applied to each one of $w_1, \ldots, w_n$ gives the value 0. But $\sigma_1, \ldots, \sigma_n$ are linearly independent as characters of the multiplicative group E^* into k^{a*}. It follows that $\alpha_i = 0$ for $i = 1, \ldots, n$, and our vectors are linearly independent.

Remark. In characteristic 0, one sees much more trivially that the trace is not identically 0. Indeed, if $c \in k$ and $c \neq 0$, then $\mathrm{Tr}(c) = nc$ where $n = [E : k]$, and $n \neq 0$. This argument also holds in characteristic p when n is prime to p.

Proposition 5.5. *Let $E = k(\alpha)$ be a separable extension. Let*

$$f(X) = \mathrm{Irr}(\alpha, k, X),$$

and let $f'(X)$ be its derivative. Let

$$\frac{f(X)}{(X - \alpha)} = \beta_0 + \beta_1 X + \cdots + \beta_{n-1} X^{n-1}$$

with $\beta_i \in E$. Then the dual basis of $1, \alpha, \ldots, \alpha^{n-1}$ is

$$\frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)}.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f. Then

$$\sum_{i=1}^{n} \frac{f(X)}{(X - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r \qquad \text{for} \quad 0 \leqq r \leqq n - 1.$$

To see this, let $g(X)$ be the difference of the left- and right-hand side of this equality. Then g has degree $\leqq n - 1$, and has n roots $\alpha_1, \ldots, \alpha_n$. Hence g is identically zero.

The polynomials

$$\frac{f(X)}{(X - \alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)}$$

are all conjugate to each other. If we define the trace of a polynomial with coefficients in E to be the polynomial obtained by applying the trace to the coefficients, then

$$\mathrm{Tr}\left[\frac{f(X)}{(X - \alpha)} \frac{\alpha^r}{f'(\alpha)}\right] = X^r.$$

Looking at the coefficients of each power of X in this equation, we see that

$$\mathrm{Tr}\left(\alpha^i \frac{\beta_j}{f'(\alpha)}\right) = \delta_{ij},$$

thereby proving our proposition.

Finally we establish a connection with determinants, whose basic properties we now assume. Let E be a finite extension of k, which we view as a finite dimensional vector space over k. For each $\alpha \in E$ we have the k-linear map

multiplication by α,

$$m_\alpha : E \to E \quad \text{such that} \quad m_\alpha(x) = \alpha x.$$

Then we have the determinant $\det(m_\alpha)$, which can be computed as the determinant of the matrix M_α representing m_α with respect to a basis. Similarly we have the trace $\mathrm{Tr}(m_\alpha)$, which is the sum of the diagonal elements of the matrix M_α.

Proposition 5.6. *Let E be a finite extension of k and let $\alpha \in E$. Then*

$$\det(m_\alpha) = N_{E/k}(\alpha) \quad \textit{and} \quad \mathrm{Tr}(m_\alpha) = \mathrm{Tr}_{E/k}(\alpha).$$

Proof. Let $F = k(\alpha)$. If $[F : k] = d$, then $1, \alpha, \ldots, \alpha^{d-1}$ is a basis for F over k. Let $\{w_1, \ldots, w_r\}$ be a basis for E over F. Then $\{\alpha^i w_j\}$ $(i = 0, \ldots, d-1; j = 1, \ldots, r)$ is a basis for E over k. Let

$$f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$$

be the irreducible polynomial of α over k. Then $N_{F/k}(\alpha) = (-1)^d a_0$, and by the transitivity of the norm, we have

$$N_{E/k}(\alpha) = N_{F/k}(\alpha)^r.$$

The reader can verify directly on the above basis that $N_{F/k}(\alpha)$ is the determinant of m_α on F, and then that $N_{F/k}(\alpha)^r$ is the determinant of m_α on E, thus concluding the proof for the determinant. The trace is handled exactly in the same way, except that $\mathrm{Tr}_{E/k}(\alpha) = r \cdot \mathrm{Tr}_{F/k}(\alpha)$. The trace of the matrix for m_α on F is equal to $-a_{d-1}$. From this the statement identifying the two traces is immediate, as it was for the norm.

§6. CYCLIC EXTENSIONS

We recall that a finite extension is said to be cyclic if it is Galois and its Galois group is cyclic. The determination of cyclic extensions when enough roots of unity are in the ground field is based on the following fact.

Theorem 6.1. (Hilbert's Theorem 90). *Let K/k be cyclic of degree n with Galois group G. Let σ be a generator of G. Let $\beta \in K$. The norm $N_k^K(\beta) = N(\beta)$ is equal to 1 if and only if there exists an element $\alpha \neq 0$ in K such that $\beta = \alpha/\sigma\alpha$.*

Proof. Assume such an element α exists. Taking the norm of β we get $N(\alpha)/N(\sigma\alpha)$. But the norm is the product over all automorphisms in G. Inserting σ just permutes these automorphisms. Hence the norm is equal to 1.

It will be convenient to use an exponential notation as follows. If $\tau, \tau' \in G$ and $\xi \in K$ we write

$$\xi^{\tau+\tau'} = \xi^\tau \xi^{\tau'}.$$

By Artin's theorem on characters, the map given by

$$\mathrm{id} + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\sigma^{n-1}$$

on K is not identically zero. Hence there exists $\theta \in K$ such that the element

$$\alpha = \theta + \beta\theta^{\sigma} + \beta^{1+\sigma}\theta^{\sigma^2} + \cdots + \beta^{1+\sigma+\cdots+\sigma^{n-2}}\theta^{\sigma^{n-1}}$$

is not equal to 0. It is then clear that $\beta\alpha^{\sigma} = \alpha$ using the fact that $N(\beta) = 1$, and hence that when we apply $\beta\sigma$ to the last term in the sum, we obtain θ. We divide by α^{σ} to conclude the proof.

Theorem 6.2. *Let k be a field, n an integer > 0 prime to the characteristic of k (if not 0), and assume that there is a primitive n-th root of unity in k.*

(i) *Let K be a cyclic extension of degree n. Then there exists $\alpha \in K$ such that $K = k(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in k$.*

(ii) *Conversely, let $a \in k$. Let α be a root of $X^n - a$. Then $k(\alpha)$ is cyclic over k, of degree d, $d \mid n$, and α^d is an element of k.*

Proof. Let ζ be a primitive n-th root of unity in k, and let K/k be cyclic with group G. Let σ be a generator of G. We have $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. By Hilbert's theorem 90, there exists $\alpha \in K$ such that $\sigma\alpha = \zeta\alpha$. Since ζ is in k, we have $\sigma^i\alpha = \zeta^i\alpha$ for $i = 1, \ldots, n$. Hence the elements $\zeta^i\alpha$ are n distinct conjugates of α over k, whence $[k(\alpha) : k]$ is at least equal to n. Since $[K : k] = n$, it follows that $K = k(\alpha)$. Furthermore,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n.$$

Hence α^n is fixed under σ, hence is fixed under each power of σ, hence is fixed under G. Therefore α^n is an element of k, and we let $a = \alpha^n$. This proves the first part of the theorem.

Conversely, let $a \in k$. Let α be a root of $X^n - a$. Then $\alpha\zeta^i$ is also a root for each $i = 1, \ldots, n$, and hence all roots lie in $k(\alpha)$ which is therefore normal over k. All the roots are distinct so $k(\alpha)$ is Galois over k. Let G be the Galois group.

If σ is an automorphism of $k(\alpha)/k$ then $\sigma\alpha$ is also a root of $X^n - a$. Hence $\sigma\alpha = \omega_\sigma\alpha$ where ω_σ is an n-th root of unity, not necessarily primitive. The map $\sigma \mapsto \omega_\sigma$ is obviously a homomorphism of G into the group of n-th roots of unity, and is injective. Since a subgroup of a cyclic group is cyclic, we conclude that G is cyclic, of order d, and $d \mid n$. The image of G is a cyclic group of order d. If σ is a generator of G, then ω_σ is a primitive dth root of unity. Now we get

$$\sigma(\alpha^d) = (\sigma\alpha)^d = (\omega_\sigma\alpha)^d = \alpha^d.$$

Hence α^d is fixed under σ, and therefore fixed under G. It is an element of k, and our theorem is proved.

We now pass to the analogue of Hilbert's theorem 90 in characteristic p for cyclic extensions of degree p.

Theorem 6.3. (Hilbert's Theorem 90, Additive Form). *Let k be a field and K/k a cyclic extension of degree n with group G. Let σ be a generator of G. Let $\beta \in K$. The trace $\mathrm{Tr}_k^K(\beta)$ is equal to 0 if and only if there exists an element $\alpha \in K$ such that $\beta = \alpha - \sigma\alpha$.*

Proof. If such an element α exists, then we see that the trace is 0 because the trace is equal to the sum taken over all elements of G, and applying σ permutes these elements.

Conversely, assume $\mathrm{Tr}(\beta) = 0$. There exists an element $\theta \in K$ such that $\mathrm{Tr}(\theta) \neq 0$. Let

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)} [\beta\theta^{\sigma} + (\beta + \sigma\beta)\theta^{\sigma^2} + \cdots + (\beta + \sigma\beta + \cdots + \sigma^{n-2}\beta)\theta^{\sigma^{n-1}}].$$

From this it follows at once that $\beta = \alpha - \sigma\alpha$.

Theorem 6.4. (Artin-Schreier) *Let k be a field of characteristic p.*

(i) *Let K be a cyclic extension of k of degree p. Then there exists $\alpha \in K$ such that $K = k(\alpha)$ and α satisfies an equation $X^p - X - a = 0$ with some $a \in k$.*

(ii) *Conversely, given $a \in k$, the polynomial $f(X) = X^p - X - a$ either has one root in k, in which case all its roots are in k, or it is irreducible. In this latter case, if α is a root then $k(\alpha)$ is cyclic of degree p over k.*

Proof. Let K/k be cyclic of degree p. Then $\mathrm{Tr}_k^K(-1) = 0$ (it is just the sum of -1 with itself p times). Let σ be a generator of the Galois group. By the additive form of Hilbert's theorem 90, there exists $\alpha \in K$ such that $\sigma\alpha - \alpha = 1$, or in other words, $\sigma\alpha = \alpha + 1$. Hence $\sigma^i\alpha = \alpha + i$ for all integers $i = 1, \ldots, p$ and α has p distinct conjugates. Hence $[k(\alpha) : k] \geqq p$. It follows that $K = k(\alpha)$. We note that

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Hence $\alpha^p - \alpha$ is fixed under σ, hence it is fixed under the powers of σ, and therefore under G. It lies in the fixed field k. If we let $a = \alpha^p - \alpha$ we see that our first assertion is proved.

Conversely, let $a \in k$. If α is a root of $X^p - X - a$ then $\alpha + i$ is also a root for $i = 1, \ldots, p$. Thus $f(X)$ has p distinct roots. If one root lies in k then all roots lie in k. Assume that no root lies in k. We contend that the

polynomial is irreducible. Suppose that

$$f(X) = g(X)h(X)$$

with $g, h \in k[X]$ and $1 \leqq \deg g < p$. Since

$$f(X) = \prod_{i=1}^{p}(X - \alpha - i)$$

we see that $g(X)$ is a product over certain integers i. Let $d = \deg g$. The coefficient of X^{d-1} in g is a sum of terms $-(\alpha + i)$ taken over precisely d integers i. Hence it is equal to $-d\alpha + j$ for some integer j. But $d \neq 0$ in k, and hence α lies in k, because the coefficients of g lie in k, contradiction. We know therefore that $f(X)$ is irreducible. All roots lie in $k(\alpha)$, which is therefore normal over k. Since $f(X)$ has no multiple roots, it follows that $k(\alpha)$ is Galois over k. There exists an automorphism σ of $k(\alpha)$ over k such that $\sigma\alpha = \alpha + 1$ (because $\alpha + 1$ is also a root). Hence the powers σ^i of σ give $\sigma^i\alpha = \alpha + i$ for $i = 1, \ldots, p$ and are distinct. Hence the Galois group consists of these powers and is cyclic, thereby proving the theorem.

For cyclic extensions of degree p^r, see the exercises on Witt vectors and the bibliography at the end of §8.

§7. SOLVABLE AND RADICAL EXTENSIONS

A finite extension E/k (which we shall assume separable for convenience) is said to be **solvable** if the Galois group of the smallest Galois extension K of k containing E is a solvable group. This is equivalent to saying that there exists a solvable Galois extension L of k such that $k \subset E \subset L$. Indeed, we have $k \subset E \subset K \subset L$ and $G(K/k)$ is a homomorphic image of $G(L/k)$.

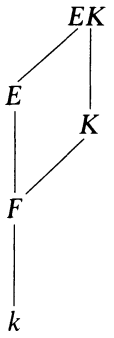
Proposition 7.1. *Solvable extensions form a distinguished class of extensions.*

Proof. Let E/k be solvable. Let F be a field containing k and assume E, F are subfields of some algebraically closed field. Let K be Galois solvable over k, and $E \subset K$. Then KF is Galois over F and $G(KF/F)$ is a subgroup of $G(K/k)$ by Theorem 1.12. Hence EF/F is solvable. It is clear that a subextension of a solvable extension is solvable. Let $E \supset F \supset k$ be a tower, and assume that E/F is solvable and F/k is solvable. Let K be a finite solvable Galois extension of k containing F. We just saw that EK/K is solvable. Let L be a solvable Galois extension of K containing EK. If σ is any embedding of L over k in a given algebraic closure, then $\sigma K = K$ and hence σL is a solvable extension of K. We let M be the compositum of all extensions σL for all embeddings σ of L over k.

Then M is Galois over k, and is therefore Galois over K. The Galois group of M over K is a subgroup of the product

$$\prod_{\sigma} G(\sigma L/K)$$

by Theorem 1.14. Hence it is solvable. We have a surjective homomorphism $G(M/k) \to G(K/k)$ by Theorem 1.10. Hence the Galois group of M/k has a solvable normal subgroup whose factor group is solvable. It is therefore solvable. Since $E \subset M$, our proof is complete.



A finite extension F of k is said to be **solvable by radicals** if it is separable and if there exists a finite extension E of k containing F, and admitting a tower decomposition

$$k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E$$

such that each step E_{i+1}/E_i is one of the following types:

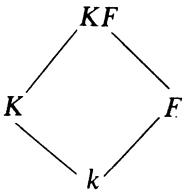
1. It is obtained by adjoining a root of unity.
2. It is obtained by adjoining a root of a polynomial $X^n - a$ with $a \in E_i$ and n prime to the characteristic.
3. It is obtained by adjoining a root of an equation $X^p - X - a$ with $a \in E_i$ if p is the characteristic > 0.

One can see at once that the class of extensions which are solvable by radicals is a distinguished class.

Theorem 7.2. *Let E be a separable extension of k. Then E is solvable by radicals if and only if E/k is solvable.*

Proof. Assume that E/k is solvable, and let K be a finite solvable Galois extension of k containing E. Let m be the product of all primes unequal to the characteristic dividing the degree $[K : k]$, and let $F = k(\zeta)$ where ζ is a primitive m-th root of unity. Then F/k is abelian. We lift K over F. Then KF is solvable over F. There is a tower of subfields between F and KF such that each step is cyclic of prime order, because every solvable group admits a tower of sub-

groups of the same type, and we can use Theorem 1.10. By Theorems 6.2 and 6.4, we conclude that KF is solvable by radicals over F, and hence is solvable by radicals over k. This proves that E/k is solvable by radicals.



Conversely, assume that E/k is solvable by radicals. For any embedding σ of E in E^a over k, the extension $\sigma E/k$ is also solvable by radicals. Hence the smallest Galois extension K of E containing k, which is a composite of E and its conjugates is solvable by radicals. Let m be the product of all primes unequal to the characteristic dividing the degree $[K : k]$ and again let $F = k(\zeta)$ where ζ is a primitive m-th root of unity. It will suffice to prove that KF is solvable over F, because it follows then that KF is solvable over k and hence $G(K/k)$ is solvable because it is a homomorphic image of $G(KF/k)$. But KF/F can be decomposed into a tower of extensions, such that each step is of prime degree and of the type described in Theorem 6.2 or Theorem 6.4, and the corresponding root of unity is in the field F. Hence KF/F is solvable, and our theorem is proved.

Remark. One could modify our preceding discussion by not assuming separability. Then one must deal with normal extensions instead of Galois extensions, and one must allow equations $X^p - a$ in the solvability by radicals, with p equal to the characteristic. Then we still have the theorem corresponding to Theorem 7.2. The proof is clear in view of Chapter V, §6.

For a proof that every solvable group is a Galois group over the rationals, I refer to Shafarevich [Sh 54], as well as contributions of Iwasawa [Iw 53].

[Iw 53] K. IWASAWA, On solvable extension of algebraic number fields, *Ann. of Math.* **58** (1953), pp. 548–572

[Sh 54] I. SHAFAREVICH, Construction of fields of algebraic numbers with given solvable Galois group, *Izv. Akad. Nauk SSSR* **18** (1954), pp. 525–578 (*Amer. Math. Soc. Transl.* **4** (1956), pp. 185–237)

§8. ABELIAN KUMMER THEORY

In this section we shall carry out a generalization of the theorem concerning cyclic extensions when the ground field contains enough roots of unity.

Let k be a field and m a positive integer. A Galois extension K of k with group G is said to be of **exponent** m if $\sigma^m = 1$ for all $\sigma \in G$.

We shall investigate abelian extensions of exponent m. We first assume that m is not a multiple of the characteristic of k (if not 0), and that k contains the group of m-th roots of unity which we denote by μ_m. We assume that all our algebraic extensions in this section are contained in a fixed algebraic closure k^a.

Let $a \in k$. The symbol $a^{1/m}$ (or $\sqrt[m]{a}$) is not well defined. If $\alpha^m = a$ and ζ is an m-th root of unity, then $(\zeta\alpha)^m = a$ also. We shall use the symbol $a^{1/m}$ to denote any such element α, which will be called an m-th root of a. Since the roots of unity are in the ground field, we observe that the field $k(\alpha)$ is the same no matter which m-th root α of a we select. We denote this field by $k(a^{1/m})$.

We denote by k^{*m} the subgroup of k^* consisting of all m-th powers of non-zero elements of k. It is the image of k^* under the homomorphism $x \mapsto x^m$.

Let B be a subgroup of k^* containing k^{*m}. We denote by $k(B^{1/m})$ or K_B the composite of all fields $k(a^{1/m})$ with $a \in B$. It is uniquely determined by B as a subfield of k^a.

Let $a \in B$ and let α be an m-th root of a. The polynomial $X^m - a$ splits into linear factors in K_B, and thus K_B is Galois over k, because this holds for all $a \in B$. Let G be the Galois group. Let $\sigma \in G$. Then $\sigma\alpha = \omega_\sigma\alpha$ for some m-th root of unity $\omega_\sigma \in \mu_m \subset k^*$. The map

$$\sigma \mapsto \omega_\sigma$$

is obviously a homomorphism of G into μ_m, i.e. for $\tau, \sigma \in G$ we have

$$\tau\sigma\alpha = \omega_\tau\omega_\sigma\alpha = \omega_\sigma\omega_\tau\alpha.$$

We may write $\omega_\sigma = \sigma\alpha/\alpha$. This root of unity ω_σ is independent of the choice of m-th root of a, for if α' is another m-th root, then $\alpha' = \zeta\alpha$ for some $\zeta \in \mu_m$, whence

$$\sigma\alpha'/\alpha' = \zeta\sigma\alpha/\zeta\alpha = \sigma\alpha/\alpha.$$

We denote ω_σ by $\langle \sigma, a \rangle$. The map

$$(\sigma, a) \mapsto \langle \sigma, a \rangle$$

gives us a map

$$G \times B \to \mu_m.$$

If $a, b \in B$ and $\alpha^m = a$, $\beta^m = b$ then $(\alpha\beta)^m = ab$ and

$$\sigma(\alpha\beta)/\alpha\beta = (\sigma\alpha/\alpha)(\sigma\beta/\beta).$$

We conclude that the map above is bilinear. Furthermore, if $a \in k^{*m}$ it follows that $\langle \sigma, a \rangle = 1$.

Theorem 8.1. *Let k be a field, m an integer > 0 prime to the characteristic of k (if not 0). We assume that k contains μ_m. Let B be a subgroup of k^* containing k^{*m} and let $K_B = k(B^{1/m})$. Then K_B is Galois, and abelian of exponent m. Let G be its Galois group. We have a bilinear map*

$$G \times B \to \mu_m \quad \text{given by} \quad (\sigma, a) \mapsto \langle \sigma, a \rangle.$$

If $\sigma \in G$ and $a \in B$, and $\alpha^m = a$ then $\langle \sigma, a \rangle = \sigma\alpha/\alpha$. The kernel on the left is 1 and the kernel on the right is k^{*m}. The extension K_B/k is finite if and only if $(B : k^{*m})$ is finite. If that is the case, then

$$B/k^{*m} \approx G^\wedge,$$

and in particular we have the equality

$$[K_B : k] = (B : k^{*m}).$$

Proof. Let $\sigma \in G$. Suppose $\langle \sigma, a \rangle = 1$ for all $a \in B$. Then for every generator α of K_B such that $\alpha^m = a \in B$ we have $\sigma\alpha = \alpha$. Hence σ induces the identity on K_B and the kernel on the left is 1. Let $a \in B$ and suppose $\langle \sigma, a \rangle = 1$ for all $\sigma \in G$. Consider the subfield $k(a^{1/m})$ of K_B. If $a^{1/m}$ is not in k, there exists an automorphism of $k(a^{1/m})$ over k which is not the identity. Extend this automorphism to K_B, and call this extension σ. Then clearly $\langle \sigma, a \rangle \neq 1$. This proves our contention.

By the duality theorem of Chapter I, §9 we see that G is finite if and only if B/k^{*m} is finite, and in that case we have the isomorphism as stated, so that in particular the order of G is equal to $(B : k^{*m})$, thereby proving the theorem.

Theorem 8.2. *Notation being as in Theorem* 8.1, *the map $B \mapsto K_B$ gives a bijection of the set of subgroups of k^* containing k^{*m} and the abelian extensions of k of exponent m.*

Proof. Let B_1, B_2 be subgroups of k^* containing k^{*m}. If $B_1 \subset B_2$ then $k(B_1^{1/m}) \subset k(B_2^{1/m})$. Conversely, assume that $k(B_1^{1/m}) \subset k(B_2^{1/m})$. We wish to prove $B_1 \subset B_2$. Let $b \in B_1$. Then $k(b^{1/m}) \subset k(B_2^{1/m})$ and $k(b^{1/m})$ is contained in a finitely generated subextension of $k(B_2^{1/m})$. Thus we may assume without loss of generality that B_2/k^{*m} is finitely generated, hence finite. Let B_3 be the subgroup of k^* generated by B_2 and b. Then $k(B_2^{1/m}) = k(B_3^{1/m})$ and from what we saw above, the degree of this field over k is precisely

$$(B_2 : k^{*m}) \quad \text{or} \quad (B_3 : k^{*m}).$$

Thus these two indices are equal, and $B_2 = B_3$. This proves that $B_1 \subset B_2$.

We now have obtained an injection of our set of groups B into the set of abelian extensions of k of exponent m. Assume finally that K is an abelian extension of k of exponent m. Any finite subextension is a composite of cyclic extensions of exponent m because any finite abelian group is a product of cyclic groups, and we can apply Corollary 1.16. By Theorem 6.2, every cyclic extension can be obtained by adjoining an m-th root. Hence K can be obtained by adjoining a family of m-th roots, say m-th roots of elements $\{b_j\}_{j \in J}$ with $b_j \in k^*$. Let B be the subgroup of k^* generated by all b_j and k^{*m}. If $b' = ba^m$ with $a, b \in k$ then obviously

$$k(b'^{1/m}) = k(b^{1/m}).$$

Hence $k(B^{1/m}) = K$, as desired.

When we deal with abelian extensions of exponent p equal to the characteristic, then we have to develop an additive theory, which bears the same relationship to Theorems 8.1 and 8.2 as Theorem 6.4 bears to Theorem 6.2.

If k is a field, we define the operator $\wp$ by

$$\wp(x) = x^p - x$$

for $x \in k$. Then $\wp$ is an additive homomorphism of k into itself. The subgroup $\wp(k)$ plays the same role as the subgroup k^{*m} in the multiplicative theory, whenever m is a prime number. The theory concerning a power of p is slightly more elaborate and is due to Witt.

We now assume k has characteristic p. A root of the polynomial $X^p - X - a$ with $a \in k$ will be denoted by $\wp^{-1}a$. If B is a subgroup of k containing $\wp k$ we let $K_B = k(\wp^{-1}B)$ be the field obtained by adjoining $\wp^{-1}a$ to k for all $a \in B$. We emphasize the fact that B is an *additive* subgroup of k.

Theorem 8.3. *Let k be a field of characteristic p. The map $B \mapsto k(\wp^{-1}B)$ is a bijection between subgroups of k containing $\wp k$ and abelian extensions of k of exponent p. Let $K = K_B = k(\wp^{-1}B)$, and let G be its Galois group. If $\sigma \in G$ and $a \in B$, and $\wp\alpha = a$, let $\langle \sigma, a \rangle = \sigma\alpha - \alpha$. Then we have a bilinear map*

$$G \times B \to \mathbf{Z}/p\mathbf{Z} \quad \text{given by} \quad (\sigma, a) \to \langle \sigma, a \rangle.$$

The kernel on the left is 1 and the kernel on the right is $\wp k$. The extension K_B/k is finite if and only if $(B : \wp k)$ is finite and if that is the case, then

$$[K_B : k] = (B : \wp k).$$

Proof. The proof is entirely similar to the proof of Theorems 8.1 and 8.2. It can be obtained by replacing multiplication by addition, and using the "$\wp$-th root" instead of an m-th root. Otherwise, there is no change in the wording of the proof.

