots, s_n$ be the elementary symmetric functions. Then $R = F[t_1, \ldots, t_n]$ is an integral extension of $S = F[s_1, \ldots, s_n]$, and actually is its integral closure in the rational field $F(t_1, \ldots, t_n)$. Let W be the group of permutation of the variables $t_1, \ldots, t_n$.
    (a) Show that $S = R^W$ is the fixed subring of R under W.
    (b) Show that the elements $t_1^{r_1} \cdots t_n^{r_n}$ with $0 \leqq r_i \leqq n - i$ form a basis of R over S, so in particular, R is free over S.

I am told that the above basis is due to Kronecker. There is a much more interesting basis, which can be defined as follows.

Let $\partial_1, \ldots, \partial_n$ be the partial derivatives with respect to $t_1, \ldots, t_n$, so $\partial_i = \partial/\partial t_i$. Let $P \in F[t] = F[t_1, \ldots, t_n]$. Substituting ∂_i for t_i $(i = 1, \ldots, n)$ gives a partial differential operator $P(\partial) = P(\partial_1, \ldots, \partial_n)$ on R. An element of S can also be viewed as an element of R. Let $Q \in R$. We say that Q is W-**harmonic** if $P(\partial)Q = 0$ for all symmetric polynomials $P \in S$ with 0 constant term. It can be shown that the W-harmonic polynomials form a finite dimensional space. Furthermore, if $\{H_1, \ldots, H_N\}$ is a basis for this space over F, then it is also a basis for R over S. This is a special case of a general theorem of Chevalley. See [La 99b], where the special case is worked out in detail.