The analogous theorem for abelian extensions of exponent p^n requires Witt vectors, and will be developed in the exercises.

Bibliography

[Wi 35] E. WITT, Der Existenzsatz für abelsche Funktionenkörper, *J. reine angew. Math.* **173** (1935), pp. 43–51

[Wi 36] E. WITT, Konstruktion von galoisschen Körpern der Charakteristik p mit vorgegebener Gruppe der Ordung p^f, *J. reine angew. Math.* **174** (1936), pp. 237–245

[Wi 37] E. WITT, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, *J. reine angew. Math.* **176** (1937), pp. 126–140

§9. THE EQUATION $X^n - a = 0$

When the roots of unity are not in the ground field, the equation $X^n - a = 0$ is still interesting but a little more subtle to treat.

Theorem 9.1. *Let k be a field and n an integer $\geqq 2$. Let $a \in k, a \neq 0$. Assume that for all prime numbers p such that $p|n$ we have $a \notin k^p$, and if $4|n$ then $a \notin -4k^4$. Then $X^n - a$ is irreducible in $k[X]$.*

Proof. Our first assumption means that a is not a p-th power in k. We shall reduce our theorem to the case when n is a prime power, by induction.

Write $n = p^r m$ with p prime to m, and p odd. Let

$$X^m - a = \prod_{v=1}^{m} (X - \alpha_v)$$

be the factorization of $X^m - a$ into linear factors, and say $\alpha = \alpha_1$. Substituting X^{p^r} for X we get

$$X^n - a = X^{p^r m} - a = \prod_{v=1}^{m} (X^{p^r} - \alpha_v).$$

We may assume inductively that $X^m - a$ is irreducible in $k[X]$. We contend that α is not a p-th power in $k(\alpha)$. Otherwise, $\alpha = \beta^p$, $\beta \in k(\alpha)$. Let N be the norm from $k(\alpha)$ to k. Then

$$-a = (-1)^m N(\alpha) = (-1)^m N(\beta^p) = (-1)^m N(\beta)^p.$$

If m is odd, a is a p-th power, which is impossible. Similarly, if m is even and p is odd, we also get a contradiction. This proves our contention, because m is prime to p. If we know our theorem for prime powers, then we conclude that $X^{p^r} - \alpha$ is irreducible over $k(\alpha)$. If A is a root of $X^{p^r} - \alpha$ then $k \subset k(\alpha) \subset k(A)$ gives a tower, of which the bottom step has degree m and the top step has degree p^r. It follows that A has degree n over k and hence that $X^n - a$ is irreducible.

We now suppose that $n = p^r$ is a prime power.

If p is the characteristic, let α be a p-th root of a. Then $X^p - a = (X - \alpha)^p$ and hence $X^{p^r} - a = (X^{p^{r-1}} - \alpha)^p$ if $r \geqq 2$. By an argument even more trivial than before, we see that α is not a p-th power in $k(\alpha)$, hence inductively $X^{p^{r-1}} - \alpha$ is irreducible over $k(\alpha)$. Hence $X^{p^r} - a$ is irreducible over k.

Suppose that p is not the characteristic. We work inductively again, and let α be a root of $X^p - a$.

Suppose a is not a p-th power in k. We claim that $X^p - a$ is irreducible. Otherwise a root α of $X^p - a$ generates an extension $k(\alpha)$ of degree $d < p$ and $\alpha^p = a$. Taking the norm from $k(\alpha)$ to k we get $N(\alpha)^p = a^d$. Since d is prime to p, it follows that a is a p-th power in k, contradiction.

Let $r \geqq 2$. We let $\alpha = \alpha_1$. We have

$$X^p - a = \prod_{v=1}^{p} (X - \alpha_v)$$

and

$$X^{p^r} - a = \prod_{v=1}^{p} (X^{p^{r-1}} - \alpha_v).$$

Assume that α is not a p-th power in $k(\alpha)$. Let A be a root of $X^{p^{r-1}} - \alpha$. If p is odd then by induction, A has degree p^{r-1} over $k(\alpha)$, hence has degree p^r over k and we are done. If $p = 2$, suppose $\alpha = -4\beta^4$ with $\beta \in k(\alpha)$. Let N be the norm from $k(\alpha)$ to k. Then $-a = N(\alpha) = 16N(\beta)^4$, so $-a$ is a square in k. Since $p = 2$ we get $\sqrt{-1} \in k(\alpha)$ and $\alpha = (\sqrt{-1}\, 2\beta^2)^2$, a contradiction. Hence again by induction, we find that A has degree p^r over k. We therefore assume that $\alpha = \beta^p$ with some $\beta \in k(\alpha)$, and derive the consequences.

Taking the norm from $k(\alpha)$ to k we find

$$-a = (-1)^p N(\alpha) = (-1)^p N(\beta^p) = (-1)^p N(\beta)^p.$$

If p is odd, then a is a p-th power in k, contradiction. Hence $p = 2$, and

$$-a = N(\beta)^2$$

is a square in k. Write $-a = b^2$ with $b \in k$. Since a is not a square in k we conclude that -1 is not a square in k. Let $i^2 = -1$. Over $k(i)$ we have the factorization

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib).$$

Each factor is of degree 2^{r-1} and we argue inductively. If $X^{2^{r-1}} \pm ib$ is reducible over $k(i)$ then $\pm ib$ is a square in $k(i)$ or lies in $-4(k(i))^4$. In either case, $\pm ib$ is a square in $k(i)$, say

$$\pm ib = (c + di)^2 = c^2 + 2cdi - d^2$$

with $c, d \in k$. We conclude that $c^2 = d^2$ or $c = \pm d$, and $\pm ib = 2cdi = \pm 2c^2 i$. Squaring gives a contradiction, namely

$$a = -b^2 = -4c^4.$$

We now conclude by unique factorization that $X^{2^r} + b^2$ cannot factor in $k[X]$, thereby proving our theorem.

The conditions of our theorem are necessary because

$$X^4 + 4b^4 = (X^2 + 2bX + 2b^2)(X^2 - 2bX + 2b^2).$$

If $n = 4m$ and $a \in -4k^4$ then $X^n - a$ is reducible.

Corollary 9.2. *Let k be a field and assume that $a \in k$, $a \neq 0$, and that a is not a p-th power for some prime p. If p is equal to the characteristic, or if p is odd, then for every integer $r \geqq 1$ the polynomial $X^{p^r} - a$ is irreducible over k.*

Proof. The assertion is logically weaker than the assertion of the theorem.

Corollary 9.3. *Let k be a field and assume that the algebraic closure k^a of k is of finite degree > 1 over k. Then $k^a = k(i)$ where $i^2 = -1$, and k has characteristic 0.*

Proof. We note that k^a is normal over k. If k^a is not separable over k, so char $k = p > 0$, then k^a is purely inseparable over some subfield of degree $>$ 1 (by Chapter V, §6), and hence there is a subfield E containing k, and an element $a \in E$ such that $X^p - a$ is irreducible over E. By Corollary 9.2, k^a cannot be of finite degree over E. (The reader may restrict his or her attention to characteristic 0 if Chapter V, §6 was omitted.)

We may therefore assume that k^a is Galois over k. Let $k_1 = k(i)$. Then k^a is also Galois over k_1. Let G be the Galois group of k^a/k_1. Suppose that there is a prime number p dividing the order of G, and let H be a subgroup of order p. Let F be its fixed field. Then $[k^a : F] = p$. If p is the characteristic, then Exercise 29 at the end of the chapter will give the contradiction. We may assume that p is not the characteristic. The p-th roots of unity $\neq 1$ are the roots of a polynomial of degree $\leqq p - 1$ (namely $X^{p-1} + \cdots + 1$), and hence must lie in F. By Theorem 6.2, it follows that k^a is the splitting field of some polynomial $X^p - a$ with $a \in F$. The polynomial $X^{p^2} - a$ is necessarily reducible. By the theorem, we must have $p = 2$ and $a = -4b^4$ with $b \in F$. This implies

$$k^a = F(a^{1/2}) = F(i).$$

But we assumed $i \in k_1$, contradiction.

Thus we have proved $k^a = k(i)$. It remains to prove that char $k = 0$, and for this I use an argument shown to me by Keith Conrad. We first show that a sum of squares in k is a square. It suffices to prove this for a sum of two squares, and in this case we write an element $x + iy \in k(i) = k^a$ as a square.

$$x + iy = (u + iv)^2, \qquad x, y, u, v \in k,$$

and then $x^2 + y^2 = (u^2 + v^2)^2$. Then to prove k has characteristic 0, we merely observe that if the characteristic is > 0, then -1 is a finite sum $1 + \ldots + 1$, whence a square by what we have just shown, but $k^a = k(i)$, so this concludes the proof.

Corollary 9.3 is due to Artin; see [Ar 24], given at the end of Chapter XI. In that chapter, much more will be proved about the field k.

Example 1. Let $k = \mathbf{Q}$ and let $G_{\mathbf{Q}} = G(\mathbf{Q}^a/\mathbf{Q})$. Then the only non-trivial torsion elements in $G_{\mathbf{Q}}$ have order 2. It follows from Artin's theory (as given in Chapter XI) that all such torsion elements are conjugate in $G_{\mathbf{Q}}$. One uses Chapter XI, Theorems 2.2, 2.4, and 2.9.)

Example 2. Let k be a field of characteristic not dividing n. Let $a \in k$, $a \neq 0$ and let K be the splitting field of $X^n - a$. Let α be one root of $X^n - a$, and let ζ be a primitive n-th root of unity. Then

$$K = k(\alpha, \zeta) = k(\alpha, \boldsymbol{\mu}_n).$$

We assume the reader is acquainted with matrices over a commutative ring. Let $\sigma \in G_{K/k}$. Then $(\sigma\alpha)^n = a$, so there exists some integer $b = b(\sigma)$ uniquely determined mod n, such that

$$\sigma(\alpha) = \alpha\zeta^{b(\sigma)}.$$

Since σ induces an automorphism of the cyclic group $\boldsymbol{\mu}_n$, there exists an integer $d(\sigma)$ relatively prime to n and uniquely determined mod n such that $\sigma(\zeta) = \zeta^{d(\sigma)}$. Let $G(n)$ be the subgroup of $GL_2(\mathbf{Z}/n\mathbf{Z})$ consisting of all matrices

$$M = \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix} \text{ with } b \in \mathbf{Z}/n\mathbf{Z} \quad \text{and} \quad d \in (\mathbf{Z}/n\mathbf{Z})^*.$$

Observe that $\#G(n) = n\varphi(n)$. We obtain an injective map

$$\sigma \mapsto M(\sigma) = \begin{pmatrix} 1 & 0 \\ b(\sigma) & d(\sigma) \end{pmatrix} \quad \text{of } G_{K/k} \hookrightarrow G(n),$$

which is immediately verified to be an injective homomorphism. The question arises, when is it an isomorphism? The next theorem gives an answer over some fields, applicable especially to the rational numbers.

Theorem 9.4. *Let k be a field. Let n be an odd positive integer prime to the characteristic, and assume that $[k(\boldsymbol{\mu}_n) : k] = \varphi(n)$. Let $a \in k$, and suppose that for each prime $p|n$ the element a is not a p-th power in k. Let K be the splitting field of $X^n - a$ over k. Then the above homomorphism $\sigma \mapsto M(\sigma)$ is an isomorphism of $G_{K/k}$ with $G(n)$. The commutator group is* $\mathrm{Gal}(K/k(\boldsymbol{\mu}_n))$, *so $k(\boldsymbol{\mu}_n)$ is the maximal abelian subextension of K.*

Proof. This is a special case of the general theory of §11, and Exercise 39, taking into account the representation of $G_{K/k}$ in the group of matrices. One need only use the fact that the order of $G_{K/k}$ is $n\varphi(n)$, according to that exercise, and so $\#(G_{K/k}) = \#G(n)$, so $G_{K/k} = G(n)$. However, we shall given an independent proof as an example of techniques of Galois theory. We prove the theorem by induction.

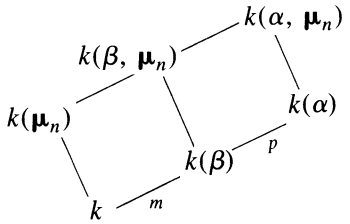
Suppose first $n = p$ is prime. Since $[k(\boldsymbol{\mu}_p) : k] = p - 1$ is prime to p, it follows that if α is a root of $X^p - a$, then $k(\alpha) \cap k(\boldsymbol{\mu}_p) = k$ because $[k(\alpha) : k] = p$. Hence $[K : k] = p(p - 1)$, so $G_{K/k} = G(p)$.

A direct computation of a commutator of elements in $G(n)$ for arbitrary n shows that the commutator subgroup is contained in the group of matrices

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, \; b \in \mathbf{Z}/n\mathbf{Z},$$

and so must be that subgroup because its factor group is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$ under the projection on the diagonal. This proves the theorem when $n = p$.

Now let $p \mid n$ and write $n = pm$. Then $[k(\boldsymbol{\mu}_m) : k] = \varphi(m)$, immediately from the hypothesis that $[k(\boldsymbol{\mu}_n) : k] = \varphi(n)$. Let α be a root of $X^n - a$, and let $\beta = \alpha^p$. Then β is a root of $X^m - a$, and by induction we can apply the theorem to $X^m - a$. The field diagram is as follows.



Since α has degree pm over k, it follows that α cannot have lower degree than p over $k(\beta)$, so $[k(\alpha) : k(\beta)] = p$ and $X^p - \beta$ is irreducible over $k(\beta)$. We apply the first part of the proof to $X^p - \beta$ over $k(\beta)$. The property concerning the maximal abelian subextension of the splitting field shows that

$$k(\alpha) \cap k(\beta, \boldsymbol{\mu}_n) = k(\beta).$$

Hence $[k(\alpha, \boldsymbol{\mu}_n) : k(\beta, \boldsymbol{\mu}_n)] = p$. By induction, $[k(\beta, \boldsymbol{\mu}_n) : k(\boldsymbol{\mu}_n)] = m$, again because of the maximal abelian subextension of the splitting field of $X^m - a$ over k. This proves that $[K : k] = n\varphi(n)$, whence $G_{K/k} = G(n)$, and the commutator statement has already been proved. This concludes the proof of Theorem 9.4.

Remarks. When n is even, there are some complications, because for instance $\mathbf{Q}(\sqrt{2})$ is contained in $\mathbf{Q}(\boldsymbol{\mu}_8)$, so there are dependence relations among the fields in question. The non-abelian extensions, as in Theorem 9.4, are of intrinsic interest because they constitute the first examples of such extensions that come to mind, but they arose in other important contexts. For instance, Artin used them to give a probabilistic model for the density of primes p such that 2 (say) is a primitive root mod p (that is, 2 generates the cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$. Instead of 2 he took any non-square integer $\neq \pm 1$. At first, Artin did not realize explicitly the above type of dependence, and so came to an answer that was off by some factor in some cases. Lehmer discovered the discrepancy by computations. As Artin then said, one has to multiply by the "obvious" factor which reflects the field dependencies. Artin never published his conjecture, but the matter is discussed in detail by Lang-Tate in the introduction to his collected papers (Addison-Wesley, Springer Verlag).

Similar conjectural probabilistic models were constructed by Lang-Trotter in connection with elliptic curves, and more generally with certain p-adic representations of the Galois group, in "Primitive points on elliptic curves", *Bull. AMS* **83** No. 2 (1977), pp. 289–292; and [LaT 75] (end of §14).

For further comments on the p-adic representations of Galois groups, see §14 and §15.

§10. GALOIS COHOMOLOGY

Let G be a group and A an abelian group which we write additively for the general remarks which we make, preceding our theorems. Let us assume that G operates on A, by means of a homomorphism $G \to \mathrm{Aut}(A)$. By a **1-cocycle** of G in A one means a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ with $\alpha_\sigma \in A$, satisfying the relations

$$\alpha_\sigma + \sigma\alpha_\tau = \alpha_{\sigma\tau}$$

for all $\sigma, \tau \in G$. If $\{\alpha_\sigma\}_{\sigma \in G}$ and $\{\beta_\sigma\}_{\sigma \in G}$ are 1-cocycles, then we can add them to get a 1-cocycle $\{\alpha_\sigma + \beta_\sigma\}_{\sigma \in G}$. It is then clear that 1-cocycles form a group, denoted by $Z^1(G, A)$. By a **1-coboundary** of G in A one means a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ such that there exists an element $\beta \in A$ for which $\alpha_\sigma = \sigma\beta - \beta$ for all $\sigma \in G$. It is then clear that a 1-coboundary is a 1-cocycle, and that the 1-coboundaries form a group, denoted by $B^1(G, A)$. The factor group

$$Z^1(G, A)/B^1(G, A)$$

is called the **first cohomology group** of G in A and is denoted by $H^1(G, A)$.

Remarks. Suppose G is cyclic. Let

$$\mathrm{Tr}_G\colon A \to A \text{ be the homomorphism } a \mapsto \sum_{\sigma \in G} \sigma(a).$$

Let γ be a generator of G. Let $(1 - \gamma)A$ be the subgroup of A consisting of all elements $a - \gamma(a)$ with $a \in A$. Then $(1 - \gamma)A$ is contained in $\ker \mathrm{Tr}_G$. The reader will verify as an exercise that there is an isomorphism

$$\ker \mathrm{Tr}_G/(1 - \gamma)A \approx H^1(G, A).$$

Then the next theorem for a cyclic group is just Hilbert's Theorem 90 of §6. *Cf.* also the cohomology of groups, Chapter XX, Exercise 4, for an even more general context.

Theorem 10.1. *Let K/k be a finite Galois extension with Galois group G. Then for the operation of G on K^* we have $H^1(G, K^*) = 1$, and for the operation of G on the additive group of K we have $H^1(G, K) = 0$. In other words, the first cohomology group is trivial in both cases.*

Proof. Let $\{\alpha_\sigma\}_{\sigma \in G}$ be a 1-cocycle of G in K^*. The multiplicative cocycle relation reads

$$\alpha_\sigma \alpha_\tau^\sigma = \alpha_{\sigma\tau}.$$

By the linear independence of characters, there exists $\theta \in K$ such that the element

$$\beta = \sum_{\tau \in G} \alpha_\tau \tau(\theta)$$

is $\neq 0$. Then

$$\sigma\beta = \sum_{\tau \in G} \alpha_\tau^\sigma \sigma\tau(\theta) = \sum_{\tau \in G} \alpha_{\sigma\tau} \alpha_\sigma^{-1} \sigma\tau(\theta)$$

$$= \alpha_\sigma^{-1} \sum_{\tau \in G} \alpha_{\sigma\tau} \sigma\tau(\theta) = \alpha_\sigma^{-1} \beta.$$

We get $\alpha_\sigma = \beta/\sigma\beta$, and using β^{-1} instead of β gives what we want.

For the additive part of the theorem, we find an element $\theta \in K$ such that the trace $\mathrm{Tr}(\theta)$ is not equal to 0. Given a 1-cocycle $\{\alpha_\sigma\}$ in the additive group of K, we let

$$\beta = \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} \alpha_\tau \tau(\theta).$$

It follows at once that $\alpha_\sigma = \beta - \sigma\beta$, as desired.

The next lemma will be applied to the non-abelian Kummer theory of the next section.

Lemma 10.2. (Sah). *Let G be a group and let E be a G-module. Let τ be in the center of G. Then $H^1(G, E)$ is annihilated by the map $x \mapsto \tau x - x$ on E. In particular, if this map is an automorphism of E, then $H^1(G, E) = 0$.*

Proof. Let f be a 1-cocycle of G in E. Then

$$f(\sigma) = f(\tau\sigma\tau^{-1}) = f(\tau) + \tau(f(\sigma\tau^{-1}))$$
$$= f(\tau) + \tau[f(\sigma) + \sigma f(\tau^{-1})].$$

Therefore

$$\tau f(\sigma) - f(\sigma) = -\sigma\tau f(\tau^{-1}) - f(\tau).$$

But $f(1) = f(1) + f(1)$ implies $f(1) = 0$, and

$$0 = f(1) = f(\tau\tau^{-1}) = f(\tau) + \tau f(\tau^{-1}).$$

This shows that $(\tau - 1)f(\sigma) = (\sigma - 1)f(\tau)$, so $(\tau - 1)f$ is a coboundary. This proves the lemma.

§11. NON-ABELIAN KUMMER EXTENSIONS

We are interested in the splitting fields of equations $X^n - a = 0$ when the n-th roots of unity are not contained in the ground field. More generally, we want to know roughly (or as precisely as possible) the Galois group of simultaneous equations of this type. For this purpose, we axiomatize the pattern of proof to an additive notation, which in fact makes it easier to see what is going on.

We fix an integer $N > 1$, and we let M range over positive integers dividing N. We let P be the set of primes dividing N. We let G be a group, and let:

A = G-module such that the isotropy group of any element of A is of finite index in G. We also assume that A is divisible by the primes $p|N$, that is

$$pA = A \qquad \text{for all } p \in P.$$

Γ = finitely generated subgroup of A such that Γ is pointwise fixed by G.

We assume that A_N is finite. Then $\frac{1}{N}\Gamma$ is also finitely generated. Note that

$$\frac{1}{N}\Gamma \supset A_N.$$

Example. For our purposes here, the above situation summarizes the properties which hold in the following situation. Let K be a finitely generated field over the rational numbers, or even a finite extension of the rational numbers. We let A be the multiplicative group of the algebraic closure K^a. We let $G = G_K$ be the Galois group $\mathrm{Gal}(K^a/K)$. We let Γ be a finitely generated subgroup of the multiplicative group K^*. Then all the above properties are satisfied. We see that $A_N = \mu_N$ is the group of N-th roots of unity. The group written $\frac{1}{N}\Gamma$ in additive notation is written $\Gamma^{1/N}$ in multiplicative notation.

Next we define the appropriate groups analogous to the Galois groups of Kummer theory, as follows. For any G-submodule B of A, we let:

$G(B)$ = image of G in $\mathrm{Aut}(B)$,

$G(N) = G(A_N)$ = image of G in $\mathrm{Aut}(A_N)$,

$H(N)$ = subgroup of G leaving A_N pointwise fixed,

$\mathrm{H}_\Gamma(M, N)$ (for $M|N$) = image of $H(N)$ in $\mathrm{Aut}\left(\frac{1}{M}\Gamma\right)$.

Then we have an exact sequence:

$$0 \to H_\Gamma(M, N) \to G\left(\frac{1}{M}\Gamma + A_N\right) \to G(N) \to 0.$$

Example. In the concrete case mentioned above, the reader will easily recognize these various groups as Galois groups. For instance, let A be the multiplicative group. Then we have the following lattice of field extensions with corresponding Galois groups:

$$G(\Gamma^{1/M}\boldsymbol{\mu}_N)\begin{cases} K(\boldsymbol{\mu}_N, \Gamma^{1/M}) \\ | \\ K(\boldsymbol{\mu}_N) \\ | \\ K \end{cases}\begin{matrix} \} H_\Gamma(M, N) \\ \\ \} G(N) \end{matrix}$$

In applications, we want to know how much degeneracy there is when we translate $K(\boldsymbol{\mu}_M, \Gamma^{1/M})$ over $K(\boldsymbol{\mu}_N)$ with $M|N$. This is the reason we play with the pair M, N rather than a single N.

Let us return to a general Kummer representation as above. We are interested especially in that part of $(\mathbf{Z}/N\mathbf{Z})^*$ contained in $G(N)$, namely the group of integers n (mod N) such that there is an element $[n]$ in $G(N)$ such that

$$[n]a = na \qquad \text{for all } a \in A_N.$$

Such elements are always contained in the center of $G(N)$, and are called **homotheties**.

Write

$$N = \prod p^{n(p)}$$

Let S be a subset of P. We want to make some non-degeneracy assumptions about $G(N)$. We call S the **special set**.

There is a product decomposition

$$(\mathbf{Z}/N\mathbf{Z})^* = \prod_{p|N} (\mathbf{Z}/p^{n(p)}\mathbf{Z})^*.$$

If $2|N$ we suppose that $2 \in S$. For each $p \in S$ we suppose that there is an integer $c(p) = p^{f(p)}$ with $f(p) \geqq 1$ such that

$$G(A_N) \supset \prod_{p \in S} U_{c(p)} \times \prod_{p \notin S} (\mathbf{Z}/p^{n(p)}\mathbf{Z})^*,$$

where $U_{c(p)}$ is the subgroup of $\mathbf{Z}(p^{n(p)})$ consisting of those elements $\equiv 1$ mod $c(p)$.

The product decomposition on the right is relative to the direct sum decomposition

$$A_N = \bigoplus_{p \mid N} A_{p^{n(p)}}.$$

The above assumption will be called the non-degeneracy assumption. The integers $c(p)$ measure the extent to which $G(A_N)$ is degenerate.

Under this assumption, we observe that

$$[2] \in G(A_M) \quad \text{if} \quad M \mid N \text{ and } M \text{ is not divisible by primes of } S;$$

$$[1 + c] \in G(A_M) \quad \text{if} \quad M \mid N \text{ and } M \text{ is divisible only by primes of } S,$$

where

$$c = c(S) = \prod_{p \in S} c(p).$$

We can then use $[2] - [1] = [1]$ and $[1 + c] - [1] = [c]$ in the context of Lemma 10.2, since $[1]$ and $[c]$ are in the center of G.

For any M we define

$$c(M) = \prod_{\substack{p \mid M \\ p \in S}} c(p).$$

Define

$$\Gamma' = \frac{1}{N} \Gamma \cap A^G$$

and the **exponent**

$$e(\Gamma'/\Gamma) = \text{smallest positive integer } e \text{ such that } e\Gamma' \subset \Gamma.$$

It is clear that degeneracy in the Galois group $H_\Gamma(M, N)$ defined above can arise from lots of roots of unity in the ground field, or at least degeneracy in the Galois group of roots of unity; and also if we look at an equation

$$X^M - a = 0,$$

from the fact that a is already highly divisible in K. This second degeneracy would arise from the exponent $e(\Gamma'/\Gamma)$, as can be seen by looking at the Galois group of the divisions of Γ. The next theorem shows that these are the only sources of degeneracy.

We have the abelian Kummer pairing for $M \mid N$,

$$H_\Gamma(M, N) \times \Gamma/M\Gamma \to A_M \quad \text{given by} \quad (\tau, x) \mapsto \tau y - y,$$

where y is any element such that $My = x$. The value of the pairing is indepen-

dent of the choice of y. Thus for $x \in \Gamma$, we have a homomorphism

$$\varphi_x : H_\Gamma(M, N) \to A_M$$

such that

$$\varphi_x(\tau) = \tau y - y, \qquad \text{where } My = x.$$

Theorem 11.1. *Let $M \mid N$. Let φ be the homomorphism*

$$\varphi : \Gamma \to \mathrm{Hom}(H_\Gamma(M, N), A_M)$$

and let Γ_φ be its kernel. Let $e_M(\Gamma) = \text{g.c.d.}\ (e(\Gamma'/\Gamma), M)$. Under the non-degeneracy assumption, we have

$$c(M)e_M(\Gamma)\Gamma_\varphi \subset M\Gamma.$$

Proof. Let $x \in \Gamma$ and suppose $\varphi_x = 0$. Let $My = x$. For $\sigma \in G$ let

$$y_\sigma = \sigma y - y.$$

Then $\{y_\sigma\}$ is a 1-cocycle of G in A_M, and by the hypothesis that $\varphi_x = 0$, this cocycle depends only on the class of σ modulo the subgroup of G leaving the elements of A_N fixed. In other words, we may view $\{y_\sigma\}$ as a cocycle of $G(N)$ in A_M. Let $c = c(N)$. By Lemma 10.2, it follows that $\{cy_\sigma\}$ splits as a cocycle of $G(N)$ in A_M. In other words, there exists $t_0 \in A_M$ such that

$$cy_\sigma = \sigma t_0 - t_0,$$

and this equation in fact holds for $\sigma \in G$. Let t be such that $ct = t_0$. Then

$$c\sigma y - cy = \sigma ct - cy,$$

whence $c(y - t)$ is fixed by all $\sigma \in G$, and therefore lies in $\frac{1}{N}\Gamma$. Therefore

$$e(\Gamma'/\Gamma)c(y - t) \in \Gamma.$$

We multiply both sides by M and observe that $cM(y - t) = cMy = cx$. This shows that

$$c(N)e(\Gamma'/\Gamma)\Gamma_\varphi \subset M\Gamma.$$

Since $\Gamma/M\Gamma$ has exponent M, we may replace $e(\Gamma'/\Gamma)$ by the greatest common divisor as stated in the theorem, and we can replace $c(N)$ by $c(M)$ to conclude the proof.

Corollary 11.2. *Assume that M is prime to $2(\Gamma' : \Gamma)$ and is not divisible by any primes of the special set S. Then we have an injection*

$$\varphi : \Gamma/M\Gamma \to \mathrm{Hom}(H_\Gamma(M, N), A_M).$$

If in addition Γ is free with basis $\{a_1, \ldots, a_r\}$, and we let $\varphi_i = \varphi_{a_i}$, then the map

$$H_\Gamma(M, N) \to A_M^{(r)} \quad \text{given by} \quad \tau \to (\varphi_1(\tau), \ldots, \varphi_r(\tau))$$

is injective. If A_M is cyclic of order M, this map is an isomorphism.

Proof. Under the hypotheses of the corollary, we have $c(M) = 1$ and $c_M(\Gamma) = 1$ in the theorem.

Example. Consider the case of Galois theory when A is the multiplicative group of K^a. Let $a_1, \ldots, a_r$ be elements of K^* which are multiplicatively independent. They generate a group as in the corollary. Furthermore, $A_M = \boldsymbol{\mu}_M$ is cyclic, so the corollary applies. If M is prime to $2(\Gamma' : \Gamma)$ and is not divisible by any primes of the special set S, *we have an isomorphism*

$$\varphi : \Gamma/M\Gamma \to \mathrm{Hom}(H_\Gamma(M, N), \boldsymbol{\mu}_M).$$

§12. ALGEBRAIC INDEPENDENCE OF HOMOMORPHISMS

Let A be an additive group, and let K be a field. Let $\lambda_1, \ldots, \lambda_n : A \to K$ be additive homomorphisms. We shall say that $\lambda_1, \ldots, \lambda_n$ are **algebraically dependent** (over K) if there exists a polynomial $f(X_1, \ldots, X_n)$ in $K[X_1, \ldots, X_n]$ such that for all $x \in A$ we have

$$f(\lambda_1(x), \ldots, \lambda_n(x)) = 0,$$

but such that f does not induce the zero function on $K^{(n)}$, i.e. on the direct product of K with itself n times. We know that with each polynomial we can associate a unique reduced polynomial giving the same function. If K is infinite, the reduced polynomial is equal to f itself. In our definition of dependence, we could as well assume that f is reduced.

A polynomial $f(X_1, \ldots, X_n)$ will be called **additive** if it induces an additive homomorphism of $K^{(n)}$ into K. Let $(Y) = (Y_1, \ldots, Y_n)$ be variables independent from (X). Let

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

where $X + Y$ is the componentwise vector addition. Then the total degree of g viewed as a polynomial in (X) with coefficients in $K[Y]$ is strictly less than the total degree of f, and similarly, its degree in each X_i is strictly less than the degree of f in each X_i. One sees this easily by considering the difference of monomials,

$$M_{(v)}(X + Y) - M_{(v)}(X) - M_{(v)}(Y)$$
$$= (X_1 + Y_1)^{v_1} \cdots (X_n + Y_n)^{v_n} - X_1^{v_1} \cdots X_n^{v_n} - Y_1^{v_1} \cdots Y_n^{v_n}.$$

A similar assertion holds for g viewed as a polynomial in (Y) with coefficients in $K[X]$.

If f is reduced, it follows that g is reduced. Hence if f is additive, it follows that g is the zero polynomial.

Example. Let K have characteristic p. Then in one variable, the map

$$\xi \mapsto a\xi^{p^m}$$

for $a \in K$ and $m \geqq 1$ is additive, and given by the additive polynomial aX^{p^m}. We shall see later that this is a typical example.

Theorem 12.1. (Artin). *Let $\lambda_1, \ldots, \lambda_n : A \to K$ be additive homomorphisms of an additive group into a field. If these homomorphisms are algebraically dependent over K, then there exists an additive polynomial*

$$f(X_1, \ldots, X_n) \neq 0$$

in $K[X]$ such that

$$f(\lambda_1(x), \ldots, \lambda_n(x)) = 0$$

for all $x \in A$.

Proof. Let $f(X) = f(X_1, \ldots, X_n) \in K[X]$ be a reduced polynomial of lowest possible degree such that $f \neq 0$ but for all $x \in A$, $f(\Lambda(x)) = 0$, where $\Lambda(x)$ is the vector $(\lambda_1(x), \ldots, \lambda_n(x))$. We shall prove that f is additive.

Let $g(X, Y) = f(X + Y) - f(X) - f(Y)$. Then

$$g(\Lambda(x), \Lambda(y)) = f(\Lambda(x + y)) - f(\Lambda(x)) - f(\Lambda(y)) = 0$$

for all $x, y \in A$. We shall prove that g induces the zero function on $K^{(n)} \times K^{(n)}$. Assume otherwise. We have two cases.

Case 1. We have $g(\xi, \Lambda(y)) = 0$ for all $\xi \in K^{(n)}$ and all $y \in A$. By hypothesis, there exists $\xi' \in K^{(n)}$ such that $g(\xi', Y)$ is not identically 0. Let $P(Y) = g(\xi', Y)$. Since the degree of g in (Y) is strictly smaller than the degree of f, we have a contradiction.

Case 2. There exist $\xi' \in K^{(n)}$ and $y' \in A$ such that $g(\xi', \Lambda(y')) \neq 0$. Let $P(X) = g(X, \Lambda(y'))$. Then P is not the zero polynomial, but $P(\Lambda(x)) = 0$ for all $x \in A$, again a contradiction.

We conclude that g induces the zero function on $K^{(n)} \times K^{(n)}$, which proves what we wanted, namely that f is additive.

We now consider additive polynomials more closely.

Let f be an additive polynomial in n variables over K, and assume that f is reduced. Let

$$f_i(X_i) = f(0, \ldots, X_i, \ldots, 0)$$

with X_i in the i-th place, and zeros in the other components. By additivity, it follows that

$$f(X_1, \ldots, X_n) = f_1(X_1) + \cdots + f_n(X_n)$$

because the difference of the right-hand side and left-hand side is a reduced polynomial taking the value 0 on $K^{(n)}$. Furthermore, each f_i is an additive polynomial in one variable. We now study such polynomials.

Let $f(X)$ be a reduced polynomial in one variable, which induces a linear map of K into itself. Suppose that there occurs a monomial $a_r X^r$ in f with coefficient $a_r \neq 0$. Then the monomials of degree r in

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

are given by

$$a_r(X + Y)^r - a_r X^r - a_r Y^r.$$

We have already seen that g is identically 0. Hence the above expression is identically 0. Hence the polynomial

$$(X + Y)^r - X^r - Y^r$$

is the zero polynomial. It contains the term $rX^{r-1}Y$. Hence if $r > 1$, our field must have characteristic p and r is divisible by p. Write $r = p^m s$ where s is prime to p. Then

$$0 = (X + Y)^r - X^r - Y^r = (X^{p^m} + Y^{p^m})^s - (X^{p^m})^s - (Y^{p^m})^s.$$

Arguing as before, we conclude that $s = 1$.

Hence if f is an additive polynomial in one variable, we have

$$f(X) = \sum_{v=0}^{m} a_v X^{p^v},$$

with $a_v \in K$. In characteristic 0, the only additive polynomials in one variable are of type aX with $a \in K$.

As expected, we define $\lambda_1, \ldots, \lambda_n$ to be **algebraically independent** if, whenever f is a reduced polynomial such that $f(\Lambda(x)) = 0$ for all $x \in K$, then f is the zero polynomial.

We shall apply Theorem 12.1 to the case when $\lambda_1, \ldots, \lambda_n$ are automorphisms of a field, and combine Theorem 12.1 with the theorem on the linear independence of characters.

Theorem 12.2. *Let K be an infinite field, and let $\sigma_1, \ldots, \sigma_n$ be the distinct elements of a finite group of automorphisms of K. Then $\sigma_1, \ldots, \sigma_n$ are algebraically independent over K.*

Proof. (Artin). In characteristic 0, Theorem 12.1 and the linear independence of characters show that our assertion is true. Let the characteristic be $p > 0$, and assume that $\sigma_1, \ldots, \sigma_n$ are algebraically dependent.

There exists an additive polynomial $f(X_1, \ldots, X_n)$ in $K[X]$ which is reduced, $f \neq 0$, and such that

$$f(\sigma_1(x), \ldots, \sigma_n(x)) = 0$$

for all $x \in K$. By what we saw above, we can write this relation in the form

$$\sum_{i=1}^{n} \sum_{r=1}^{m} a_{ir} \sigma_i(x)^{p^r} = 0$$

for all $x \in K$, and with not all coefficients a_{ir} equal to 0. Therefore by the linear independence of characters, the automorphisms

$$\{\sigma_i^{p^r}\} \qquad \text{with} \quad i = 1, \ldots, n \quad \text{and} \quad r = 1, \ldots, m$$

cannot be all distinct. Hence we have

$$\sigma_i^{p^r} = \sigma_j^{p^s}$$

with either $i \neq j$ or $r \neq s$. Say $r \leqq s$. For all $x \in K$ we have

$$\sigma_i(x)^{p^r} = \sigma_j(x)^{p^s}.$$

Extracting p-th roots in characteristic p is unique. Hence

$$\sigma_i(x) = \sigma_j(x)^{p^{s-r}} = \sigma_j(x^{p^{s-r}})$$

for all $x \in K$. Let $\sigma = \sigma_j^{-1}\sigma_i$. Then

$$\sigma(x) = x^{p^{s-r}}$$

for all $x \in K$. Taking $\sigma^n = \mathrm{id}$ shows that

$$x = x^{p^{n(s-r)}}$$

for all $x \in K$. Since K is infinite, this can hold only if $s = r$. But in that case, $\sigma_i = \sigma_j$, contradicting the fact that we started with distinct automorphisms.

§13. THE NORMAL BASIS THEOREM

Theorem 13.1. *Let K/k be a finite Galois extension of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the elements of the Galois group G. Then there exists an element $w \in K$ such that $\sigma_1 w, \ldots, \sigma_n w$ form a basis of K over k.*

Proof. We prove this here only when k is infinite. The case when k is finite can be proved later by methods of linear algebra, as an exercise.

For each $\sigma \in G$, let X_σ be a variable, and let $t_{\sigma,\tau} = X_{\sigma^{-1}\tau}$. Let $X_i = X_{\sigma_i}$. Let

$$f(X_1, \ldots, X_n) = \det(t_{\sigma_i, \sigma_j}).$$

Then f is not identically 0, as one sees by substituting 1 for X_{id} and 0 for X_σ if $\sigma \neq \mathrm{id}$. Since k is infinite, f is reduced. Hence the determinant will not be 0 for all $x \in K$ if we substitute $\sigma_i(x)$ for X_i in f. Hence there exists $w \in K$ such that

$$\det(\sigma_i^{-1}\sigma_j(w)) \neq 0.$$

Suppose $a_1, \ldots, a_n \in k$ are such that

$$a_1\sigma_1(w) + \cdots + a_n\sigma_n(w) = 0.$$

Apply σ_i^{-1} to this relation for each $i = 1, \ldots, n$. Since $a_j \in k$ we get a system of linear equations, regarding the a_j as unknowns. Since the determinant of the coefficients is $\neq 0$, it follows that

$$a_j = 0 \qquad \text{for} \quad j = 1, \ldots, n$$

and hence that w is the desired element.

Remark. In terms of representations as in Chapters III and XVIII, the normal basis theorem says that the representation of the Galois group on the additive group of the field is the regular representation. One may also say that K is free of dimension 1 over the group ring $k[G]$. Such a result may be viewed as the first step in much more subtle investigations having to do with algebraic number theory. Let K be a number field (finite extension of $\mathbf{Q}$) and let $\mathfrak{o}_K$ be its ring of algebraic integers, which will be defined in Chapter VII, §1. Then one may ask for a description of $\mathfrak{o}_K$ as a $\mathbf{Z}[G]$ module, which is a much more difficult problem. For fundamental work about this problem, see A. Fröhlich, *Galois Module Structures of Algebraic Integers*, Ergebnisse der Math. 3 Folge Vol. 1, Springer Verlag (1983). See also the reference [CCFT 91] given at the end of Chapter III, §1.

§14. INFINITE GALOIS EXTENSIONS

Although we have already given some of the basic theorems of Galois theory already for possibly infinite extensions, the non-finiteness did not really appear in a substantial way. We now want to discuss its role more extensively.

Let K/k be a Galois extension with group G. For each finite Galois subextension F, we have the Galois groups $G_{K/F}$ and $G_{F/k}$. Put $H = G_{K/F}$. Then H has finite index, equal to $\#(G_{F/k}) = [F : k]$. This just comes as a special case of the general Galois theory. We have a canonical homomorphism

$$G \to G/H = G_{F/k}.$$

Therefore by the universal property of the inverse limit, we obtain a homomorphism

$$G \to \lim_{H \in \mathfrak{F}} G/H,$$

where the limit is taken for H in the family $\mathfrak{F}$ of Galois groups $G_{K/F}$ as above.

Theorem 14.1. *The homomorphism $G \to \lim G/H$ is an isomorphism.*

Proof. First the kernel is trivial, because if σ is in the kernel, then σ restricted to every finite subextension of K is trivial, and so is trivial on K. Recall that an element of the inverse limit is a family $\{\sigma_H\}$ with $\sigma_H \in G/H$, satisfying a certain compatibility condition. This compatibility condition means that we may define an element σ of G as follows. Let $\alpha \in K$. Then α is contained in some finite Galois extension $F \subset K$. Let $H = \mathrm{Gal}(K/F)$. Let $\sigma\alpha = \sigma_H\alpha$. The compatibility condition means that $\sigma_H\alpha$ is independent of the choice of F. Then it is immediately verified that σ is an automorphism of K over k, which maps to each σ_H in the canonical map of G into G/H. Hence the map $G \to \varprojlim G/H$ is surjective, thereby proving the theorem.

Remark. For the topological interpretation, see Chapter I, Theorem 10.1, and Exercise 43.

Example. Let $\boldsymbol{\mu}[p^\infty]$ be the union of all groups of roots of unity $\boldsymbol{\mu}[p^n]$, where p is a prime and $n = 1, 2, \ldots$ ranges over the positive integers. Let $K = \mathbf{Q}(\boldsymbol{\mu}[p^\infty])$. Then K is an abelian infinite extension of $\mathbf{Q}$. Let $\mathbf{Z}_p$ be the ring of p-adic integers, and $\mathbf{Z}_p^*$ the group of units. From §3, we know that $(\mathbf{Z}/p^n\mathbf{Z})^*$ is isomorphic to $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}[p^n]/\mathbf{Q}))$. These isomorphisms are compatible in the tower of p-th roots of unity, so we obtain an isomorphism

$$\mathbf{Z}_p^* \to \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}[p^\infty]/\mathbf{Q})).$$

Towers of cyclotomic fields have been extensively studied by Iwasawa. Cf. a systematic exposition and bibliography in [La 90].

For other types of representations in a group $GL_2(\mathbf{Z}_p)$, see Serre [Se 68], [Se 72], Shimura [Shi 71], and Lang-Trotter [LaT 75]. One general framework in which the representation of Galois groups on roots of unity can be seen has to do with commutative algebraic groups, starting with elliptic curves. Specifically, consider an equation

$$y^2 = 4x^3 - g_2x - g_3$$

with $g_2, g_3 \in \mathbf{Q}$ and non-zero discriminant: $\Delta = g_2^3 - 27g_3^2 \neq 0$. The set of solutions together with a point at infinity is denoted by E. From complex analysis (or by purely algebraic means), one sees that if K is an extension of $\mathbf{Q}$, then the set of solutions $E(K)$ with $x, y \in K$ and ∞ form a group, called the group of rational points of E in K. One is interested in the torsion group, say $E(\mathbf{Q}^a)_{\text{tor}}$ of points in the algebraic closure, or for a given prime p, in the group $E(\mathbf{Q}^a)[p^r]$ and $E(\mathbf{Q}^a)[p^\infty]$. As an abelian group, there is an isomorphism

$$E(\mathbf{Q}^a)[p^r] \approx (\mathbf{Z}/p^r\mathbf{Z}) \times (\mathbf{Z}/p^r\mathbf{Z}),$$

so the Galois group operates on the points of order p^r via a representation in $GL_2(\mathbf{Z}/p^r\mathbf{Z})$, rather than $GL_1(\mathbf{Z}/p^r\mathbf{Z}) = (\mathbf{Z}/p^r\mathbf{Z})^*$ in the case of roots of unity. Passing to the inverse limit, one obtains a representation of $\text{Gal}(\mathbf{Q}^a/\mathbf{Q}) = G_{\mathbf{Q}}$ in $GL_2(\mathbf{Z}_p)$. One of Serre's theorems is that the image of $G_{\mathbf{Q}}$ in $GL_2(\mathbf{Z}_p)$ is a subgroup of finite index, equal to $GL_2(\mathbf{Z}_p)$ for all but a finite number of primes p, if $\text{End}_{\mathbf{C}}(E) = \mathbf{Z}$.

More generally, using freely the language of algebraic geometry, when A is a commutative algebraic group, say with coefficients in $\mathbf{Q}$, then one may consider its group of points $A(\mathbf{Q}^a)_{\text{tor}}$, and the representation of $G_{\mathbf{Q}}$ in a similar way. Developing the notions to deal with these situations leads into algebraic geometry.

Instead of considering cyclotomic extensions of a ground field, one may also consider extensions of cyclotomic fields. The following conjecture is due to Shafarevich. See the references at the end of §7.

Conjecture 14.2. *Let $k_0 = \mathbf{Q}(\mu)$ be the compositum of all cyclotomic extensions of $\mathbf{Q}$ in a given algebraic closure $\mathbf{Q}^a$. Let k be a finite extension of k_0. Let $G_k = \text{Gal}(\mathbf{Q}^a/k)$. Then G_k is isomorphic to the completion of a free group on countably many generators.*

If G is the free group, then we recall that the completion is the inverse limit $\varprojlim G/H$, taken over all normal subgroups H of finite index. Readers should view this conjecture as being in analogy to the situation with Riemann surfaces, as mentioned in Example 9 of §2. It would be interesting to investigate the extent to which the conjecture remains valid if $\mathbf{Q}(\mu)$ is replaced by $\mathbf{Q}(A(\mathbf{Q}^a)_{\text{tor}})$, where A is an elliptic curve. For some results about free groups occurring as Galois groups, see also Wingberg [Wi 91].

Bibliography

[La 90] S. LANG, *Cyclotomic Fields I and II*, Second Edition, Springer Verlag, 1990 (Combined edition from the first editions, 1978, 1980)

[LaT 75] S. LANG and H. TROTTER, *Distribution of Frobenius Elements in GL_2-Extensions of the Rational Numbers*, Springer Lecture Notes **504** (1975)

[Se 68] J.-P. SERRE, *Abelian l-adic Representations and Elliptic Curves*, Benjamin, 1968

[Se 72] J.-P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), pp. 259–331

[Shi 71] G. SHIMURA, *Introduction to the arithmetic theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971

[Wi 91] K. WINGBERG, On Galois groups of p-closed algebraic number fields with restricted ramification, I, *J. reine angew. Math.* **400** (1989), pp. 185–202; and II, *ibid.*, **416** (1991), pp. 187–194

§15. THE MODULAR CONNECTION

This final section gives a major connection between Galois theory and the theory of modular forms, which has arisen since the 1960s.

One fundamental question is whether given a finite group G, there exists a Galois extension K of $\mathbf{Q}$ whose Galois group is G. In Exercise 23 you will prove this when G is abelian.

Already in the nineteenth century, number theorists realized the big difference between abelian and non-abelian extensions, and started understanding abelian extensions. Kronecker stated and gave what are today considered incomplete arguments that every finite abelian extension of $\mathbf{Q}$ is contained in some extension $\mathbf{Q}(\zeta)$, where ζ is a root of unity. The difficulty lay in the peculiarities of the prime 2. The trouble was fixed by Weber at the end of the nineteenth century. Note that the trouble with 2 has been systematic since then. It arose in Artin's conjecture about densities of primitive roots as mentioned in the remarks after Theorem 9.4. It arose in the Grunwald theorem of class field theory (corrected by Wang, cf. Artin-Tate [ArT 68], Chapter 10). It arose in Shafarevich's proof that given a solvable group, there exists a Galois extension of $\mathbf{Q}$ having that group as Galois group, mentioned at the end of §7.

Abelian extensions of a number field F are harder to describe than over the rationals, and the fundamental theory giving a description of such extensions is called class field theory (see the above reference). I shall give one significant example exhibiting the flavor. Let R_F be the ring of algebraic integers in F. It can be shown that R_F is a Dedekind ring. (*Cf.* [La 70], Chapter I, §6, Theorem 2.) Let P be a prime ideal of R_F. Then $P \cap \mathbf{Z} = (p)$ for some prime number p.

Furthermore, R_F/P is a finite field with q elements. Let K be a finite Galois extension of F. It will be shown in Chapter VII that there exists a prime Q of R_K such that $Q \cap R_F = P$. Furthermore, there exists an element

$$\mathrm{Fr}_Q \in G = \mathrm{Gal}(K/F)$$

such that $\mathrm{Fr}_Q(Q) = Q$ and for all $\alpha \in R_K$ we have

$$\mathrm{Fr}_Q \alpha \equiv \alpha^q \bmod Q.$$

We call Fr_Q a **Frobenius element** in the Galois group G associated with Q. (See Chapter VII, Theorem 2.9.) Furthermore, for all but a finite number of Q, two such elements are conjugate to each other in G. We denote any of them by Fr_P. If G is abelian, then there is only one element Fr_P in the Galois group.

Theorem 15.1. *There exists a unique finite abelian extension K of F having the following property. If P_1, P_2 are prime ideals of R_F, then $\mathrm{Fr}_{P_1} = \mathrm{Fr}_{P_2}$ if and only if there is an element α of K such that $\alpha P_1 = P_2$.*

In a similar but more complicated manner, one can characterize all abelian extensions of F. This theory is known as class field theory, developed by Kronecker, Weber, Hilbert, Takagi, and Artin. The main statement concerning the Frobenius automorphism as above is Artin's Reciprocity Law. Artin-Tate's notes give a cohomological account of class field theory. My *Algebraic Number Theory* gives an account following Artin's first proof dating back to 1927, with later simplifications by Artin himself. Both techniques are valuable to know.

Cyclotomic extensions should be viewed in the light of Theorem 15.1. Indeed, let $K = \mathbf{Q}(\zeta)$, where ζ is a primitive n-th root of unity. For a prime $p \nmid n$, we have the Frobenius automorphism Fr_p, whose effect on ζ is $\mathrm{Fr}_p(\zeta) = \zeta^p$. Then

$$\mathrm{Fr}_{p_1} = \mathrm{Fr}_{p_2} \quad \text{if and only if} \quad p_1 \equiv p_2 \bmod n.$$

To encompass both Theorem 15.1 and the cyclotomic case in one framework, one has to formulate the result of class field theory for generalized ideal classes, not just the ordinary ones when two ideals are equivalent if and only if they differ multiplicatively by a non-zero field element. See my *Algebraic Number Theory* for a description of these generalized ideal classes.

The non-abelian case is much more difficult. I shall indicate briefly a special case which gives some of the flavor of what goes on. The problem is to do for non-abelian extensions what Artin did for abelian extensions. Artin went as far as saying that the problem was not to give proofs but to formulate what was to be proved. The insight of Langlands and others in the sixties shows that actually Artin was mistaken. The problem lies in both. Shimura made several computations in this direction involving "modular forms" [Sh 66]. Langlands gave a number of conjectures relating Galois groups with "automorphic forms", which showed that the answer lay in deeper theories, whose formulations, let alone their proofs, were difficult. Great progress was made in the seventies by Serre and Deligne, who proved a first case of Langland's conjecture [DeS 74].

The study of non-abelian Galois groups occurs via their linear "representations". For instance, let l be a prime number. We can ask whether $GL_n(\mathbf{F}_l)$, or $GL_2(\mathbf{F}_l)$, or $PGL_2(\mathbf{F}_l)$ occurs as a Galois group over $\mathbf{Q}$, and "how". The problem is to find natural objects on which the Galois group operates as a linear map, such that we get in a natural way an isomorphism of this Galois group with one of the above linear groups. The theories which indicate in which direction to find such objects are much beyond the level of this course, and lie in the theory of modular functions, involving both analysis and algebra, which form a background for the number theoretic applications. Again I pick a special case to give the flavor.

Let K be a finite Galois extension of $\mathbf{Q}$, with Galois group

$$G = \mathrm{Gal}(K/\mathbf{Q}).$$

Let

$$\rho\colon G \to GL_2(\mathbf{F}_l)$$

be a homomorphism of G into the group of 2×2 matrices over the finite field $\mathbf{F}_l$ for some prime l. Such a homomorphism is called a **representation** of G. From elementary linear algebra, if

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a 2×2 matrix, we have its trace and determinant defined by

$$\mathrm{tr}(M) = a + d \quad \text{and} \quad \det M = ad - bc.$$

Thus we can take the trace and determinant $\mathrm{tr}\ \rho(\sigma)$ and $\det \rho(\sigma)$ for $\sigma \in G$.

Consider the infinite product with a variable q:

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} a_n q^n.$$

The coefficients a_n are integers, and $a_1 = 1$.

Theorem 15.2. *For each prime l there exists a unique Galois extension K of $\mathbf{Q}$, with Galois group G, and an injective homomorphism*

$$\rho\colon G \to GL_2(\mathbf{F}_l)$$

having the following property. For all but a finite number of primes p, if a_p is the coefficient of q^p in $\Delta(q)$, then we have

$$\mathrm{tr}\ \rho(\mathrm{Fr}_p) \equiv a_p \bmod l \quad \text{and} \quad \det \rho(\mathrm{Fr}_p) \equiv p^{11} \bmod l.$$

Furthermore, for all primes $l \neq 2, 3, 5, 7, 23, 691$, the image $\rho(G)$ in $GL_2(\mathbf{F}_l)$ consists of those matrices $M \in GL_2(\mathbf{F}_l)$ such that $\det M$ *is an eleventh power in $\mathbf{F}_l^*$.*

The above theorem was conjectured by Serre in 1968 [Se 68]. A proof of the existence as in the first statement was given by Deligne [De 68]. The second statement, describing how big the Galois group actually is in the group of matrices $GL_2(\mathbf{F}_l)$ is due to Serre and Swinnerton-Dyer [Se 72], [SwD 73].

The point of $\Delta(q)$ is that if we put $q = e^{2\pi iz}$, where z is a variable in the upper half-plane, then Δ is a modular form of weight 12. For definitions and an introduction, see the last chapter of [Se 73], [La 73], [La 76], and the following comments. The general result behind Theorem 15.2 for modular forms of weight $\geqq 2$ was given by Deligne [De 73]. For weight 1, it is due to Deligne-Serre [DeS 74]. We summarize the situation as follows.

Let N be a positive integer. To N we associate the subgroups

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$$

of $SL_2(\mathbf{Z})$ defined by the conditions for a matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$:

$\alpha \in \Gamma(N)$ if and only if $a \equiv d \equiv 1 \bmod N$ and $b \equiv c \equiv 0 \bmod N$;

$\alpha \in \Gamma_1(N)$ if and only if $a \equiv d \equiv 1 \bmod N$ and $c \equiv 0 \bmod N$;

$\alpha \in \Gamma_0(N)$ if and only if $c \equiv 0 \bmod N$.

Let f be a function on the upper half-plane $\mathfrak{H} = \{z \in \mathbf{C}, \operatorname{Im}(z) > 0\}$. Let k be an integer. For

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{R}),$$

define $f \circ [\gamma]_k$ (an operation on the right) by

$$f \circ [\gamma]_k(z) = (cz + d)^{-k} f(\gamma z) \quad \text{where} \quad \gamma z = \frac{az + b}{cz + d}.$$

Let Γ be a subgroup of $SL_2(\mathbf{Z})$ containing $\Gamma(N)$. We define f to be **modular of weight k on Γ** if:

$\mathbf{M_k}$ 1. f is holomorphic on $\mathfrak{H}$;

$\mathbf{M_k}$ 2. f is holomorphic at the cusps, meaning that for all $\alpha \in SL_2(\mathbf{Z})$, the function $f \circ [\alpha]_k$ has a power series expansion

$$f \circ [\alpha]_k(z) = \sum_{n=0}^{\infty} a_n e^{2\pi inz/N};$$

$\mathbf{M_k}$ 3. We have $f \circ [\gamma]_k = f$ for all $\gamma \in \Gamma$.

One says that f is **cuspidal** if in **$\mathbf{M_k}$ 2** the power series has a zero; that is, the power starts with $n \geqq 1$.

Suppose that f is modular of weight k on $\Gamma(N)$. Then f is modular on $\Gamma_1(N)$ if and only if $f(z+1) = f(z)$, or equivalently f has an expansion of the form

$$f(z) = f_\infty(q_z) = \sum_{n=0}^{\infty} a_n q^n \quad \text{where} \quad q = q_z = e^{2\pi i z}.$$

This power series is called the q-**expansion** of f.

Suppose f has weight k on $\Gamma_1(N)$. If $\gamma \in \Gamma_0(N)$ and γ is the above written matrix, then $f \circ [\gamma]_k$ depends only on the image of d in $(\mathbf{Z}/N\mathbf{Z})^*$, and we then denote $f \circ [\gamma]_k$ by $f \circ [d]_k$. Let

$$\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$$

be a homomorphism (also called a **Dirichlet character**). One says that ε is **odd** if $\varepsilon(-1) = -1$, and **even** if $\varepsilon(-1) = 1$. One says that f is **modular of type** (k, ε) on $\Gamma_0(N)$ if f has weight k on $\Gamma_1(N)$, and

$$f \circ [d]_k = \varepsilon(d) f \quad \text{for all} \quad d \in (\mathbf{Z}/N\mathbf{Z})^*.$$

It is possible to define an algebra of operators on the space of modular forms of given type. This requires more extensive background, and I refer the reader to [La 76] for a systematic exposition. Among all such forms, it is then possible to distinguish some of them which are eigenvectors for this Hecke algebra, or, as one says, eigenfunctions for this algebra. One may then state the Deligne-Serre theorem as follows.

Let $f \neq 0$ be a modular form of type $(1, \varepsilon)$ on $\Gamma_0(N)$, so f has weight 1. Assume that ε is odd. Assume that f is an eigenfunction of the Hecke algebra, with q-expansion $f_\infty = \sum a_n q^n$, normalized so that $a_1 = 1$. Then there exists a unique finite Galois extension K of $\mathbf{Q}$ with Galois group G, and a representation $\rho\colon G \to GL_2(\mathbf{C})$ (actually an injective homomorphism), such that for all primes $p \nmid N$ the characteristic polynomial of $\rho(\mathrm{Fr}_p)$ is

$$X^2 - a_p X + \varepsilon(p).$$

The representation ρ is irreducible if and only if f is cuspidal.

Note that the representation ρ has values in $GL_2(\mathbf{C})$. For extensive work of Serre and his conjectures concerning representations of Galois groups in $GL_2(\mathbf{F})$ when $\mathbf{F}$ is a finite field, see [Se 87]. Roughly speaking, the general philosophy started by a conjecture of Taniyama-Shimura and the Langlands conjectures is that everything in sight is "modular". Theorem 15.2 and the Deligne-Serre theorem are prototypes of results in this direction. For "modular" representations in $GL_2(\mathbf{F})$, when $\mathbf{F}$ is a finite field, Serre's conjectures have been proved, mostly by Ribet [Ri 90]. As a result, following an idea of Frey, Ribet also showed how the Taniyama-Shimura conjecture implies Fermat's last theorem [Ri 90b]. Note that Serre's conjectures that certain representations in $GL_2(\mathbf{F})$ are modular imply the Taniyama-Shimura conjecture.

Bibliography

[ArT 68] E. ARTIN and J. TATE, *Class Field Theory*, Benjamin-Addison-Wesley, 1968 (reprinted by Addison-Wesley, 1991)

[De 68] P. DELIGNE, Formes modulaires et représentations l-adiques, *Séminaire Bourbaki* 1968–1969, exp. No. 355

[De 73] P. DELIGNE, Formes modulaires et représentations de $GL(2)$, *Springer Lecture Notes* **349** (1973), pp. 55–105

[DeS 74] P. DELIGNE and J. P. SERRE, Formes modulaires de poids 1, *Ann. Sci. ENS* **7** (1974), pp. 507–530

[La 70] S. LANG, *Algebraic Number Theory*, Springer Verlag, reprinted from Addison-Wesley (1970)

[La 73] S. LANG, *Elliptic functions*, Springer Verlag, 1973

[La 76] S. LANG, *Introduction to modular forms*, Springer Verlag, 1976

[Ri 90a] K. RIBET, On modular representations of $\mathrm{Gal}(\overline{Q}/Q)$ arising from modular forms, *Invent. Math.* **100** (1990), pp. 431–476

[Ri 90b] K. RIBET, From the Taniyama-Shimura conjecture to Fermat's last theorem, *Annales de la Fac. des Sci. Toulouse* (1990), pp. 116–139

[Se 68] J.-P. SERRE, Une interprétation des congruences relatives à la fonction de Ramanujan, *Séminaire Delange-Pisot-Poitou*, 1967–1968

[Se 72] J.-P. SERRE, Congruences et formes modulaires (d'après Swinnerton-Dyer), *Séminaire Bourbaki*, 1971–1972

[Se 73] J.-P. SERRE, *A course in arithmetic*, Springer Verlag, 1973

[Se 87] J.-P. SERRE, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{Q}/Q)$, *Duke Math. J.* **54** (1987), pp. 179–230

[Shi 66] G. SHIMURA, A reciprocity law in non-solvable extensions, *J. reine angew. Math.* **221** (1966), pp. 209–220

[Shi 71] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, 1971

[SwD 73] H. P. SWINNERTON-DYER, On l-adic representations and congruences for coefficients of modular forms, (Antwerp conference) *Springer Lecture Notes* **350** (1973)

EXERCISES

1. What is the Galois group of the following polynomials?
   (a) $X^3 - X - 1$ over $\mathbf{Q}$.
   (b) $X^3 - 10$ over $\mathbf{Q}$.
   (c) $X^3 - 10$ over $\mathbf{Q}(\sqrt{2})$.
   (d) $X^3 - 10$ over $\mathbf{Q}(\sqrt{-3})$.
   (e) $X^3 - X - 1$ over $\mathbf{Q}(\sqrt{-23})$.
   (f) $X^4 - 5$ over $\mathbf{Q}$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(i)$.
   (g) $X^4 - a$ where a is any integer $\neq 0$, $\neq \pm 1$ and is square free. Over $\mathbf{Q}$.

(h) $X^3 - a$ where a is any square-free integer $\geqq 2$. Over $\mathbf{Q}$.
(i) $X^4 + 2$ over $\mathbf{Q}$, $\mathbf{Q}(i)$.
(j) $(X^2 - 2)(X^2 - 3)(X^2 - 5)(X^2 - 7)$ over $\mathbf{Q}$.
(k) Let $p_1, \ldots, p_n$ be distinct prime numbers. What is the Galois group of $(X^2 - p_1) \cdots (X^2 - p_n)$ over $\mathbf{Q}$?
(l) $(X^3 - 2)(X^3 - 3)(X^2 - 2)$ over $\mathbf{Q}(\sqrt{-3})$.
(m) $X^n - t$, where t is transcendental over the complex numbers $\mathbf{C}$ and n is a positive integer. Over $\mathbf{C}(t)$.
(n) $X^4 - t$, where t is as before. Over $\mathbf{R}(t)$.

2. Find the Galois groups over $\mathbf{Q}$ of the following polynomials.
(a) $X^3 + X + 1$ (b) $X^3 - X + 1$ (g) $X^3 + X^2 - 2X - 1$
(c) $X^3 + 2X + 1$ (d) $X^3 - 2X + 1$
(e) $X^3 - X - 1$ (f) $X^3 - 12X + 8$

3. Let $k = \mathbf{C}(t)$ be the field of rational functions in one variable. Find the Galois group over k of the following polynomials:
(a) $X^3 + X + t$ (b) $X^3 - X + t$
(c) $X^3 + tX + 1$ (d) $X^3 - 2tX + t$
(e) $X^3 - X - t$ (f) $X^3 + t^2X - t^3$

4. Let k be a field of characteristic $\neq 2$. Let $c \in k$, $c \notin k^2$. Let $F = k(\sqrt{c})$. Let $\alpha = a + b\sqrt{c}$ with $a, b \in k$ and not both $a, b = 0$. Let $E = F(\sqrt{\alpha})$. Prove that the following conditions are equivalent.
(1) E is Galois over k.
(2) $E = F(\sqrt{\alpha'})$, where $\alpha' = a - b\sqrt{c}$.
(3) Either $\alpha\alpha' = a^2 - cb^2 \in k^2$ or $c\alpha\alpha' \in k^2$.
Show that when these conditions are satisfied, then E is cyclic over k of degree 4 if and only if $c\alpha\alpha' \in k^2$.

5. Let k be a field of characteristic $\neq 2, 3$. Let $f(X)$, $g(X) = X^2 - c$ be irreducible polynomials over k, of degree 3 and 2 respectively. Let D be the discriminant of f. Assume that
$$[k(D^{1/2}) : k] = 2 \quad \text{and} \quad k(D^{1/2}) \neq k(c^{1/2}).$$
Let α be a root of f and β a root of g in an algebraic closure. Prove:
(a) The splitting field of fg over k has degree 12.
(b) Let $\gamma = \alpha + \beta$. Then $[k(\gamma) : k] = 6$.

6. (a) Let K be cyclic over k of degree 4, and of characteristic $\neq 2$. Let $G_{K/k} = \langle\sigma\rangle$. Let E be the unique subfield of K of degree 2 over k. Since $[K : E] = 2$, there exists $\alpha \in K$ such that $\alpha^2 = \gamma \in E$ and $K = E(\alpha)$. Prove that there exists $z \in E$ such that
$$z\sigma z = -1, \quad \sigma\alpha = z\alpha, \quad z^2 = \sigma\gamma/\gamma.$$
(b) Conversely, let E be a quadratic extension of k and let $G_{E/k} = \langle\tau\rangle$. Let $z \in E$ be an element such that $z\tau z = -1$. Prove that there exists $\gamma \in E$ such that $z^2 = \tau\gamma/\gamma$. Then $E = k(\gamma)$. Let $\alpha^2 = \gamma$, and let $K = k(\alpha)$. Show that K is Galois, cyclic of degree 4 over k. Let σ be an extension of τ to K. Show that σ is an automorphism of K which generates $G_{K/k}$, satisfying $\sigma^2\alpha = -\alpha$ and $\sigma\alpha = \pm z\alpha$. Replacing z by $-z$ originally if necessary, one can then have $\sigma\alpha = z\alpha$.

7. (a) Let $K = \mathbf{Q}(\sqrt{a})$ where $a \in \mathbf{Z}$, $a < 0$. Show that K cannot be embedded in a cyclic extension whose degree over $\mathbf{Q}$ is divisible by 4.
   (b) Let $f(X) = X^4 + 30X^2 + 45$. Let α be a root of F. Prove that $\mathbf{Q}(\alpha)$ is cyclic of degree 4 over $\mathbf{Q}$.
   (c) Let $f(X) = X^4 + 4X^2 + 2$. Prove that f is irreducible over $\mathbf{Q}$ and that the Galois group is cyclic.

8. Let $f(X) = X^4 + aX^2 + b$ be an irreducible polynomial over $\mathbf{Q}$, with roots $\pm\alpha, \pm\beta$, and splitting field K.
   (a) Show that $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to a subgroup of D_8 (the non-abelian group of order 8 other than the quaternion group), and thus is isomorphic to one of the following:
   (i) $\mathbf{Z}/4\mathbf{Z}$ (ii) $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (iii) D_8.
   (b) Show that the first case happens if and only if
   $$\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbf{Q}.$$
   Case (ii) happens if and only if $\alpha\beta \in \mathbf{Q}$ or $\alpha^2 - \beta^2 \in \mathbf{Q}$. Case (iii) happens otherwise. (Actually, in (ii), the case $\alpha^2 - \beta^2 \in \mathbf{Q}$ cannot occur. It corresponds to a subgroup of $D_8 \subset S_4$ which is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, but is not transitive on $\{1,2,3,4\}$).
   (c) Find the splitting field K in $\mathbf{C}$ of the polynomial
   $$X^4 - 4X^2 - 1.$$
   Determine the Galois group of this splitting field over $\mathbf{Q}$, and describe fully the lattices of subfields and of subgroups of the Galois group.

9. Let K be a finite separable extension of a field k, of prime degree p. Let $\theta \in K$ be such that $K = k(\theta)$, and let $\theta_1, \ldots, \theta_p$ be the conjugates of θ over k in some algebraic closure. Let $\theta = \theta_1$. If $\theta_2 \in k(\theta)$, show that K is Galois and in fact cyclic over k.

10. Let $f(X) \in \mathbf{Q}[X]$ be a polynomial of degree n, and let K be a splitting field of f over $\mathbf{Q}$. Suppose that $\mathrm{Gal}(K/\mathbf{Q})$ is the symmetric group S_n with $n > 2$.
   (a) Show that f is irreducible over $\mathbf{Q}$.
   (b) If α is a root of f, show that the only automorphism of $\mathbf{Q}(\alpha)$ is the identity.
   (c) If $n \geqq 4$, show that $\alpha^n \notin \mathbf{Q}$.

11. A polynomial $f(X)$ is said to be **reciprocal** if whenever α is a root, then $1/\alpha$ is also a root. We suppose that f has coefficients in a subfield $k \subset \mathbf{R} \subset \mathbf{C}$. If f is irreducible over k, and has a nonreal root of absolute value 1, show that f is reciprocal of even degree.

12. What is the Galois group over the rationals of $X^5 - 4X + 2$?

13. What is the Galois group over the rationals of the following polynomials:
   (a) $X^4 + 2X^2 + X + 3$
   (b) $X^4 + 3X^3 - 3X - 2$
   (c) $X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15$
   [*Hint*: Reduce mod 2, 3, 5.]

14. Prove that given a symmetric group S_n, there exists a polynomial $f(X) \in \mathbf{Z}[X]$ with leading coefficient 1 whose Galois group over $\mathbf{Q}$ is S_n. [*Hint*: Reducing mod 2, 3, 5, show that there exists a polynomial whose reductions are such that the Galois group

contains enough cycles to generate S_n. Use the Chinese remainder theorem, also to be able to apply Eisenstein's criterion.]

15. Let K/k be a Galois extension, and let F be an intermediate field between k and K. Let H be the subgroup of $\mathrm{Gal}(K/k)$ mapping F into itself. Show that H is the normalizer of $\mathrm{Gal}(K/F)$ in $\mathrm{Gal}(K/k)$.

16. Let K/k be a finite Galois extension with group G. Let $\alpha \in K$ be such that $\{\sigma\alpha\}_{\sigma\in G}$ is a normal basis. For each subset S of G let $S(\alpha) = \sum_{\sigma\in S}\sigma\alpha$. Let H be a subgroup of G and let F be the fixed field of H. Show that there exists a basis of F over k consisting of elements of the form $S(\alpha)$.

Cyclotomic fields

17. (a) Let k be a field of characteristic $\nmid 2n$, for some odd integer $n \geqq 1$, and let ζ be a primitive n-th root of unity, in k. Show that k also contains a primitive $2n$-th root of unity.
    (b) Let k be a finite extension of the rationals. Show that there is only a finite number of roots of unity in k.

18. (a) Determine which roots of unity lie in the following fields: $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{-5})$.
    (b) For which integers m does a primitive m-th root of unity have degree 2 over $\mathbf{Q}$?

19. Let ζ be a primitive n-th root of unity. Let $K = \mathbf{Q}(\zeta)$.
    (a) If $n = p^r$ ($r \geqq 1$) is a prime power, show that $N_{K/\mathbf{Q}}(1 - \zeta) = p$.
    (b) If n is composite (divisible by at least two primes) then $N_{K/\mathbf{Q}}(1 - \zeta) = 1$.

20. Let $f(X) \in \mathbf{Z}[X]$ be a non-constant polynomial with integer coefficients. Show that the values $f(a)$ with $a \in \mathbf{Z}^+$ are divisible by infinitely many primes.

    Note: This is trivial. A much deeper question is whether there are infinitely many a such that $f(a)$ is prime. There are three necessary conditions:
    The leading coefficient of f is positive.
    The polynomial is irreducible.
    The set of values $f(\mathbf{Z}^+)$ has no common divisor > 1.

    A conjecture of Bouniakowski [Bo 1854] states that these conditions are sufficient. The conjecture was rediscovered later and generalized to several polynomials by Schinzel [Sch 58]. A special case is the conjecture that $X^2 + 1$ represents infinitely many primes. For a discussion of the general conjecture and a quantitative version giving a conjectured asymptotic estimate, see Bateman and Horn [BaH 62]. Also see the comments in [HaR 74]. More precisely, let $f_1, \ldots, f_r$ be polynomials with integer coefficients satisfying the first two conditions (positive leading coefficient, irreducible). Let

$$f = f_1 \cdots f_r$$

    be their product, and assume that f satisfies the third condition. Define:

    $\pi_{(f)}(x)$ = number of positive integers $n \leqq x$ such that $f_1(n), \ldots, f_r(n)$ are all primes.

    (We ignore the finite number of values of n for which some $f_i(n)$ is negative.) The

Bateman-Horn conjecture is that

$$\pi_{(f)}(x) \sim (d_1 \cdots d_r)^{-1} C(f) \int_0^x \frac{1}{(\log t)^r}\, dt,$$

where

$$C(f) = \prod_p \left\{ \left(1 - \frac{1}{p}\right)^{-r} \left(1 - \frac{N_f(p)}{p}\right) \right\},$$

the product being taken over all primes p, and $N_f(p)$ is the number of solutions of the congruence

$$f(n) \equiv 0 \bmod p.$$

Bateman and Horn show that the product converges absolutely. When $r = 1$ and $f(n) = an + b$ with a, b relatively prime integers, $a > 0$, then one gets Dirichlet's theorem that there are infinitely many primes in an arithmetic progression, together with the Dirichlet density of such primes.

[BaH 62] P. T. BATEMAN and R. HORN, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962) pp. 363-367

[Bo 1854] V. BOUNIAKOWSKY, Sur les diviseurs numériques invariables des fonctions rationnelles entières, *Mémoires sc. math. et phys. T. VI* (1854-1855) pp. 307-329

[HaR 74] H. HALBERSTAM and H.-E. RICHERT, *Sieve methods*, Academic Press, 1974

[Sch 58] A. SCHINZEL and W. SIERPINSKI, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958) pp. 185-208

21. (a) Let a be a non-zero integer, p a prime, n a positive integer, and $p \nmid n$. Prove that $p \mid \Phi_n(a)$ if and only if a has period n in $(\mathbf{Z}/p\mathbf{Z})^*$.
    (b) Again assume $p \nmid n$ Prove that $p \mid \Phi_n(a)$ for some $a \in \mathbf{Z}$ if and only if $p \equiv 1 \bmod n$. Deduce from this that there are infinitely many primes $\equiv 1 \bmod n$, a special case of Dirichlet's theorem for the existence of primes in an arithmetic progression.

22. Let $F = \mathbf{F}_p$ be the prime field of characteristic p. Let K be the field obtained from F by adjoining all primitive l-th roots of unity, for all prime numbers $l \neq p$. Prove that K is algebraically closed. [*Hint*: Show that if q is a prime number, and r an integer $\geqq 1$, there exists a prime l such that the period of $p \bmod l$ is q^r, by using the following old trick of Van der Waerden: Let l be a prime dividing the number

$$b = \frac{p^{q^r} - 1}{p^{q^{r-1}} - 1} = (p^{q^{r-1}} - 1)^{q-1} + q(p^{q^{r-1}} - 1)^{q-2} + \cdots + q.$$

If l does not divide $p^{q^{r-1}} - 1$, we are done. Otherwise, $l = q$. But in that case q^2 does not divide b, and hence there exists a prime $l \neq q$ such that l divides b. Then the degree of $F(\zeta_l)$ over F is q^r, so K contains subfields of arbitrary degree over F.]

23. (a) Let G be a finite *abelian* group. Prove that there exists an abelian extension of $\mathbf{Q}$ whose Galois group is G.

(b) Let k be a finite extension of $\mathbf{Q}$, and $G \neq \{1\}$ a finite abelian group. Prove that there exist infinitely many abelian extensions of k whose Galois group is G.

24. Prove that there are infinitely many non-zero relatively prime integers a, b such that $-4a^3 - 27b^2$ is a square in $\mathbf{Z}$.

25. Let k be a field such that every finite extension is cyclic. Show that there exists an automorphism σ of k^a over k such that k is the fixed field of σ.

26. Let $\mathbf{Q}^a$ be a fixed algebraic closure of $\mathbf{Q}$. Let E be a maximal subfield of $\mathbf{Q}^a$ not containing $\sqrt{2}$ (such a subfield exists by Zorn's lemma). Show that every finite extension of E is cyclic. (Your proof should work taking any algebraic irrational number instead of $\sqrt{2}$.)

27. Let k be a field, k^a an algebraic closure, and σ an automorphism of k^a leaving k fixed. Let F be the fixed field of σ. Show that every finite extension of F is cyclic. (The above two problems are examples of Artin, showing how to dig holes in an algebraically closed field.)

28. Let E be an algebraic extension of k such that every non-constant polynomial $f(X)$ in $k[X]$ has at least one root in E. Prove that E is algebraically closed. [*Hint*: Discuss the separable and purely inseparable cases separately, and use the primitive element theorem.]

29. (a) Let K be a cyclic extension of a field F, with Galois group G generated by σ. Assume that the characteristic is p, and that $[K:F] = p^{m-1}$ for some integer $m \geqq 2$. Let β be an element of K such that $\mathrm{Tr}_F^K(\beta) = 1$. Show that there exists an element α in K such that

$$\sigma\alpha - \alpha = \beta^p - \beta.$$

(b) Prove that the polynomial $X^p - X - \alpha$ is irreducible in $K[X]$.

(c) If θ is a root of this polynomial, prove that $F(\theta)$ is a Galois, cyclic extension of degree p^m of F, and that its Galois group is generated by an extension σ^* of σ such that

$$\sigma^*(\theta) = \theta + \beta.$$

30. Let A be an abelian group and let G be a finite cyclic group operating on A [by means of a homomorphism $G \to \mathrm{Aut}(A)$]. Let σ be a generator of G. We define the trace $\mathrm{Tr}_G = \mathrm{Tr}$ on A by $\mathrm{Tr}(x) = \sum_{\tau \in G} \tau x$. Let A_{Tr} denote the kernel of the trace, and let $(1 - \sigma)A$ denote the subgroup of A consisting of all elements of type $y - \sigma y$. Show that $H^1(G, A) \approx A_{\mathrm{Tr}}/(1 - \sigma)A$.

31. Let F be a finite field and K a finite extension of F. Show that the norm N_F^K and the trace Tr_F^K are surjective (as maps from K into F).

32. Let E be a finite separable extension of k, of degree n. Let $W = (w_1, \ldots, w_n)$ be elements of E. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of E in k^a over k. Define the **discriminant** of W to be

$$D_{E/k}(W) = \det(\sigma_i w_j)^2.$$

Prove:

(a) If $V = (v_1, \ldots, v_n)$ is another set of elements of E and $C = (c_{ij})$ is a matrix of elements of k such that $w_i = \sum c_{ij} v_j$, then

$$D_{E/k}(W) = \det(C)^2 D_{E/k}(V).$$

(b) The discriminant is an element of k.

(c) Let $E = k(\alpha)$ and let $f(X) = \operatorname{Irr}(\alpha, k, X)$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f and say $\alpha = \alpha_1$. Then

$$f'(\alpha) = \prod_{j=2}^{n} (\alpha - \alpha_j).$$

Show that

$$D_{E/k}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_k^E(f'(\alpha)).$$

(d) Let the notation be as in (a). Show that $\det(\operatorname{Tr}(w_i w_j)) = (\det(\sigma_i w_j))^2$. [*Hint*: Let A be the matrix $(\sigma_i w_j)$. Show that ${}^tAA$ is the matrix $(\operatorname{Tr}(w_i w_j))$.]

Rational functions

33. Let $K = \mathbf{C}(x)$ where x is transcendental over $\mathbf{C}$, and let ζ be a primitive cube root of unity in $\mathbf{C}$. Let σ be the automorphism of K over $\mathbf{C}$ such that $\sigma x = \zeta x$. Let τ be the automorphism of K over $\mathbf{C}$ such that $\tau x = x^{-1}$. Show that

$$\sigma^3 = 1 = \tau^2 \quad \text{and} \quad \tau\sigma = \sigma^{-1}\tau.$$

Show that the group of automorphisms G generated by σ and τ has order 6 and the subfield F of K fixed by G is the field $\mathbf{C}(y)$ where $y = x^3 + x^{-3}$.

34. Give an example of a field K which is of degree 2 over two distinct subfields E and F respectively, but such that K is not algebraic over $E \cap F$.

35. Let k be a field and X a variable over k. Let

$$\varphi(X) = \frac{f(X)}{g(X)}$$

be a rational function in $k(X)$, expressed as a quotient of two polynomials f, g which are relatively prime. Define the degree of φ to be $\max(\deg f, \deg g)$. Let $Y = \varphi(X)$. (a) Show that the degree of φ is equal to the degree of the field extension $k(X)$ over $k(Y)$ (assuming $Y \notin k$). (b) Show that every automorphism of $k(X)$ over k can be represented by a rational function φ of degree 1, and is therefore induced by a map

$$X \mapsto \frac{aX + b}{cX + d}$$

with $a, b, c, d \in k$ and $ad - bc \neq 0$. (c) Let G be the group of automorphisms of $k(X)$ over k. Show that G is generated by the following automorphisms:

$$\tau_b : X \mapsto X + b, \qquad \sigma_a : X \mapsto aX \quad (a \neq 0), \qquad X \mapsto X^{-1}$$

with $a, b \in k$.

36. Let k be a finite field with q elements. Let $K = k(X)$ be the rational field in one variable. Let G be the group of automorphisms of K obtained by the mappings

$$X \mapsto \frac{aX + b}{cX + d}$$

with a, b, c, d in k and $ad - bc \neq 0$. Prove the following statements:

(a) The order of G is $q^3 - q$.

(b) The fixed field of G is equal to $k(Y)$ where

$$Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}.$$

(c) Let H_1 be the subgroup of G consisting of the mappings $X \mapsto aX + b$ with $a \neq 0$. The fixed field of H_1 is $k(T)$ where $T = (X^q - X)^{q-1}$.

(d) Let H_2 be the subgroup of H_1 consisting of the mappings $X \to X + b$ with $b \in k$. The fixed field of H_2 is equal to $k(Z)$ where $Z = X^q - X$.

Some aspects of Kummer theory

37. Let k be a field of characteristic 0. Assume that for each finite extension E of k, the index $(E^* : E^{*n})$ is finite for every positive integer n. Show that for each positive integer n, there exists only a finite number of abelian extensions of k of degree n.

38. Let $a \neq 0, \neq \pm 1$ be a square-free integer. For each prime number p, let K_p be the splitting field of the polynomial $X^p - a$ over $\mathbf{Q}$. Show that $[K_p : \mathbf{Q}] = p(p-1)$. For each square-free integer $m > 0$, let

$$K_m = \prod_{p \mid m} K_p$$

be the compositum of all fields K_p for $p \mid m$. Let $d_m = [K_m : \mathbf{Q}]$ be the degree of K_m over $\mathbf{Q}$. Show that if m is odd then $d_m = \prod_{p \mid m} d_p$, and if m is even, $m = 2n$ then $d_{2n} = d_n$ or $2d_n$ according as $\sqrt{a}$ is or is not in the field of m-th roots of unity $\mathbf{Q}(\zeta_m)$.

39. Let K be a field of characteristic 0 for simplicity. Let Γ be a finitely generated subgroup of K^*. Let N be an *odd* positive integer. Assume that for each prime $p \mid N$ we have

$$\Gamma = \Gamma^{1/p} \cap K,$$

and also that $\mathrm{Gal}(K(\mu_N)/K) \approx \mathbf{Z}(N)^*$. Prove the following.

(a) $\Gamma/\Gamma^N \approx \Gamma/(\Gamma \cap K^{*N}) \approx \Gamma K^{*N}/K^{*N}$.

(b) Let $K_N = K(\mu_N)$. Then

$$\Gamma \cap K_N^{*N} = \Gamma^N.$$

[*Hint*: If these two groups are not equal, then for some prime $p \mid N$ there exists an element $a \in \Gamma$ such that

$$a = b^p \quad \text{with} \quad b \in K_N \quad \text{but} \quad b \notin K.$$

In other words, a is not a p-th power in K but becomes a p-th power in K_N. The equation $x^p - a$ is irreducible over K. Show that b has degree p over $K(\mu_p)$, and that $K(\mu_p, a^{1/p})$ is not abelian over K, so $a^{1/p}$ has degree p over $K(\mu_p)$. Finish the proof yourself.]

(c) Conclude that the natural Kummer map

$$\Gamma/\Gamma^N \to \mathrm{Hom}(H_\Gamma(N), \mu_N)$$

is an isomorphism.

(d) Let $G_\Gamma(N) = \mathrm{Gal}(K(\Gamma^{1/N}, \mu_N)/K)$. Then the commutator subgroup of $G_\Gamma(N)$ is $H_\Gamma(N)$, and in particular $\mathrm{Gal}(K_N/K)$ is the maximal abelian quotient of $G_\Gamma(N)$.

40. Let K be a field and p a prime number not equal to the characteristic of K. Let Γ be a finitely generated subgroup of K^*, and assume that Γ is equal to its own p-division group in K, that is if $z \in K$ and $z^p \in \Gamma$, then $z \in \Gamma$. If p is odd, assume that $\mu_p \subset K$, and if $p = 2$, assume that $\mu_4 \subset K$. Let

$$(\Gamma : \Gamma^p) = p^{r+1}.$$

Show that $\Gamma^{1/p}$ is its own p-division group in $K(\Gamma^{1/p})$, and

$$[K(\Gamma^{1/p^m}) : K] = p^{m(r+1)}$$

for all positive integers m.

41. **Relative invariants (Sato).** Let k be a field and K an extension of k. Let G be a group of automorphisms of K over k, and assume that k is the fixed field of G. (We do not assume that K is algebraic over k.) By a **relative invariant** of G in K we shall mean an element $P \in K$, $P \neq 0$, such that for each $\sigma \in G$ there exists an element $\chi(\sigma) \in k$ for which $P^\sigma = \chi(\sigma)P$. Since σ is an automorphism, we have $\chi(\sigma) \in k^*$. We say that the map $\chi : G \to k^*$ **belongs** to P, and call it a **character**. Prove the following statements:

(a) The map χ above is a homomorphism.

(b) If the same character χ belongs to relative invariants P and Q then there exists $c \in k^*$ such that $P = cQ$.

(c) The relative invariants form a multiplicative group, which we denote by I. Elements $P_1, \ldots, P_m$ of I are called multiplicatively independent mod k^* if their images in the factor group I/k^* are multiplicatively independent, i.e. if given integers $v_1, \ldots, v_m$ such that

$$P_1^{v_1} \cdots P_m^{v_m} = c \in k^*,$$

then $v_1 = \cdots = v_m = 0$.

(d) If $P_1, \ldots, P_m$ are multiplicatively independent mod k^* prove that they are algebraically independent over k. [*Hint*: Use Artin's theorem on characters.]

(e) Assume that $K = k(X_1, \ldots, X_n)$ is the quotient field of the polynomial ring $k[X_1, \ldots, X_n] = k[X]$, and assume that G induces an automorphism of the polynomial ring. Prove: If $F_1(X)$ and $F_2(X)$ are relative invariant polynomials, then their g.c.d. is relative invariant. If $P(X) = F_1(X)/F_2(X)$ is a relative invariant, and is the quotient of two relatively prime polynomials, then $F_1(X)$ and $F_2(X)$ are relative invariants. Prove that the relative invariant polynomials generate I/k^*. Let S be the set of relative invariant polynomials which cannot be factored into a product of two relative invariant polynomials of degrees $\geqq 1$. Show that the elements of S/k^* are multiplicatively independent, and hence that I/k^* is a free abelian group. [If you know about transcendence degree, then using (d) you can conclude that this group is finitely generated.]

42. Let $f(z)$ be a rational function with coefficients in a finite extension of the rationals. Assume that there are infinitely many roots of unity ζ such that $f(\zeta)$ is a root of unity. Show that there exists an integer n such that $f(z) = cz^n$ for some constant c (which is in fact a root of unity).

This exercise can be generalized as follows: Let Γ_0 be a finitely generated multiplicative group of complex numbers. Let Γ be the group of all complex numbers γ such that γ^m lies in Γ_0 for some integer $m \neq 0$. Let $f(z)$ be a rational function with complex coefficients such that there exist infinitely many $\gamma \in \Gamma$ for which $f(\gamma)$ lies in Γ. Then again, $f(z) = cz^n$ for some c and n. (Cf. *Fundamentals of Diophantine Geometry*.)

43. Let K/k be a Galois extension. We define the **Krull topology** on the group $G(K/k) = G$ by defining a base for open sets to consist of all sets σH where $\sigma \in G$ and $H = G(K/F)$ for some finite extension F of k contained in K.
    (a) Show that if one takes only those sets σH for which F is finite Galois over k then one obtains another base for the same topology.
    (b) The projective limit $\varprojlim G/H$ is embedded in the direct product
    $$\varprojlim_H G/H \to \prod_H G/H.$$
    Give the direct product the product topology. By Tychonoff's theorem in elementary point set topology, the direct product is compact because it is a direct product of finite groups, which are compact (and of course also discrete). Show that the inverse limit $\varprojlim G/H$ is closed in the product, and is therefore compact.
    (c) Conclude that $G(K/k)$ is compact.
    (d) Show that every closed subgroup of finite index in $G(K/k)$ is open.
    (e) Show that the closed subgroups of $G(K/k)$ are precisely those subgroups which are of the form $G(K/F)$ for some extension F of k contained in K.
    (f) Let H be an arbitrary subgroup of G and let F be the fixed field of H. Show that $G(K/F)$ is the closure of H in G.

44. Let k be a field such that every finite extension is cyclic, and having one extension of degree n for each integer n. Show that the Galois group $G = G(k^a/k)$ is the inverse limit $\lim \mathbf{Z}/m\mathbf{Z}$, as $m\mathbf{Z}$ ranges over all ideals of $\mathbf{Z}$, ordered by inclusion. Show that this limit is isomorphic to the direct product of the limits
$$\prod_p \lim_{n\to\infty} \mathbf{Z}/p^n\mathbf{Z} = \prod_p \mathbf{Z}_p$$
taken over all prime numbers p, in other words, it is isomorphic to the product of all p-adic integers.

45. Let k be a perfect field and k^a its algebraic closure. Let $\sigma \in G(k^a/k)$ be an element of infinite order, and suppose k is the fixed field of σ. For each prime p, let K_p be the composite of all cyclic extensions of k of degree a power of p.
    (a) Prove that k^a is the composite of all extensions K_p.
    (b) Prove that either $K_p = k$, or K_p is infinite cyclic over k. In other words, K_p cannot be finite cyclic over k and $\neq k$.
    (c) Suppose $k^a = K_p$ for some prime p, so k^a is an infinite cyclic tower of p-extensions. Let u be a p-adic unit, $u \in \mathbf{Z}_p^*$ such that u does not represent a rational number. Define σ^u, and prove that σ, σ^u are linearly independent

over $\mathbf{Z}$, i.e. the group generated by σ and σ^u is free abelian of rank 2. In particular $\{\sigma\}$ and $\{\sigma, \sigma^u\}$ have the same fixed field k.

Witt vectors

46. Let $x_1, x_2, \ldots$ be a sequence of algebraically independent elements over the integers $\mathbf{Z}$. For each integer $n \geqq 1$ define

$$x^{(n)} = \sum_{d \mid n} d x_d^{n/d}.$$

Show that x_n can be expressed in terms of $x^{(d)}$ for $d \mid n$, with rational coefficients.

Using vector notation, we call $(x_1, x_2, \ldots)$ the Witt components of the vector x, and call $(x^{(1)}, x^{(2)}, \ldots)$ its **ghost** components. We call x a **Witt vector**.

Define the power series

$$f_x(t) = \prod_{n \geqq 1} (1 - x_n t^n).$$

Show that

$$-t \frac{d}{dt} \log f_x(t) = \sum_{n \geqq 1} x^{(n)} t^n.$$

[By $\frac{d}{dt} \log f(t)$ we mean $f'(t)/f(t)$ if $f(t)$ is a power series, and the derivative $f'(t)$ is taken formally.]

If x, y are two Witt vectors, define their sum and product componentwise *with respect to the ghost components*, i.e.

$$(x + y)^{(n)} = x^{(n)} + y^{(n)}.$$

What is $(x + y)_n$? Well, show that

$$f_x(t) f_y(t) = \prod (1 + (x + y)_n t^n) = f_{x+y}(t).$$

Hence $(x + y)_n$ is a polynomial with integer coefficients in $x_1, y_1, \ldots, x_n, y_n$. Also show that

$$f_{xy}(t) = \prod_{d, e \geqq 1} (1 - x_d^{m/d} y_e^{m/e} t^m)^{de/m}$$

where m is the least common multiple of d, e and d, e range over all integers $\geqq 1$. Thus $(xy)_n$ is also a polynomial in $x_1, y_1 \ldots, x_n, y_n$ with integer coefficients. The above arguments are due to Witt (oral communication) and differ from those of his original paper.

If A is a commutative ring, then taking a homomorphic image of the polynomial ring over $\mathbf{Z}$ into A, we see that we can define addition and multiplication of Witt vectors with components in A, and that these Witt vectors form a ring $W(A)$. Show that W is a functor, i.e. that any ring homomorphism φ of A into a commutative ring A' induces a homomorphism $W(\varphi) : W(A) \to W(A')$.

47. Let p be a prime number, and consider the projection of $W(A)$ on vectors whose components are indexed by a power of p. Now use the log to the base p to index these components, so that we write x_n instead of x_{p^n}. For instance, x_0 now denotes what was x_1 previously. For a Witt vector $x = (x_0, x_1, \ldots, x_n, \ldots)$ define

$$Vx = (0, x_0, x_1, \ldots) \quad \text{and} \quad Fx = (x_0^p, x_1^p, \ldots).$$

Thus V is a shifting operator. We have $V \circ F = F \circ V$. Show that

$$(Vx)^{(n)} = px^{(n-1)} \quad \text{and} \quad x^{(n)} = (Fx)^{(n-1)} + p^n x_n.$$

Also from the definition, we have

$$x^{(n)} = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n.$$

48. Let k be a field of characteristic p, and consider $W(k)$. Then V is an additive endomorphism of $W(k)$, and F is a ring homomorphism of $W(k)$ into itself. Furthermore, if $x \in W(k)$ then

$$px = VFx.$$

If $x, y \in W(k)$, then $(V^i x)(V^j y) = V^{i+j}(F^{p^j} x \cdot F^{p^i} y)$. For $a \in k$ denote by $\{a\}$ the Witt vector $(a, 0, 0, \ldots)$. Then we can write symbolically

$$x = \sum_{i=0}^{\infty} V^i \{x_i\}.$$

Show that if $x \in W(k)$ and $x_0 \neq 0$ then x is a unit in $W(k)$. *Hint*: One has

$$1 - x\{x_0^{-1}\} = Vy$$

and then

$$x\{x_0^{-1}\} \sum_0^{\infty} (Vy)^i = (1 - Vy) \sum_0^{\infty} (Vy)^i = 1.$$

49. Let n be an integer $\geqq 1$ and p a prime number again. Let k be a field of characteristic p. Let $W_n(k)$ be the ring of truncated Witt vectors $(x_0, \ldots, x_{n-1})$ with components in k. We view $W_n(k)$ as an additive group. If $x \in W_n(k)$, define $\wp(x) = Fx - x$. Then $\wp$ is a homomorphism. If K is a Galois extension of k, and $\sigma \in G(K/k)$, and $x \in W_n(K)$ we can define σx to have component $(\sigma x_0, \ldots, \sigma x_{n-1})$. Prove the analogue of Hilbert's Theorem 90 for Witt vectors, and prove that the first cohomology group is trivial. (One takes a vector whose trace is not 0, and finds a coboundary the same way as in the proof of Theorem 10.1).

50. If $x \in W_n(k)$, show that there exists $\xi \in W_n(\bar{k})$ such that $\wp(\xi) = x$. Do this inductively, solving first for the first component, and then showing that a vector $(0, \alpha_1, \ldots, \alpha_{n-1})$ is in the image of $\wp$ if and only if $(\alpha_1, \ldots, \alpha_{n-1})$ is in the image of $\wp$. Prove inductively that if $\xi, \xi' \in W_n(k')$ for some extension k' of k and if $\wp\xi = \wp\xi'$ then $\xi - \xi'$ is a vector with components in the prime field. Hence the solutions of $\wp\xi = x$ for given $x \in W_n(k)$ all differ by the vectors with components in the prime field, and there are p^n such vectors. We define

$$k(\xi) = k(\xi_0, \ldots, \xi_{n-1}),$$

or symbolically,

$$k(\wp^{-1}x).$$

Prove that it is a Galois extension of k, and show that the cyclic extensions of k, of degree p^n, are precisely those of type $k(\wp^{-1}x)$ with a vector x such that $x_0 \notin \wp k$.

51. Develop the Kummer theory for abelian extensions of k of exponent p^n by using $W_n(k)$. In other words, show that there is a bijection between subgroups B of $W_n(k)$ containing $\wp W_n(k)$ and abelian extensions as above, given by

$$B \mapsto K_B$$

where $K_B = k(\wp^{-1}B)$. All of this is due to Witt, cf. the references at the end of §8, especially [Wi 37]. The proofs are the same, *mutatis mutandis*, as those given for the Kummer theory in the text.

Further Progress and directions

Major progress was made in the 90s concerning some problems mentioned in the chapter. Foremost was Wiles's proof of enough of the Shimura-Taniyama conjecture to imply Fermat's Last Theorem [Wil 95], [TaW 95].

[TaW 95] R. TAYLOR and A. WILES, Ring-theoretic properties or certain Hecke algebras, *Annals of Math.* **141** (1995) pp. 553–572

[Wil 95] A. WILES, Modular elliptic curves and Fermat's last theorem, *Annals. of Math.* **141** (1995) pp. 443–551

Then a proof of the complete Shimura-Taniyama conjecture was given in [BrCDT 01].

[BrCDT 01] C. BREUIL, B. CONRAD, F. DIAMOND, R. TAYLOR, On the modularity of elliptic curves over **Q**: Wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001) pp. 843–839

In a quite different direction, Neukirch started the characterization of number fields by their absolute Galois groups [Ne 68], [Ne 69a], [Ne 69b], and proved it for Galois extensions of **Q**. His results were extended and his subsequent conjectures were proved by Ikeda and Uchida [Ik 77], [Uch 77], [Uch 79], [Uch 81]. These results were extended to finitely generated extensions of **Q** (function fields) by Pop [Pop 94], who has a more extensive bibliography on these and related questions of algebraic geometry. For these references, see the bibliography at the end of the book.

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*
© Springer Science+Business Media LLC 2002

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.

CHAPTER VIII

Transcendental Extensions

Both for their own sake and for applications to the case of finite extensions of the rational numbers, one is led to deal with ground fields which are function fields, i.e. finitely generated over some field k, possibly by elements which are not algebraic. This chapter gives some basic properties of such fields.

§1. TRANSCENDENCE BASES

Let K be an extension field of a field k. Let S be a subset of K. We recall that S (or the elements of S) is said to be algebraically independent over k, if whenever we have a relation

$$0 = \sum a_{(\nu)} M_{(\nu)}(S) = \sum a_{(\nu)} \prod_{x \in S} x^{\nu(x)}$$

with coefficients $a_{(\nu)} \in k$, almost all $a_{(\nu)} = 0$, then we must necessarily have all $a_{(\nu)} = 0$.

We can introduce an ordering among algebraically independent subsets of K, by ascending inclusion. These subsets are obviously inductively ordered, and thus there exist maximal elements. If S is a subset of K which is algebraically independent over k, and if the cardinality of S is greatest among all such subsets, then we call this cardinality the **transcendence degree or dimension** of K over k. Actually, we shall need to distinguish only between finite transcendence degree or infinite transcendence degree. We observe that

S. Lang, *Algebra*
© Springer Science+Business Media LLC 2002

the notion of transcendence degree bears to the notion of algebraic independence the same relation as the notion of dimension bears to the notion of linear independence.

We frequently deal with families of elements of K, say a family $\{x_i\}_{i \in I}$, and say that such a family is algebraically independent over k if its elements are distinct (in other words, $x_i \neq x_j$ if $i \neq j$) and if the set consisting of the elements in this family is algebraically independent over k.

A subset S of K which is algebraically independent over k and is maximal with respect to the inclusion ordering will be called a **transcendence base** of K over k. From the maximality, it is clear that if S is a transcendence base of K over k, then K is algebraic over $k(S)$.

Theorem 1.1. *Let K be an extension of a field k. Any two transcendence bases of K over k have the same cardinality. If Γ is a subset of K such that K is algebraic over $k(\Gamma)$, and S is a subset of Γ which is algebraically independent over k, then there exists a transcendence base $\mathfrak{B}$ of K over k such that $S \subset \mathfrak{B} \subset \Gamma$.*

Proof. We shall prove that if there exists one finite transcendence base, say $\{x_1, \ldots, x_m\}$, $m \geqq 1$, m minimal, then any other transcendence base must also have m elements. For this it will suffice to prove: If $w_1, \ldots, w_n$ are elements of K which are algebraically independent over k then $n \leqq m$ (for we can then use symmetry). By assumption, there exists a non-zero irreducible polynomial f_1 in $m + 1$ variables with coefficients in k such that

$$f_1(w_1, x_1, \ldots, x_m) = 0.$$

After renumbering $x_1, \ldots, x_m$ we may write $f_1 = \sum g_j(w_1, x_2, \ldots, x_m) x_1^j$ with some $g_N \neq 0$ with some $N \geqq 1$. No irreducible factor of g_N vanishes on $(w_1, x_2, \ldots, x_n)$, otherwise w_1 would be a root of two distinct irreducible polynomials over $k(x_1, \ldots, x_m)$. Hence x_1 is algebraic over $k(w_1, x_2, \ldots, x_m)$ and $w_1, x_2, \ldots, x_m$ are algebraically independent over k, otherwise the minimality of m would be contradicted. Suppose inductively that after a suitable renumbering of $x_2, \ldots, x_m$ we have found $w_1, \ldots, w_r$ $(r < n)$ such that K is algebraic over $k(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m)$. Then there exists a non-zero polynomial f in $m + 1$ variables with coefficients in k such that

$$f(w_{r+1}, w_1, \ldots, w_r, x_{r+1}, \ldots, x_m) = 0.$$

Since the w's are algebraically independent over k, it follows by the same argument as in the first step that some x_j, say x_{r+1}, is algebraic over $k(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. Since a tower of algebraic extensions is algebraic, it follows that K is algebraic over $k(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. We can repeat the procedure, and if $n \geqq m$ we can replace all the x's by w's, to see that K is algebraic over $k(w_1, \ldots, w_m)$. This shows that $n \geqq m$ implies $n = m$, as desired.

We have now proved: Either the transcendence degree is finite, and is equal to the cardinality of any transcendence base, or it is infinite, and every transcendence base is infinite. The cardinality statement in the infinite case will be left as an exercise. We shall also leave as an exercise the statement that a set of algebraically independent elements can be completed to a transcendence base, selected from a given set Γ such that K is algebraic over $k(\Gamma)$. (The reader will note the complete analogy of our statements with those concerning linear bases.)

Note. *The preceding section is the only one used in the next chapter. The remaining sections are more technical, especially §3 and §4 which will not be used in the rest of the book. Even §2 and §5 will only be mentioned a couple of times, and so the reader may omit them until they are referred to again.*

§2. NOETHER NORMALIZATION THEOREM

Theorem 2.1. *Let $k[x_1, \ldots, x_n] = k[x]$ be a finitely generated entire ring over a field k, and assume that $k(x)$ has transcendence degree r. Then there exist elements $y_1, \ldots, y_r$ in $k[x]$ such that $k[x]$ is integral over*

$$k[y] = k[y_1, \ldots, y_r].$$

Proof. If $(x_1, \ldots, x_n)$ are already algebraically independent over k, we are done. If not, there is a non-trivial relation

$$\sum a_{(j)} x_1^{j_1} \cdots x_n^{j_n} = 0$$

with each coefficient $a_{(j)} \in k$ and $a_{(j)} \neq 0$. The sum is taken over a finite number of distinct n-tuples of integers $(j_1, \ldots, j_n)$, $j_\nu \geqq 0$. Let $m_2, \ldots, m_n$ be positive integers, and put

$$y_2 = x_2 - x_1^{m_2}, \ldots, y_n = x_n - x_1^{m_n}.$$

Substitute $x_i = y_i + x_1^{m_i}$ $(i = 2, \ldots, n)$ in the above equation. Using vector notation, we put $(m) = (1, m_2, \ldots, m_n)$ and use the dot product $(j) \cdot (m)$ to denote $j_1 + m_2 j_2 + \cdots + m_n j_n$. If we expand the relation after making the above substitution, we get

$$\sum c_{(j)} x_1^{(j)\cdot(m)} + f(x_1, y_2, \ldots, y_n) = 0$$

where f is a polynomial in which no pure power of x_1 appears. We now select d to be a large integer [say greater than any component of a vector (j) such that $c_{(j)} \neq 0$] and take

$$(m) = (1, d, d^2, \ldots, d^n).$$

Then all $(j)\cdot(m)$ are distinct for those (j) such that $c_{(j)} \neq 0$. In this way we obtain an integral equation for x_1 over $k[y_2, \ldots, y_n]$. Since each x_i $(i > 1)$ is integral over $k[x_1, y_2, \ldots, y_n]$, it follows that $k[x]$ is integral over $k[y_2, \ldots, y_n]$. We can now proceed inductively, using the transitivity of integral extensions to shrink the number of y's until we reach an algebraically independent set of y's.

The advantage of the proof of Theorem 2.1 is that it is applicable when k is a finite field. The disadvantage is that it is not linear in $x_1, \ldots, x_n$. We now deal with another technique which leads into certain aspects of algebraic geometry on which we shall comment after the next theorem.

We start again with $k[x_1, \ldots, x_n]$ finitely generated over k and entire. Let (u_{ij}) $(i, j = 1, \ldots, n)$ be algebraically independent elements over $k(x)$, and let $k_u = k(u) = k(u_{ij})_{\text{all } i,j}$. Put

$$y_i = \sum_{j=1}^{n} u_{ij} x_j.$$

This amounts to a generic linear change of coordinates in n-space, to use geometric terminology. Again we let r be the transcendence degree of $k(x)$ over k.

Theorem 2.2. *With the above notation, $k_u[x]$ is integral over $k_u[y_1, \ldots, y_r]$.*

Proof. Suppose some x_i is not integral over $k_u[y_1, \ldots, y_r]$. Then there exists a place φ of $k_u(y)$ finite on $k_u[y_1, \ldots, y_r]$ but taking the value ∞ on some x_i. Using Proposition 3.4 of Chapter VII, and renumbering the indices if necessary, say $\varphi(x_j/x_n)$ is finite for all i. Let $z'_j = \varphi(x_j/x_n)$ for $j = 1, \ldots, n$. Then dividing the equations $y_i = \sum u_{ij} x_j$ by x_n (for $i = 1, \ldots, r$) and applying the place, we get

$$\begin{aligned} 0 &= u_{11} z'_1 + u_{12} z'_2 + \cdots + u_{1n}, \\ &\vdots \\ 0 &= u_{r1} z'_1 + u_{r2} z'_2 + \cdots + u_{rn}. \end{aligned}$$

The transcendence degree of $k(z')$ over k cannot be r, for otherwise, the place φ would be an isomorphism of $k(x)$ on its image. [Indeed, if, say, $z'_1, \ldots, z'_r$ are algebraically independent and $z_i = x_i/x_n$, then $z_1, \ldots, z_r$ are also algebraically independent, and so form a transcendence base for $k(x)$ over k. Then the place is an isomorphism from $k(z_1, \ldots, z_r)$ to $k(z'_1, \ldots, z'_r)$, and hence is an isomorphism from $k(x)$ to its image.] We then conclude that

$$u_{1n}, \ldots, u_{rn} \in k(u_{ij}, z') \qquad \text{with} \quad i = 1, \ldots, r; \quad j = 1, \ldots, n-1.$$

Hence the transcendence degree of $k(u)$ over k would be $\leqq rn - 1$, which is a contradiction, proving the theorem.

Corollary 2.3. *Let k be a field, and let $k(x)$ be a finitely generated extension of transcendence degree r. There exists a polynomial $P(u) = P(u_{ij}) \in k[u]$ such that if $(c) = (c_{ij})$ is a family of elements $c_{ij} \in k$ satisfying $P(c) \neq 0$, and we let $y_i' = \sum c_{ij}x_j$, then $k[x]$ is integral over $k[y_1', \ldots, y_r']$.*

Proof. By Theorem 2.2, each x_i is integral over $k_u[y_1, \ldots, y_r]$. The coefficients of an integral equation are rational functions in k_u. We let $P(u)$ be a common denominator for these rational functions. If $P(c) \neq 0$, then there is a homomorphism

$$\varphi: k(x)[u, P(u)^{-1}] \to k(x)$$

such that $\varphi(u) = (c)$, and such that φ is the identity on $k(x)$. We can apply φ to an integral equation for x_i over $k_u[y]$ to get an integral equation for x_i over $k[y']$, thus concluding the proof.

Remark. After Corollary 2.3, there remains the problem of finding explicitly integral equations for $x_1, \ldots, x_n$ (or $y_{r+1}, \ldots, y_n$) over $k_u[y_1, \ldots, y_r]$. This is an elimination problem, and I have decided to refrain from further involvement in algebraic geometry at this point. But it may be useful to describe the geometric language used to interpret Theorem 2.2 and further results in that line. After the generic change of coordinates, the map

$$(y_1, \ldots, y_n) \mapsto (y_1, \ldots, y_r)$$

is the generic projection of the variety whose coordinate ring is $k[x]$ on affine r-space. This projection is finite, and in particular, the inverse image of a point on affine r-space is finite. Furthermore, if $k(x)$ is separable over k (a notion which will be defined in §4), then the extension $k_u(y)$ is finite separable over $k_u(y_1, \ldots, y_r)$ (in the sense of Chapter V). To determine the degree of this finite extension is essentially Bezout's theorem. Cf. [La 58], Chapter VIII, §6.

The above techniques were created by van der Waerden and Zariski, cf., for instance, also Exercises 5 and 6. These techniques have unfortunately not been completely absorbed in some more recent expositions of algebraic geometry. To give a concrete example: When Hartshorne considers the intersection of a variety and a sufficiently general hyperplane, he does not discuss the "generic" hyperplane (that is, with algebraically independent coefficients over a given ground field), and he assumes that the variety is non-singular from the start (see his Theorem 8.18 of Chapter 8, [Ha 77]). But the description of the intersection can be done without simplicity assumptions, as in Theorem 7 of [La 58], Chapter VII, §6, and the corresponding lemma. Something was lost in discarding the technique of the algebraically independent (u_{ij}).

After two decades when the methods illustrated in Chapter X have been prevalent, there is a return to the more explicit methods of generic constructions using the algebraically independent (u_{ij}) and similar ones for some

applications because part of algebraic geometry and number theory are returning to some problems asking for explicit or effective constructions, with bounds on the degrees of solutions of algebraic equations. See, for instance, [Ph 91–95], [So 90], and the bibliography at the end of Chapter X, §6. Returning to some techniques, however, does not mean abandoning others; it means only expanding available tools.

Bibliography

[Ha 77] R. HARTSHORNE, *Algebraic Geometry*, Springer-Verlag, New York, 1977

[La 58] S. LANG, *Introduction to Algebraic Geometry*, Wiley–Interscience, New York, 1958

[Ph 91–95] P. PHILIPPON, Sur des hauteurs alternatives, I *Math. Ann.* 289 (1991) pp. 255–283; II *Ann. Inst. Fourier* 44 (1994) pp. 1043–1065; III *J. Math. Pures Appl.* 74 (1995) pp. 345–365

[So 90] C. SOULÉ, Géometrie d'Arakelov et théorie des nombres transcendants, Asterisque 198–200 (1991) pp. 355–371

§3. LINEARLY DISJOINT EXTENSIONS

In this section we discuss the way in which two extensions K and L of a field k behave with respect to each other. We assume that all the fields involved are contained in one field Ω, assumed algebraically closed.

K is said to be **linearly disjoint from L over k** if every finite set of elements of K that is linearly independent over k is still such over L.

The definition is unsymmetric, but we prove right away that the property of being linearly disjoint is actually symmetric for K and L. Assume K linearly disjoint from L over k. Let $y_1, \ldots, y_n$ be elements of L linearly independent over k. Suppose there is a non-trivial relation of linear dependence over K,

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = 0. \tag{1}$$

Say $x_1, \ldots, x_r$ are linearly independent over k, and $x_{r+1}, \ldots, x_n$ are linear combinations $x_i = \sum_{\mu=1}^{r} a_{i\mu} x_\mu$, $i = r+1, \ldots, n$. We can write the relation (1) as follows:

$$\sum_{\mu=1}^{r} x_\mu y_\mu + \sum_{i=r+1}^{n} \left(\sum_{\mu=1}^{r} a_{i\mu} x_\mu \right) y_i = 0$$

and collecting terms, after inverting the second sum, we get

$$\sum_{\mu=1}^{r} \left(y_\mu + \sum_{i=r+1}^{n} (a_{i\mu} y_i) \right) x_\mu = 0.$$

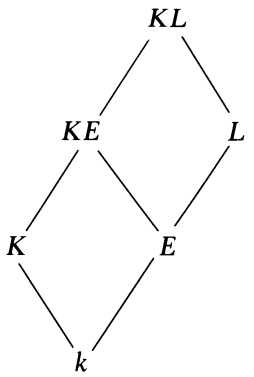
The y's are linearly independent over k, so the coefficients of x_μ are $\neq 0$. This contradicts the linear disjointness of K and L over k.

We now give two criteria for linear disjointness.

Criterion 1. Suppose that K is the quotient field of a ring R and L the quotient field of a ring S. To test whether L and K are linearly disjoint, it suffices to show that if elements $y_1, \ldots, y_n$ of S are linearly independent over k, then there is no linear relation among the y's with coefficients in R. Indeed, if elements $y_1, \ldots, y_n$ of L are linearly independent over k, and if there is a relation $x_1 y_1 + \cdots + x_n y_n = 0$ with $x_i \in K$, then we can select y in S and x in R such that $xy \neq 0$, $yy_i \in S$ for all i, and $xx_i \in R$ for all i. Multiplying the relation by xy gives a linear dependence between elements of R and S. However, the yy_i are obviously linearly independent over k, and this proves our criterion.

Criterion 2. Again let R be a subring of K such that K is its quotient field and R is a vector space over k. Let $\{u_\alpha\}$ be a basis of R considered as a vector space over k. To prove K and L linearly disjoint over k, it suffices to show that the elements $\{u_\alpha\}$ of this basis remain linearly independent over L. Indeed, suppose this is the case. Let $x_1, \ldots, x_m$ be elements of R linearly independent over k. They lie in a finite dimension vector space generated by some of the u_α, say $u_1, \ldots, u_n$. They can be completed to a basis for this space over k. Lifting this vector space of dimension n over L, it must conserve its dimension because the u's remain linearly independent by hypothesis, and hence the x's must also remain linearly independent.

Proposition 3.1. *Let K be a field containing another field k, and let $L \supset E$ be two other extensions of k. Then K and L are linearly disjoint over k if and only if K and E are linearly disjoint over k and KE, L are linearly disjoint over E.*



Proof. Assume first that K, E are linearly disjoint over k, and KE, L are linearly disjoint over E. Let $\{\kappa\}$ be a basis of K as vector space over k (we use the elements of this basis as their own indexing set), and let $\{\alpha\}$ be a basis of E over k. Let $\{\lambda\}$ be a basis of L over E. Then $\{\alpha\lambda\}$ is a basis of L over k. If K and L are not linearly disjoint over k, then there exists a relation

$$\sum_{\lambda,\alpha}\left(\sum_{\kappa} c_{\kappa\lambda\alpha}\kappa\right)\lambda\alpha = 0 \qquad \text{with some } c_{\kappa\lambda\alpha} \neq 0,\ c_{\kappa\lambda\alpha} \in k.$$

Changing the order of summation gives

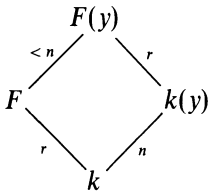
$$\sum_{\lambda}\left(\sum_{\kappa,\lambda} c_{\kappa\lambda\alpha}\kappa\alpha\right)\lambda = 0$$

contradicting the linear disjointness of L and KE over E.

Conversely, assume that K and L are linearly disjoint over k. Then *a fortiori*, K and E are also linearly disjoint over k, and the field KE is the quotient field of the ring $E[K]$ generated over E by all elements of K. This ring is a vector space over E, and a basis for K over k is also a basis for this ring $E[K]$ over E. With this remark, and the criteria for linear disjointness, we see that it suffices to prove that the elements of such a basis remain linearly independent over L. At this point we see that the arguments given in the first part of the proof are reversible. We leave the formalism to the reader.

We introduce another notion concerning two extensions K and L of a field k. We shall say that K is **free from L over k** if every finite set of elements of K algebraically independent over k remains such over L. If (x) and (y) are two sets of elements in Ω, we say that they are **free over k** (or **independent over k**) if $k(x)$ and $k(y)$ are free over k.

Just as with linear disjointness, our definition is unsymmetric, and we prove that the relationship expressed therein is actually symmetric. Assume therefore that K is free from L over k. Let $y_1, \ldots, y_n$ be elements of L, algebraically independent over k. Suppose they become dependent over K. They become so in a subfield F of K finitely generated over k, say of transcendence degree r over k. Computing the transcendence degree of $F(y)$ over k in two ways gives a contradiction (cf. Exercise 5).



Proposition 3.2. *If K and L are linearly disjoint over k, then they are free over k.*

Proof. Let $x_1, \ldots, x_n$ be elements of K algebraically independent over k. Suppose they become algebraically dependent over L. We get a relation

$$\sum y_a M_a(x) = 0$$

between monomials $M_a(x)$ with coefficients y_a in L. This gives a linear relation among the $M_a(x)$. But these are linearly independent over k because the x's are assumed algebraically independent over k. This is a contradiction.

Proposition 3.3. *Let L be an extension of k, and let $(u) = (u_1, \ldots, u_r)$ be a set of quantities algebraically independent over L. Then the field $k(u)$ is linearly disjoint from L over k.*

Proof. According to the criteria for linear disjointness, it suffices to prove that the elements of a basis for the ring $k[u]$ that are linearly independent over k remain so over L. In fact the monomials $M(u)$ give a basis of $k[u]$ over k. They must remain linearly independent over L, because as we have seen, a linear relation gives an algebraic relation. This proves our proposition.

Note finally that the property that two extensions K and L of a field k are linearly disjoint or free is of finite type. To prove that they have either property, it suffices to do it for all subfields K_0 and L_0 of K and L respectively which are finitely generated over k. This comes from the fact that the definitions involve only a finite number of quantities at a time.

§4. SEPARABLE AND REGULAR EXTENSIONS

Let K be a finitely generated extension of k, $K = k(x)$. We shall say that it is **separably generated** if we can find a transcendence basis $(t_1, \ldots, t_r)$ of K/k such that K is separably algebraic over $k(t)$. Such a transcendence base is said to be a **separating transcendence base** for K over k.

We always denote by p the characteristic if it is not 0. The field obtained from k by adjoining all p^m-th roots of all elements of k will be denoted by k^{1/p^m}. The compositum of all such fields for $m = 1, 2, \ldots$, is denoted by k^{1/p^∞}.

Proposition 4.1. *The following conditions concerning an extension field K of k are equivalent:*

(i) *K is linearly disjoint from k^{1/p^∞}.*
(ii) *K is linearly disjoint from k^{1/p^m} for some m.*

(iii) *Every subfield of K containing k and finitely generated over k is separably generated.*

Proof. It is obvious that (i) implies (ii). In order to prove that (ii) implies (iii), we may clearly assume that K is finitely generated over k, say

$$K = k(x) = k(x_1, \ldots, x_n).$$

Let the transcendence degree of this extension be r. If $r = n$, the proof is complete. Otherwise, say $x_1, \ldots, x_r$ is a transcendence base. Then x_{r+1} is algebraic over $k(x_1, \ldots, x_r)$. Let $f(X_1, \ldots, X_{r+1})$ be a polynomial of lowest degree such that

$$f(x_1, \ldots, x_{r+1}) = 0.$$

Then f is irreducible. We contend that not all x_i $(i = 1, \ldots, r+1)$ appear to the p-th power throughout. If they did, we could write $f(X) = \sum c_\alpha M_\alpha(X)^p$ where $M_\alpha(X)$ are monomials in $X_1, \ldots, X_{r+1}$ and $c_\alpha \in k$. This would imply that the $M_\alpha(x)$ are linearly dependent over $k^{1/p}$ (taking the p-th root of the equation $\sum c_\alpha M_\alpha(x)^p = 0$). However, the $M_\alpha(x)$ are linearly independent over k (otherwise we would get an equation for $x_1, \ldots, x_{r+1}$ of lower degree) and we thus get a contradiction to the linear disjointness of $k(x)$ and $k^{1/p}$. Say X_1 does not appear to the p-th power throughout, but actually appears in $f(X)$. We know that $f(X)$ is irreducible in $k[X_1, \ldots, X_{r+1}]$ and hence $f(x) = 0$ is an irreducible equation for x_1 over $k(x_2, \ldots, x_{r+1})$. Since X_1 does not appear to the p-th power throughout, this equation is a separable equation for x_1 over $k(x_2, \ldots, x_{r+1})$, in other words, x_1 is separable algebraic over $k(x_2, \ldots, x_{r+1})$. From this it follows that it is separable algebraic over $k(x_2, \ldots, x_n)$. If $(x_2, \ldots, x_n)$ is a transcendence base, the proof is complete. If not, say that x_2 is separable over $k(x_3, \ldots, x_n)$. Then $k(x)$ is separable over $k(x_3, \ldots, x_n)$. Proceeding inductively, we see that the procedure can be continued until we get down to a transcendence base. This proves that (ii) implies (iii). It also proves that a separating transcendence base for $k(x)$ over k can be selected from the given set of generators (x).

To prove that (iii) implies (i) we may assume that K is finitely generated over k. Let (u) be a transcendence base for K over k. Then K is separably algebraic over $k(u)$. By Proposition 3.3, $k(u)$ and k^{1/p^∞} are linearly disjoint. Let $L = k^{1/p^\infty}$. Then $k(u)L$ is purely inseparable over $k(u)$, and hence is linearly disjoint from K over $k(u)$ by the elementary theory of finite algebraic extensions. Using Proposition 3.1, we conclude that K is linearly disjoint from L over k, thereby proving our theorem.

An extension K of k satisfying the conditions of Proposition 4.1 is called **separable**. This definition is compatible with the use of the word for algebraic extensions.

The first condition of our theorem is known as **MacLane's criterion**. It has the following immediate corollaries.

Corollary 4.2. *If K is separable over k, and E is a subfield of K containing k, then E is separable over k.*

Corollary 4.3. *Let E be a separable extension of k, and K a separable extension of E. Then K is a separable extension of k.*

Proof. Apply Proposition 3.1 and the definition of separability.

Corollary 4.4. *If k is perfect, every extension of k is separable.*

Corollary 4.5. *Let K be a separable extension of k, and free from an extension L of k. Then KL is a separable extension of L.*

Proof. An element of KL has an expression in terms of a finite number of elements of K and L. Hence any finitely generated subfield of KL containing L is contained in a composite field FL, where F is a subfield of K finitely generated over k. By Corollary 4.2, we may assume that K is finitely generated over k. Let (t) be a transcendence base of K over k, so K is separable algebraic over $k(t)$. By hypothesis, (t) is a transcendence base of KL over L, and since every element of K is separable algebraic over $k(t)$, it is also separable over $L(t)$. Hence KL is separably generated over L. This proves the corollary.

Corollary 4.6. *Let K and L be two separable extensions of k, free from each other over k. Then KL is separable over k.*

Proof. Use Corollaries 4.5 and 4.3.

Corollary 4.7. *Let K, L be two extensions of k, linearly disjoint over k. Then K is separable over k if and only if KL is separable over L.*

Proof. If K is not separable over k, it is not linearly disjoint from $k^{1/p}$ over k, and hence *a fortiori* it is not linearly disjoint from $Lk^{1/p}$ over k. By Proposition 4.1, this implies that KL is not linearly disjoint from $Lk^{1/p}$ over L, and hence that KL is not separable over L. The converse is a special case of Corollary 4.5, taking into account that linearly disjoint fields are free.

We conclude our discussion of separability with two results. The first one has already been proved in the first part of Proposition 4.1, but we state it here explicitly.

Proposition 4.8. *If K is a separable extension of k, and is finitely generated, then a separating transcendence base can be selected from a given set of generators.*

To state the second result we denote by K^{p^m} the field obtained from K by raising all elements of K to the p^m-th power.

Proposition 4.9. *Let K be a finitely generated extension of a field k. If $K^{p^m}k = K$ for some m, then K is separably algebraic over k. Conversely, if K is separably algebraic over k, then $K^{p^m}k = K$ for all m.*

Proof. If K/k is separably algebraic, then the conclusion follows from the elementary theory of finite algebraic extensions. Conversely, if K/k is finite algebraic but not separable, then the maximal separable extension of k in K cannot be all of K, and hence K^pk cannot be equal to K. Finally, if there exists an element t of K transcendental over k, then $k(t^{1/p^m})$ has degree p^m over $k(t)$, and hence there exists a t such that t^{1/p^m} does not lie in K. This proves our proposition.

There is a class of extensions which behave particularly well from the point of view of changing the ground field, and are especially useful in algebraic geometry. We put some results together to deal with such extensions. Let K be an extension of a field k, with algebraic closure K^a. We claim that the following two conditions are equivalent:

REG 1. k is algebraically closed in K (i.e. every element of K algebraic over k lies in k), and K is separable over k.

REG 2. K is linearly disjoint from k^a over k.

We show the equivalence. Assume **REG 2**. By Proposition 4.1, we know that K is separably generated over k. It is obvious that k must be algebraically closed in K. Hence **REG 2** implies **REG 1**. To prove the converse we need a lemma.

Lemma 4.10. *Let k be algebraically closed in extension K. Let x be some element of an extension of K, but algebraic over k. Then $k(x)$ and K are linearly disjoint over k, and $[k(x):k] = [K(x):K]$.*

Proof. Let $f(X)$ be the irreducible polynomial for x over k. Then f remains irreducible over K; otherwise, its factors would have coefficients algebraic over k, hence in k. Powers of x form a basis of $k(x)$ over k, hence the same powers form a basis of $K(x)$ over K. This proves the lemma.

To prove **REG 2** from **REG 1**, we may assume without loss of generality that K is finitely generated over k, and it suffices to prove that K is linearly disjoint from an arbitrary finite algebraic extension L of k. If L is separable algebraic over k, then it can be generated by one primitive element, and we can apply Lemma 4.10.

More generally, let E be the maximal separable subfield of L containing k. By Proposition 3.1, we see that it suffices to prove that KE and L are linearly disjoint over E. Let (t) be a separating transcendence base for K over k. Then K is separably algebraic over $k(t)$. Furthermore, (t) is also a separating transcendence base for KE over E, and KE is separable algebraic

over $E(t)$. Thus KE is separable over E, and by definition KE is linearly disjoint from L over K because L is purely inseparable over E. This proves that **REG 1** implies **REG 2**.

Thus we can define an extension K of k to be **regular** if it satisfies either one of the equivalent conditions **REG 1** or **REG 2**.

Proposition 4.11.

(a) *Let K be a regular extension of k, and let E be a subfield of K containing k. Then E is regular over k.*
(b) *Let E be a regular extension of k, and K a regular extension of E. Then K is a regular extension of k.*
(c) *If k is algebraically closed, then every extension of k is regular.*

Proof. Each assertion is immediate from the definition conditions **REG 1** and **REG 2**.

Theorem 4.12. *Let K be a regular extension of k, let L be an arbitrary extension of k, both contained in some larger field, and assume that K, L are free over k. Then K, L are linearly disjoint over k.*

Proof (Artin). Without loss of generality, we may assume that K is finitely generated over k. Let $x_1, \ldots, x_n$ be elements of K linearly independent over k. Suppose we have a relation of linear dependence

$$x_1 y_1 + \cdots + x_n y_n = 0$$

with $y_i \in L$. Let φ be a k^a-valued place of L over k. Let (t) be a transcendence base of K over k. By hypothesis, the elements of (t) remain algebraically independent over L, and hence φ can be extended to a place of KL which is identity on $k(t)$. This place must then be an isomorphism of K on its image, because K is a finite algebraic extension of $k(t)$ (remark at the end of Chapter VII, §3). After a suitable isomorphism, we may take a place equivalent to φ which is the identity on K. Say $\varphi(y_i/y_n)$ is finite for all i (use Proposition 3.4 of Chapter VII). We divide the relation of linear dependence by y_n and apply φ to get $\sum x_i \varphi(y_i/y_n) = 0$, which gives a linear relation among the x_i with coefficients in k^a, contradicting the linear disjointness. This proves the theorem.

Theorem 4.13. *Let K be a regular extension of k, free from an extension L of k over k. Then KL is a regular extension of L.*

Proof. From the hypothesis, we deduce that K is free from the algebraic closure L^a of L over k. By Theorem 4.12, K is linearly disjoint from L^a over k. By Proposition 3.1, KL is linearly disjoint from L^a over L, and hence KL is regular over L.

Corollary 4.14. *Let K, L be regular extensions of k, free from each other over k. Then KL is a regular extension of k.*

Proof. Use Corollary 4.13 and Proposition 4.11(b).

Theorem 4.13 is one of the main reasons for emphasizing the class of regular extensions: they remain regular under arbitrary base change of the ground field k. Furthermore, Theorem 4.12 in the background is important in the study of polynomial ideals as in the next section, and we add some remarks here on its implications. We now assume that the reader is acquainted with the most basic properties of the tensor product (Chapter XVI, §1 and §2).

Corollary 4.15. *Let $K = k(x)$ be a finitely generated regular extension, free from an extension L of k, and both contained in some larger field. Then the natural k-algebra homomorphism*

$$L \otimes_k k[x] \to L[x]$$

is an isomorphism.

Proof. By Theorem 4.12 the homomorphism is injective, and it is obviously surjective, whence the corollary follows.

Corollary 4.16. *Let $k(x)$ be a finitely generated regular extension, and let $\mathfrak{p}$ be the prime ideal in $k[X]$ vanishing on (x), that is, consisting of all polynomials $f(X) \in k[X]$ such that $f(x) = 0$. Let L be an extension of k, free from $k(x)$ over k. Let $\mathfrak{p}_L$ be the prime ideal in $L[X]$ vanishing on (x). Then $\mathfrak{p}_L = \mathfrak{p}L[X]$, that is $\mathfrak{p}_L$ is the ideal generated by $\mathfrak{p}$ in $L[X]$, and in particular, this ideal is prime.*

Proof. Consider the exact sequence

$$0 \to \mathfrak{p} \to k[X] \to k[x] \to 0.$$

Since we are dealing with vector spaces over a field, the sequence remains exact when tensored with any k-space, so we get an exact sequence

$$0 \to L \otimes_k \mathfrak{p} \to L[X] \to L \otimes_k k[x] \to 0.$$

By Corollary 4.15, we know that $L \otimes_k k[x] \approx L[x]$, and the image of $L \otimes_k \mathfrak{p}$ in $L[X]$ is $\mathfrak{p}L[X]$, so the lemma is proved.

Corollary 4.16 shows another aspect whereby regular extensions behave well under extension of the base field, namely the way the prime ideal $\mathfrak{p}$ remains prime under such extensions.

§5. DERIVATIONS

A **derivation** D of a ring R is a mapping $D: R \to R$ of R into itself which is linear and satisfies the ordinary rule for derivatives, i.e.,

$$D(x + y) = Dx + Dy \qquad \text{and} \qquad D(xy) = xDy + yDx.$$

As an example of derivations, consider the polynomial ring $k[X]$ over a field k. For each variable X_i, the partial derivative $\partial/\partial X_i$ taken in the usual manner is a derivation of $k[X]$.

Let R be an entire ring and let K be its quotient field. Let $D: R \to R$ be a derivation. Then D extends uniquely to a derivation of K, by defining

$$D(u/v) = \frac{vDu - uDv}{v^2}.$$

It is immediately verified that the expression on the right-hand side is independent of the way we represent an element of K as u/v $(u, v \in R)$, and satisfies the conditions defining a derivation.

Note. In this section, we shall discuss derivations of fields. For derivations in the context of rings and modules, see Chapter XIX, §3.

A derivation of a field K is **trivial** if $Dx = 0$ for all $x \in K$. It is trivial **over a subfield** k of K if $Dx = 0$ for all $x \in k$. A derivation is always trivial over the prime field: One sees that

$$D(1) = D(1 \cdot 1) = 2D(1),$$

whence $D(1) = 0$.

We now consider the problem of extending derivations. Let

$$L = K(x) = K(x_1, \ldots, x_n)$$

be a finitely generated extension. If $f \in K[X]$, we denote by $\partial f/\partial x_i$ the polynomials $\partial f/\partial X_i$ evaluated at (x). Given a derivation D on K, does there exist a derivation D^* on L coinciding with D on K? If $f(X) \in K[X]$ is a polynomial vanishing on (x), then any such D^* must satisfy

$$0 = D^*f(x) = f^D(x) + \sum (\partial f/\partial x_i) D^*x_i, \tag{1}$$

where f^D denotes the polynomial obtained by applying D to all coefficients of f. Note that if relation (1) is satisfied for every element in a finite set of generators of the ideal in $K[X]$ vanishing on (x), then (1) is satisfied by every polynomial of this ideal. This is an immediate consequence of the rules for derivations. The preceding ideal will also be called the ideal determined by (x) in $K[X]$.

The above necessary condition for the existence of a D^* turns out to be sufficient.

Theorem 5.1. *Let D be a derivation of a field K. Let*

$$(x) = (x_1, \ldots, x_n)$$

be a finite family of elements in an extension of K. Let $\{f_\alpha(X)\}$ be a set of generators for the ideal determined by (x) in $K[X]$. Then, if (u) is any set of elements of $K(x)$ satisfying the equations

$$0 = f_\alpha^D(x) + \sum (\partial f_\alpha/\partial x_i)u_i,$$

there is one and only one derivation D^* of $K(x)$ coinciding with D on K, and such that $D^*x_i = u_i$ for every i.

Proof. The necessity has been shown above. Conversely, if $g(x)$, $h(x)$ are in $K[x]$, and $h(x) \neq 0$, one verifies immediately that the mapping D^* defined by the formulas

$$D^*g(x) = g^D(x) + \sum \frac{\partial g}{\partial x_i} u_i,$$

$$D^*(g/h) = \frac{hD^*g - gD^*h}{h^2},$$

is well defined and is a derivation of $K(x)$.

Consider the special case where (x) consists of one element x. Let D be a given derivation on K.

Case 1. x is separable algebraic over K. Let $f(X)$ be the irreducible polynomial satisfied by x over K. Then $f'(x) \neq 0$. We have

$$0 = f^D(x) + f'(x)u,$$

whence $u = -f^D(x)/f'(x)$. Hence D extends to $K(x)$ uniquely. If D is trivial on K, then D is trivial on $K(x)$.

Case 2. x is transcendental over K. Then D extends, and u can be selected arbitrarily in $K(x)$.

Case 3. x is purely inseparable over K, so $x^p - a = 0$, with $a \in K$. Then D extends to $K(x)$ if and only if $Da = 0$. In particular if D is trivial on K, then u can be selected arbitrarily.

Proposition 5.2. *A finitely generated extension $K(x)$ over K is separable algebraic if and only if every derivation D of $K(x)$ which is trivial on K is trivial on $K(x)$.*

Proof. If $K(x)$ is separable algebraic over K, this is Case 1. Conversely, if it is not, we can make a tower of extensions between K and $K(x)$, such

that each step is covered by one of the three above cases. At least one step will be covered by Case 2 or 3. Taking the uppermost step of this latter type, one sees immediately how to construct a derivation trivial on the bottom and nontrivial on top of the tower.

Proposition 5.3. *Given K and elements $(x) = (x_1, \ldots, x_n)$ in some extension field, assume that there exist n polynomials $f_i \in K[X]$ such that:*

(i) $f_i(x) = 0$, *and*
(ii) $\det(\partial f_i/\partial x_j) \neq 0$.

Then (x) is separably algebraic over K.

Proof. Let D be a derivation on $K(x)$, trivial on K. Having $f_i(x) = 0$ we must have $Df_i(x) = 0$, whence the Dx_i satisfy n linear equations such that the coefficient matrix has non-zero determinant. Hence $Dx_i = 0$, so D is trivial on $K(x)$. Hence $K(x)$ is separable algebraic over K by Proposition 5.2.

The following proposition will follow directly from Cases 1 and 2.

Proposition 5.4. *Let $K = k(x)$ be a finitely generated extension of k. An element z of K is in $K^p k$ if and only if every derivation D of K over k is such that $Dz = 0$.*

Proof. If z is in $K^p k$, then it is obvious that every derivation D of K over k vanishes on z. Conversely, if $z \notin K^p k$, then z is purely inseparable over $K^p k$, and by Case 3 of the extension theorem, we can find a derivation D trivial on $K^p k$ such that $Dz = 1$. This derivation is at first defined on the field $K^p k(z)$. One can extend it to K as follows. Suppose there is an element $w \in K$ such that $w \notin K^p k(z)$. Then $w^p \in K^p k$, and D vanishes on w^p. We can then again apply Case 3 to extend D from $K^p k(z)$ to $K^p k(z, w)$. Proceeding stepwise, we finally reach K, thus proving our proposition.

The derivations D of a field K form a vector space over K if we define zD for $z \in K$ by $(zD)(x) = zDx$.

Let K be a finitely generated extension of k, of dimension r over k. We denote by $\mathfrak{D}$ the K-vector space of derivations D of K over k (derivations of K which are trivial on k). For each $z \in K$, we have a pairing

$$(D, z) \mapsto Dz$$

of $(\mathfrak{D}, K)$ into K. Each element z of K gives therefore a K-linear functional of $\mathfrak{D}$. This functional is denoted by dz. We have

$$d(yz) = y\,dz + z\,dy,$$

$$d(y + z) = dy + dz.$$

These linear functionals form a subspace $\mathfrak{F}$ of the dual space of $\mathfrak{D}$, if we define $y\,dz$ by $(D, y\,dz) \mapsto yDz$.

Proposition 5.5. *Assume that K is a separably generated and finitely generated extension of k of transcendence degree r. Then the vector space $\mathfrak{D}$ (over K) of derivations of K over k has dimension r. Elements $t_1, \ldots, t_r$ of K from a separating transcendence base of K over k if and only if $dt_1, \ldots, dt_r$ form a basis of the dual space of $\mathfrak{D}$ over K.*

Proof. If $t_1, \ldots, t_r$ is a separating transcendence base for K over k, then we can find derivations $D_1, \ldots, D_r$ of K over k such that $D_i t_j = \delta_{ij}$, by Cases 1 and 2 of the extension theorem. Given $D \in \mathfrak{D}$, let $w_i = Dt_i$. Then clearly $D = \sum w_i D_i$, and so the D_i form a basis for $\mathfrak{D}$ over K, and the dt_i form the dual basis. Conversely, if $dt_1, \ldots, dt_r$ is a basis for $\mathfrak{F}$ over K, and if K is not separably generated over $k(t)$, then by Cases 2 and 3 we can find a derivation D which is trivial on $k(t)$ but nontrivial on K. If $D_1, \ldots, D_r$ is the dual basis of $dt_1, \ldots, dt_r$ (so $D_i t_j = \delta_{ij}$) then $D, D_1, \ldots, D_r$ would be linearly independent over K, contradicting the first part of the theorem.

Corollary 5.6. *Let K be a finitely generated and separably generated extension of k. Let z be an element of K transcendental over k. Then K is separable over $k(z)$ if and only if there exists a derivation D of K over k such that $Dz \neq 0$.*

Proof. If K is separable over $k(z)$, then z can be completed to a separating base of K over k and we can apply the proposition. If $Dz \neq 0$, then $dz \neq 0$, and we can complete dz to a basis of $\mathfrak{F}$ over K. Again from the proposition, it follows that K will be separable over $k(z)$.

Note. Here we have discussed derivations of fields. For derivations in the context of rings and modules, see Chapter XVI.

As an application, we prove:

Theorem 5.7. (Zariski–Matsusaka). *Let K be a finitely generated separable extension of a field k. Let $y, z \in K$ and $z \notin K^p k$ if the characteristic is $p > 0$. Let u be transcendental over K, and put $k_u = k(u)$, $K_u = K(u)$.*

(a) *For all except possibly one value of $c \in k$, K is a separable extension of $k(y + cz)$. Furthermore, K_u is separable over $k_u(y + uz)$.*

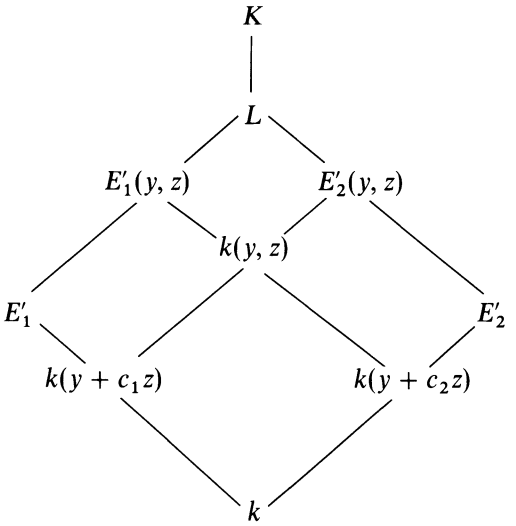
(b) *Assume that K is regular over k, and that its transcendence degree is at least 2. Then for all but a finite number of elements $c \in k$, K is a regular extension of $k(y + cz)$. Furthermore, K_u is regular over $k_u(y + uz)$.*

Proof. We shall use throughout the fact that a subfield of a finitely generated extension is also finitely generated (see Exercise 4).

If w is an element of K, and if there exists a derivation D of K over k such that $Dw \neq 0$, then K is separable over $k(w)$, by Corollary 5.6. Also by Corollary 5.6, there exists D such that $Dz \neq 0$. Then for all elements $c \in k$, except possibly one, we have $D(y + cz) = Dy + cDz \neq 0$. Also we may extend D to K_u over k_u by putting $Du = 0$, and then one sees that

$D(y+uz)= Dy + uDz \neq 0$, so K is separable over $k(y + cz)$ except possibly for one value of c, and K_u is separable over $k_u(y + uz)$. In what follows, we assume that the constants $c_1, c_2, \ldots$ are different from the exceptional constant, and hence that K is separable over $k(y + c_i z)$ for $i = 1, 2$.

Assume next that K is regular over k and that the transcendence degree is at least 2. Let $E_i = k(y + c_i z)$ $(i = 1, 2)$ and let E_i' be the algebraic closure of E_i in K. We must show that $E_i' = E_i$ for all but a finite number of constants. Note that $k(y, z) = E_1 E_2$ is the compositum of E_1 and E_2, and that $k(y, z)$ has transcendence degree 2 over k. Hence E_1' and E_2' are free over k. Being subfields of a regular extension of k, they are regular over k, and are therefore linearly disjoint by Theorem 4.12.



By construction, E_1' and E_2' are finite separable algebraic extensions of E_1 and E_2 respectively. Let L be the separable algebraic closure of $k(y, z)$ in K. There is only a finite number of intermediate fields between $k(y, z)$ and L. Furthermore, by Proposition 3.1 the fields $E_1'(y, z)$ and $E_2'(y, z)$ are linearly disjoint over $k(y, z)$. Let c_1 range over the finite number of constants which will exhaust the intermediate extensions between L and $k(y, z)$ obtainable by lifting over $k(y, z)$ a field of type E_i'. If c_2 is now chosen different from any one of these constants c_1, then the only way in which the condition of linear disjointness mentioned above can be compatible with our choice of c_2 is that $E_2'(y, z) = k(y, z)$, i.e. that $E_2' = k(y + c_2 z)$. This means that $k(y + c_2 z)$ is algebraically closed in K, and hence that K is regular over $k(y + c_2 z)$.

As for K_u, let $u_1, u_2, \ldots$ be infinitely many elements algebraically independent over K. Let $k' = k(u_1, u_2, \ldots)$ and $K' = K(u_1, u_2, \ldots)$ be the fields obtained by adjoining these elements to k and K respectively. By what has already been proved, we know that K' is regular over $k'(u + u_i z)$ for all but a finite number of integers i, say for $i = 1$. Our assertion (a) is then a consequence of Corollary 4.14. This concludes the proof of Theorem 5.7.

Theorem 5.8. *Let $K = k(x_1, \ldots, x_n) = k(x)$ be a finitely generated regular extension of a field k. Let $u_1, \ldots, u_n$ be algebraically independent over $k(x)$. Let*

$$u_{n+1} = u_1 x_1 + \cdots + u_n x_n,$$

and let $k_u = k(u_1, \ldots, u_n, u_{n+1})$. Then $k_u(x)$ is separable over k_u, and if the transcendence degree of $k(x)$ over k is $\geqq 2$, then $k_u(x)$ is regular over k_u.

Proof. By the separability of $k(x)$ over k, some x_i does not lie in $K^p k$, say $x_n \notin K^p k$. Then we take

$$y = u_1 x_1 + \cdots + u_{n-1} x_{n-1} \qquad \text{and} \qquad z = x_n,$$

so that $u_{n+1} = y + u_n z$, and we apply Theorem 5.7 to conclude the proof.

Remark. In the geometric language of the next chapter, Theorem 5.8 asserts that the intersection of a k-variety with a generic hyperplane

$$u_1 X_1 + \cdots + u_n X_n - u_{n+1} = 0$$

is a k_u-variety, if the dimension of the k-variety is $\geqq 2$. In any case, the extension $k_u(x)$ is separable over k_u.

EXERCISES

1. Prove that the complex numbers have infinitely many automorphisms. [*Hint*: Use transcendence bases.] Describe all automorphisms and their cardinality.

2. A subfield k of a field K is said to be algebraically closed in K if every element of K which is algebraic over k is contained in k. Prove: If k is algebraically closed in K, and K, L are free over k, and L is separable over k or K is separable over k, then L is algebraically closed in KL.

3. Let $k \subset E \subset K$ be extension fields. Show that

$$\text{tr. deg. } (K/k) = \text{tr. deg. } (K/E) + \text{tr. deg. } (E/k).$$

If $\{x_i\}$ is a transcendence base of E/k, and $\{y_j\}$ is a transcendence base of K/E, then $\{x_i, y_j\}$ is a transcendence base of K/k.

4. Let K/k be a finitely generated extension, and let $K \supset E \supset k$ be a subextension. Show that E/k is finitely generated.

5. Let k be a field and $k(x_1, \ldots, x_n) = k(x)$ a finite separable extension. Let $u_1, \ldots, u_n$ be algebraically independent over k. Let

$$w = u_1 x_1 + \cdots + u_n x_n.$$

Let $k_u = k(u_1, \ldots, u_n)$. Show that $k_u(w) = k_u(x)$.

6. Let $k(x) = k(x_1, \ldots, x_n)$ be a separable extension of transcendence degree $r \geqq 1$. Let u_{ij} $(i = 1, \ldots, r;\ j = 1, \ldots, n)$ be algebraically independent over $k(x)$. Let

$$y_i = \sum_{j=1}^{n} u_{ij} x_j.$$

Let $k_u = k(u_{ij})_{\text{all } i,j}$.

(a) Show that $k_u(x)$ is separable algebraic over $k_u(y_1, \ldots, y_r)$.

(b) Show that there exists a polynomial $P(u) \in k[u]$ having the following property. Let $(c) = (c_{ij})$ be elements of k such that $P(c) \neq 0$. Let

$$y_i' = \sum_{j=1}^{n} c_{ij} x_j.$$

Then $k(x)$ is separable algebraic over $k(y')$.

7. Let k be a field and $k[x_1, \ldots, x_n] = R$ a finitely generated entire ring over k with quotient field $k(x)$. Let L be a finite extension of $k(x)$. Let I be the integral closure of R in L. Show that I is a finite R-module. [Use Noether normalization, and deal with the inseparability problem and the separable case in two steps.]

8. Let D be a derivation of a field K. Then $D^n\colon K \to K$ is a linear map. Let $P_n = \operatorname{Ker} D^n$, so P_n is an additive subgroup of K. An element $x \in K$ is called a **logarithmic derivative** (in K) if there exists $y \in K$ such that $x = Dy/y$. Prove:

(a) An element $x \in K$ is the logarithmic derivative of an element $y \in P_n$ but $y \notin P_{n-1}$ $(n > 0)$ if and only if

$$(D + x)^n(1) = 0 \qquad \text{and} \qquad (D + x)^{n-1}(1) \neq 0.$$

(b) Assume that $K = \bigcup P_n$, i.e. given $x \in K$ then $x \in P_n$ for some $n > 0$. Let F be a subfield of K such that $DF \subset F$. Prove that x is a logarithmic derivative in F if and only if x is a logarithmic derivative in K. [*Hint*: If $x = Dy/y$ then $(D + x) = y^{-1}D \circ y$ and conversely.]

9. Let k be a field of characteristic 0, and let $z_1, \ldots, z_r$ be algebraically independent over k. Let (e_{ij}), $i = 1, \ldots, m$ and $j = 1, \ldots, r$ be a matrix of integers with $r \geqq m$, and assume that this matrix has rank m. Let

$$w_i = z_1^{e_{i1}} \cdots z_r^{e_{ir}} \qquad \text{for} \quad i = 1, \ldots, m.$$

Show that $w_1, \ldots, w_m$ are algebraically independent over k. [*Hint*: Consider the K-homomorphism mapping the K-space of derivations of K/k into $K^{(r)}$ given by

$$D \mapsto (Dz_1/z_1, \ldots, Dz_r/z_r),$$

and derive a linear condition for those D vanishing on $k(w_1, \ldots, w_m)$.]

10. Let k, (z) be as in Exercise 9. Show that if P is a rational function then

$$d(P(z)) = \operatorname{grad} P(z) \cdot dz,$$

using vector notation, i.e. $dz = (dz_1, \ldots, dz_r)$ and $\operatorname{grad} P = (D_1 P, \ldots, D_r P)$. Define $d \log P$ and express it in terms of coordinates. If P, Q are rational functions in $k(z)$ show that

$$d \log(PQ) = d \log P + d \log Q.$$

CHAPTER IX

Algebraic Spaces

This chapter gives the basic results concerning solutions of polynomial equations in several variables over a field k. First it will be proved that if such equations have a common zero in some field, then they have a common zero in the algebraic closure of k, and such a zero can be obtained by the process known as specialization. However, it is useful to deal with transcendental extensions of k as well. Indeed, if $\mathfrak{p}$ is a prime ideal in $k[X] = k[X_1, \ldots, X_n]$, then $k[X]/\mathfrak{p}$ is a finitely generated ring over k, and the images x_i of X_i in this ring may be transcendental over k, so we are led to consider such rings.

Even if we want to deal only with polynomial equations over a field, we are led in a natural way to deal with equations over the integers $\mathbf{Z}$. Indeed, if the equations are homogeneous in the variables, then we shall prove in §3 and §4 that there are universal polynomials in their coefficients which determine whether these equations have a common zero or not. "Universal" means that the coefficients are integers, and any given special case comes from specializing these universal polynomials to the special case.

Being led to consider polynomial equations over $\mathbf{Z}$, we then consider ideals $\mathfrak{a}$ in $\mathbf{Z}[X]$. The zeros of such an ideal form what is called an algebraic space. If $\mathfrak{p}$ is a prime ideal, the zeros of $\mathfrak{p}$ form what is called an arithmetic variety. We shall meet the first example in the discussion of elimination theory, for which I follow van der Waerden's treatment in the first two editions of his *Moderne Algebra*, Chapter XI.

However, when taking the polynomial ring $\mathbf{Z}[X]/\mathfrak{a}$ for some ideal $\mathfrak{a}$, it usually happens that such a factor ring has divisors of zero, or even nilpotent elements. Thus it is also natural to consider arbitrary commutative rings, and to lay the foundations of algebraic geometry over arbitrary commutative rings as did Grothendieck. We give some basic definitions for this purpose in §5. Whereas the present chapter gives the flavor of algebraic geometry dealing with specific polynomial ideals, the next chapter gives the flavor of geometry developing from commutative algebra, and its systematic application to the more general cases just mentioned.

S. Lang, *Algebra*
© Springer Science+Business Media LLC 2002

The present chapter and the next will also serve the purpose of giving the reader an introduction to books on algebraic geometry, notably Hartshorne's systematic basic account. For instance, I have included those results which are needed for Hartshorne's Chapter I and II.

§1. HILBERT'S NULLSTELLENSATZ

The Nullstellensatz has to do with a special case of the extension theorem for homomorphisms, applied to finitely generated rings over fields.

Theorem 1.1. *Let k be a field, and let $k[x] = k[x_1, \ldots, x_n]$ be a finitely generated ring over k. Let $\varphi : k \to L$ be an embedding of k into an algebraically closed field L. Then there exists an extension of φ to a homomorphism of $k[x]$ into L.*

Proof. Let $\mathfrak{M}$ be a maximal ideal of $k[x]$. Let σ be the canonical homomorphism $\sigma : k[x] \to k[x]/\mathfrak{M}$. Then $\sigma k[\sigma x_1, \ldots, \sigma x_n]$ is a field, and is in fact an extension field of σk. If we can prove our theorem when the finitely generated ring is in fact a field, then we apply $\varphi \circ \sigma^{-1}$ on σk and extend this to a homomorphism of $\sigma k[\sigma x_1, \ldots, \sigma x_n]$ into L to get what we want.

Without loss of generality, we therefore assume that $k[x]$ is a field. If it is algebraic over k, we are done (by the known result for algebraic extensions). Otherwise, let $t_1, \ldots, t_r$ be a transcendence basis, $r \geqq 1$. Without loss of generality, we may assume that φ is the identity on k. Each element $x_1, \ldots, x_n$ is algebraic over $k(t_1, \ldots, t_r)$. If we multiply the irreducible polynomial $\mathrm{Irr}(x_i, k(t), X)$ by a suitable non-zero element of $k[t]$, then we get a polynomial all of whose coefficients lie in $k[t]$. Let $a_1(t), \ldots, a_n(t)$ be the set of the leading coefficients of these polynomials, and let $a(t)$ be their product,

$$a(t) = a_1(t) \cdots a_n(t).$$

Since $a(t) \neq 0$, there exist elements $t_1', \ldots, t_r' \in k^a$ such that $a(t') \neq 0$, and hence $a_i(t') \neq 0$ for any i. Each x_i is integral over the ring

$$k\left[t_1, \ldots, t_r, \frac{1}{a_1(t)}, \ldots, \frac{1}{a_r(t)}\right].$$

Consider the homomorphism

$$\varphi : k[t_1, \ldots, t_r] \to k^a$$

such that φ is the identity on k, and $\varphi(t_j) = t_j'$. Let $\mathfrak{p}$ be its kernel. Then $a(t) \notin \mathfrak{p}$.

Our homomorphism φ extends uniquely to the local ring $k[t]_{\mathfrak{p}}$ and by the preceding remarks, it extends to a homomorphism of

$$k[t]_{\mathfrak{p}}[x_1, \ldots, x_n]$$

into k^a, using Proposition 3.1 of Chapter VII. This proves what we wanted.

Corollary 1.2. *Let k be a field and $k[x_1, \ldots, x_n]$ a finitely generated extension ring of k. If $k[x]$ is a field, then $k[x]$ is algebraic over k.*

Proof. All homomorphisms of a field are isomorphisms (onto the image), and there exists a homomorphism of $k[x]$ over k into the algebraic closure of k.

Corollary 1.3. *Let $k[x_1, \ldots, x_n]$ be a finitely generated entire ring over a field k, and let $y_1, \ldots, y_m$ be non-zero elements of this ring. Then there exists a homomorphism*

$$\psi : k[x] \to k^a$$

over k such that $\psi(y_j) \neq 0$ for all $j = 1, \ldots, m$.

Proof. Consider the ring $k[x_1, \ldots, x_n, y_1^{-1}, \ldots, y_m^{-1}]$ and apply the theorem to this ring.

Let S be a set of polynomials in the polynomial ring $k[X_1, \ldots, X_n]$ in n variables. Let L be an extension field of k. By a **zero** of S in L one means an n-tuple of elements $(c_1, \ldots, c_n)$ in L such that

$$f(c_1, \ldots, c_n) = 0$$

for all $f \in S$. If S consists of one polynomial f, then we also say that (c) is a zero of f. The set of all zeros of S is called an **algebraic set** in L (or more accurately in $L^{(n)}$). Let $\mathfrak{a}$ be the ideal generated by all elements of S. Since $S \subset \mathfrak{a}$ it is clear that every zero of $\mathfrak{a}$ is also a zero of S. However, the converse obviously holds, namely every zero of S is also a zero of $\mathfrak{a}$ because every element of $\mathfrak{a}$ is of type

$$g_1(X)f_1(X) + \cdots + g_m(X)f_m(X)$$

with $f_j \in S$ and $g_i \in k[X]$. Thus when considering zeros of a set S, we may just consider zeros of an ideal. We note parenthetically that every ideal is finitely generated, and so every algebraic set is the set of zeros of a finite number of polynomials. As another corollary of Theorem 1.1, we get:

Theorem 1.4. *Let $\mathfrak{a}$ be an ideal in $k[X] = k[X_1, \ldots, X_n]$. Then either $\mathfrak{a} = k[X]$ or $\mathfrak{a}$ has a zero in k^a.*

Proof. Suppose $\mathfrak{a} \neq k[X]$. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$, and $k[X]/\mathfrak{m}$ is a field, which is a finitely generated extension of k, because it is generated by the images of $X_1, \ldots, X_n \bmod \mathfrak{m}$. By Corollary 2.2, this field is algebraic over k, and can therefore be embedded in the algebraic closure k^a. The homomorphism on $k[X]$ obtained by the composition of the canonical map mod $\mathfrak{m}$, followed by this embedded gives the desired zero of $\mathfrak{a}$, and concludes the proof of the theorem.

In §3 we shall consider conditions on a family of polynomials to have a common zero. Theorem 1.4 implies that if they have a common zero in some field, then they have a common zero in the algebraic closure of the field generated by their coefficients over the prime field.

Theorem 1.5. (Hilbert's Nullstellensatz). *Let $\mathfrak{a}$ be an ideal in $k[X]$. Let f be a polynomial in $k[X]$ such that $f(c) = 0$ for every zero $(c) = (c_1, \ldots, c_n)$ of $\mathfrak{a}$ in k^a. Then there exists an integer $m > 0$ such that $f^m \in \mathfrak{a}$.*

Proof. We may assume that $f \neq 0$. We use the Rabinowitsch trick of introducing a new variable Y, and of considering the ideal $\mathfrak{a}'$ generated by $\mathfrak{a}$ and $1 - Yf$ in $k[X, Y]$. By Theorem 1.4, and the current assumption, the ideal $\mathfrak{a}'$ must be the whole polynomial ring $k[X, Y]$, so there exist polynomials $g_i \in k[X, Y]$ and $h_i \in \mathfrak{a}$ such that

$$1 = g_0(1 - Yf) + g_1h_1 + \cdots + g_rh_r.$$

We substitute f^{-1} for Y and multiply by an appropriate power f^m of f to clear denominators on the right-hand side. This concludes the proof.

For questions involving how effective the Nullstellensatz can be made, see the following references also related to the discussion of elimination theory discussed later in this chapter.

Bibliography

[BeY 91] C. BERENSTEIN and A. YGER, Effective Bezout identities in $\mathbf{Q}[z_1, \ldots, z_n]$, *Acta Math.* **166** (1991), pp. 69–120

[Br 87] D. BROWNAWELL, Bounds for the degree in Nullstellensatz, *Ann. of Math.* **126** (1987), pp. 577–592

[Br 88] D. BROWNAWELL, Local diophantine nullstellen inequalities, *J. Amer. Math. Soc.* **1** (1988), pp. 311–322

[Br 89] D. BROWNAWELL, Applications of Cayley-Chow forms, *Springer Lecture Notes* **1380:** *Number Theory, Ulm 1987*, H. P. Schlickewei and E. Wirsing (eds.), pp. 1–18

[Ko 88] J. KOLLAR, Sharp effective nullstellensatz, *J. Amer. Math. Soc.* **1 No. 4** (1988), pp. 963–975

§2. ALGEBRAIC SETS, SPACES AND VARIETIES

We shall make some very elementary remarks on algebraic sets. Let k be a field, and let A be an algebraic set of zeros in some fixed algebraically closed extension field of k. The set of all polynomials $f \in k[X_1, \ldots, X_n]$ such that $f(x) = 0$ for all $(x) \in A$ is obviously an ideal $\mathfrak{a}$ in $k[X]$, and is determined by A. We shall call it the ideal **belonging** to A, or say that it is **associated** with A. If A is the set of zeros of a set S of polynomials, then $S \subset \mathfrak{a}$, but $\mathfrak{a}$ may be bigger than S. On the other hand, we observe that A is also the set of zeros of $\mathfrak{a}$.

Let A, B be algebraic sets, and $\mathfrak{a}$, $\mathfrak{b}$ their associated ideals. Then it is clear that $A \subset B$ if and only if $\mathfrak{a} \supset \mathfrak{b}$. Hence $A = B$ if and only if $\mathfrak{a} = \mathfrak{b}$. This has an important consequence. Since the polynomial ring $k[X]$ is Noetherian, it follows that algebraic sets satisfy the dual property, namely every descending sequence of algebraic sets

$$A_1 \supset A_2 \supset \cdots$$

must be such that $A_m = A_{m+1} = \cdots$ for some integer m, i.e. all A_v are equal for $v \geqq m$. Furthermore, dually to another property characterizing the Noetherian condition, we conclude that every non-empty set of algebraic sets contains a minimal element.

Theorem 2.1. *The finite union and the finite intersection of algebraic sets are algebraic sets. If A, B are the algebraic sets of zeros of ideals $\mathfrak{a}$, $\mathfrak{b}$, respectively, then $A \cup B$ is the set of zeros of $\mathfrak{a} \cap \mathfrak{b}$ and $A \cap B$ is the set of zeros of $(\mathfrak{a}, \mathfrak{b})$.*

Proof. We first consider $A \cup B$. Let $(x) \in A \cup B$. Then (x) is a zero of $\mathfrak{a} \cap \mathfrak{b}$. Conversely, let (x) be a zero of $\mathfrak{a} \cap \mathfrak{b}$, and suppose $(x) \notin A$. There exists a polynomial $f \in \mathfrak{a}$ such that $f(x) \neq 0$. But $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ and hence $(fg)(x) = 0$ for all $g \in \mathfrak{b}$, whence $g(x) = 0$ for all $g \in \mathfrak{b}$. Hence (x) lies in B, and $A \cup B$ is an algebraic set of zeros of $\mathfrak{a} \cap \mathfrak{b}$.

To prove that $A \cap B$ is an algebraic set, let $(x) \in A \cap B$. Then (x) is a zero of $(\mathfrak{a}, \mathfrak{b})$. Conversely, let (x) be a zero of $(\mathfrak{a}, \mathfrak{b})$. Then obviously $(x) \in A \cap B$, as desired. This proves our theorem.

An algebraic set V is called ***k*-irreducible** if it cannot be expressed as a union $V = A \cup B$ of algebraic sets A, B with A, B distinct from V. We also say irreducible instead of ***k*-irreducible**.

Theorem 2.2. *Let A be an algebraic set.*

(i) *Then A can be expressed as a finite union of irreducible algebraic sets $A = V_1 \cup \ldots \cup V_r$.*

(ii) *If there is no inclusion relation among the V_i, i.e. if $V_i \not\subset V_j$ for $i \neq j$, then the representation is unique.*

(iii) *Let $W, V_1, \ldots, V_r$ be irreducible algebraic sets such that*

$$W \subset V_1 \cup \ldots \cup V_r.$$

Then $W \subset V_i$ for some i.

Proof. We first show existence. Suppose the set of algebraic sets which cannot be represented as a finite union of irreducible ones is not empty. Let V be a minimal element in its. Then V cannot be irreducible, and we can write $V = A \cup B$ where A, B are algebraic sets, but $A \neq V$ and $B \neq V$. Since each one of A, B is strictly smaller than V, we can express A, B as finite unions of irreducible algebraic sets, and thus get an expression for V, contradiction.

The uniqueness will follow from (iii), which we prove next. Let W be contained in the union $V_1 \cup \ldots \cup V_r$. Then

$$W = (W \cap V_1) \cup \ldots \cup (W \cap V_r).$$

Since each $W \cap V_i$ is an algebraic set, by the irreducibility of W we must have $W = W \cap V_i$ for some i. Hence $W \subset V_i$ for some i, thus proving (iii).

Now to prove (ii), apply (iii) to each W_j. Then for each j there is some i such that $W_j \subset V_i$. Similarly for each i there exists ν such that $V_i \subset W_\nu$. Since there is no inclusion relation among the W_j's, we must have $W_j = V_i = W_\nu$. This proves that each W_j appears among the V_i's and each V_i appears among the W_j's, and proves the uniqueness of the representation. It also concludes the proof of Theorem 2.2.

Theorem 2.3 *An algebraic set is irreducible if and only if its associated ideal is prime.*

Proof. Let V be irreducible and let $\mathfrak{p}$ be its associated ideal. If $\mathfrak{p}$ is not prime, we can find two polynomials $f, g \in k[X]$ such that $f \notin \mathfrak{p}$, $g \notin \mathfrak{p}$, but $fg \in \mathfrak{p}$. Let $\mathfrak{a} = (\mathfrak{p}, f)$ and $\mathfrak{b} = (\mathfrak{p}, g)$. Let A be the algebraic set of zeros of $\mathfrak{a}$, and B the algebraic set of zeros of $\mathfrak{b}$. Then $A \subset V$, $A \neq V$ and $B \subset V$, $B \neq V$. Furthermore $A \cup B = V$. Indeed, $A \cup B \subset V$ trivially. Conversely, let $(x) \in V$. Then $(fg)(x) = 0$ implies $f(x)$ or $g(x) = 0$. Hence $(x) \in A$ or $(x) \in B$, proving $V = A \cup B$, and V is not irreducible. Conversely, let V be the algebraic set of zeros of a prime ideal $\mathfrak{p}$. Suppose $V = A \cup B$ with $A \neq V$ and $B \neq V$. Let $\mathfrak{a}, \mathfrak{b}$ be the ideals associated with A and B respectively. There exist polynomials $f \in \mathfrak{a}, f \notin \mathfrak{p}$ and $g \in \mathfrak{b}, g \notin \mathfrak{p}$. But fg vanishes on $A \cup B$ and hence lies in $\mathfrak{p}$, contradiction which proves the theorem.

Warning. Given a field k and a prime ideal $\mathfrak{p}$ in $k[X]$, it may be that the ideal generated by $\mathfrak{p}$ in $k^a[X]$ is not prime, and the algebraic set defined over k^a by $\mathfrak{p}k^a[X]$ has more than one component, and so is not irreducible. Hence the prefix referring to k is really necessary.

It is also useful to extend the terminology of algebraic sets as follows. Given an ideal $\mathfrak{a} \subset k[X]$, to each field K containing k we can associate to $\mathfrak{a}$ the set

$\mathfrak{Z}_{\mathfrak{a}}(K)$ consisting of the zeros of $\mathfrak{a}$ in K. Thus $\mathfrak{Z}_{\mathfrak{a}}$ is an association

$$\mathfrak{Z}_{\mathfrak{a}} : K \mapsto \mathfrak{Z}_{\mathfrak{a}}(K) \subset K^{(n)}.$$

We shall speak of $\mathfrak{Z}_{\mathfrak{a}}$ itself as an **algebraic space**, so that $\mathfrak{Z}_{\mathfrak{a}}$ is not a set, but to each field K associates the set $\mathfrak{Z}_{\mathfrak{a}}(K)$. Thus $\mathfrak{Z}_{\mathfrak{a}}$ is a functor from extensions K of k to sets (functorial with respect to field isomorphisms). By a k-**variety** we mean the algebraic space associated with a prime ideal $\mathfrak{p}$.

The notion of associated ideal applies also to such $\mathfrak{Z}_{\mathfrak{a}}$, and the associated ideal of $\mathfrak{Z}_{\mathfrak{a}}$ is also $\mathrm{rad}(\mathfrak{a})$. We shall omit the subscript $\mathfrak{a}$ and write simply $\mathfrak{Z}$ for this generalized notion of algebraic space. Of course we have

$$\mathfrak{Z}_{\mathfrak{a}} = \mathfrak{Z}_{\mathrm{rad}(\mathfrak{a})}.$$

We say that $\mathfrak{Z}_{\mathfrak{a}}(K)$ is the set of **points of** $\mathfrak{Z}_{\mathfrak{a}}$ **in** K. By the Hilbert Nullstellensatz, Theorem 1.1, it follows that if $K \subset K'$ are two algebraically closed fields containing k, then the ideals associated with $\mathfrak{Z}_{\mathfrak{a}}(K)$ and $\mathfrak{Z}_{\mathfrak{a}}(K')$ are equal to each other, and also equal to $\mathrm{rad}(\mathfrak{a})$. Thus the smallest algebraically closed field k^{a} containing k already determines these ideals. However, it is also useful to consider larger fields which contain transcendental elements, as we shall see.

As another example, consider the polynomial ring $k[X_1, \ldots, X_n] = k[X]$. Let $\mathbf{A}^n$ denote the algebraic space associated with the zero ideal. Then $\mathbf{A}^n$ is called **affine** n-space. Let K be a field containing k. For each n-tuple $(c_1, \ldots, c_n) \in K^{(n)}$ we get a homomorphism

$$\varphi : k[X_1, \ldots, X_n] \to K$$

such that $\varphi(X_i) = c_i$ for all i. Thus points in $\mathbf{A}^n(K)$ correspond bijectively to homomorphisms of $k(X)$ into K.

More generally, let V be a k-variety with associated prime ideal $\mathfrak{p}$. Then $k[X]/\mathfrak{p}$ is entire. Denote by ξ_i the image of X_i under the canonical homomorphism $k[X] \to k[X]/\mathfrak{p}$. We call (ξ) **the generic point** of V over k. On the other hand, let (x) be a point of V in some field K. Then $\mathfrak{p}$ vanishes on (x), so the homomorphism $\varphi : k[X] \to k[x]$ sending $X_i \mapsto x_i$ factors through $k[X]/\mathfrak{p} = k[\xi]$, whence we obtain a natural homomorphism $k[\xi] \to k[x]$. If this homomorphism is an isomorphism, then we call (x) **a generic point** of V in K.

Given two points $(x) \in \mathbf{A}^n(K)$ and $(x') \in \mathbf{A}^n(K')$, we say that (x') is a **specialization** of (x) (over k) if the map $x_i \mapsto x_i'$ is induced by a homomorphism $k[x] \to k[x']$. From the definition of a generic point of a variety, it is then immediate that:

A variety V is the set of specializations of its generic point, or of a generic point.

In other words, $V(K)$ is the set of specializations of (ξ) in K for every field K containing k.

Let us look at the converse construction of algebraic sets. Let $(x) = (x_1, \ldots, x_n)$ be an n-tuple with coordinates $x_i \in K$ for some extension field K of k. Let $\mathfrak{p}$ be the ideal in $k[X]$ consisting of all polynomials $f(X)$ such that

$f(x) = 0$. We call $\mathfrak{p}$ the ideal **vanishing** on (x). Then $\mathfrak{p}$ is prime, because if $fg \in \mathfrak{p}$ so $f(x)g(x) = 0$, then $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$ since K has no divisors of 0. Hence $\mathfrak{X}_\mathfrak{p}$ is a k-variety V, and (x) is a generic point of V over k because $k[X]/\mathfrak{p} \approx k[x]$.

For future use, we state the next result for the polynomial ring over a factorial ring rather than over a field.

Theorem 2.4. *Let R be a factorial ring, and let $W_1, \ldots, W_m$ be m independent variables over its quotient field k. Let $k(w_1, \ldots, w_m)$ be an extension of transcendence degree $m - 1$. Then the ideal in $R[W]$ vanishing on (w) is principal.*

Proof. By hypothesis there is some polynomial $P(W) \in R[W]$ of degree $\geqq 1$ vanishing on (w), and after taking an irreducible factor we may assume that this polynomial is irreducible, and so is a prime element in the factorial ring $R[W]$. Let $G(W) \in R[W]$ vanish on (w). To prove that P divides G, after selecting some irreducible factor of G vanishing on (w) if necessary, we may assume without loss of generality that G is a prime element in $R[W]$. One of the variables W_i occurs in $P(W)$, say W_m, so that w_m is algebraic over $k(w_1, \ldots, w_{m-1})$. Then $(w_1, \ldots, w_{m-1})$ are algebraically independent, and hence W_m also occurs in G. Furthermore, $P(w_1, \ldots, w_{m-1}, W_m)$ is irreducible as a polynomial in $k(w_1, \ldots, w_{m-1})[W_m]$ by the Gauss lemma as in Chapter IV, Theorem 2.3. Hence there exists a polynomial $H(W_m) \in k(w_1, \ldots, w_{m-1})[W_m]$ such that

$$G(W) = H(W_m)P(W).$$

Let $R' = R[w_1, \ldots, w_{m-1}]$. Then P, G have content 1 as polynomials in $R'[W_m]$. By Chapter IV Corollary 2.2 we conclude that $H \in R'[W_m] \approx R[W]$, which proves Theorem 2.4.

Next we consider homogeneous ideals and projective space. A polynomial $f(X) \in k[X]$ can be written as a linear combination

$$f(X) = \sum c_{(\nu)} M_{(\nu)}(X)$$

with monomials $M_{(\nu)}(X) = X_1^{\nu_1} \cdots X_n^{\nu_n}$ and $c_{(\nu)} \in k$. We denote the **degree** of $M_{(\nu)}$ by

$$|\nu| = \deg M_{(\nu)} = \sum \nu_i.$$

If in this expression for f the degrees of the monomials $X^{(\nu)}$ are all the same (whenever the coefficient $c_{(\nu)}$ is $\neq 0$), then we say that f is a **form**, or also that f is a **homogeneous** (of that degree). An arbitrary polynomial $f(X)$ in $K[X]$ can also be written

$$f(X) = \sum f^{(d)}(X),$$

where each $f^{(d)}$ is a form of degree d (which may be 0). We call $f^{(d)}$ the **homogeneous part** of f of degree d.

An ideal $\mathfrak{a}$ of $k[X]$ is called **homogeneous** if whenever $f \in \mathfrak{a}$ then each homogeneous part $f^{(d)}$ also lies in $\mathfrak{a}$.

Proposition 2.5. *An ideal* $\mathfrak{a}$ *is homogeneous if and only if* $\mathfrak{a}$ *has a set of generators over* $k[X]$ *consisting of forms.*

Proof. Suppose $\mathfrak{a}$ is homogeneous and that $f_1, \ldots, f_r$ are generators. By hypothesis, for each integer $d \geqq 0$ the homogeneous components $f_i^{(d)}$ also lie in $\mathfrak{a}$, and the set of such $f_i^{(d)}$ (for all i, d) form a set of homogeneous generators. Conversely, let f be a homogeneous element in $\mathfrak{a}$ and let $g \in K[X]$ be arbitrary. For each d, $g^{(d)}f$ lies in $\mathfrak{a}$, and $g^{(d)}f$ is homogeneous, so all the homogeneous components of gf also lie in $\mathfrak{a}$. Applying this remark to the case when f ranges over a set of homogeneous generators for $\mathfrak{a}$ shows that $\mathfrak{a}$ is homogeneous, and concludes the proof of the proposition.

An algebraic space $\mathfrak{X}$ is called **homogeneous** if for every point $(x) \in \mathfrak{X}$ and t transcencental over $k(x)$, the point (tx) also lies in $\mathfrak{X}$. If t, u are transcendental over $k(x)$, then there is an isomorphism

$$k[x, t] \xrightarrow{\approx} k[x, u]$$

which sends t on u and restricts to the identity on $k[x]$, so to verify the above condition, it suffices to verify it for some transcendental t over $k(x)$.

Proposition 2.6. *An algebraic space* $\mathfrak{X}$ *is homogeneous if and only if its associated ideal* $\mathfrak{a}$ *is homogeneous.*

Proof. Suppose $\mathfrak{X}$ is homogeneous. Let $f(X) \in k[X]$ vanish on $\mathfrak{X}$. For each $(x) \in \mathfrak{X}$ and t transcendental over $k(x)$ we have

$$0 = f(x) = f(tx) = \sum_d t^d f^{(d)}(x).$$

Therefore $f^{(d)}(x) = 0$ for all d, whence $f^{(d)} \in \mathfrak{a}$ for all d. Hence $\mathfrak{a}$ is homogeneous. Conversely, suppose $\mathfrak{a}$ homogeneous. By the Hilbert Nullstellensatz, we know that $\mathfrak{X}$ consists of the zeros of $\mathfrak{a}$, and hence consists of the zeros of a set of homogeneous generators for $\mathfrak{a}$. But if f is one of those homogeneous generators of degree d, and (x) is a point of $\mathfrak{X}$, then for t transcendental over $k(x)$ we have

$$0 = f(x) = t^d f(x) = f(tx),$$

so (tx) is also a zero of $\mathfrak{a}$. Hence $\mathfrak{X}$ is homogeneous, thus proving the proposition.

Proposition 2.7. *Let* $\mathfrak{X}$ *be a homogeneous algebraic space. Then each irreducible component* V *of* $\mathfrak{X}$ *is also homogeneous.*

Proof. Let $V = V_1, \ldots, V_r$ be the irreducible components of $\mathfrak{X}$, without inclusion relation. By Remark 3.3 we know that $V_1 \not\subset V_2 \cup \ldots \cup V_r$, so there is a point $(x) \in V_1$ such that $(x) \notin V_1$ for $i = 2, \ldots, r$. By hypothesis, for t transcendental over $k(x)$ it follows that $(tx) \in \mathfrak{X}$ so $(tx) \in V_i$ for some i. Specializing to $t = 1$, we conclude that $(x) \in V_i$, so $i = 1$, which proves that V_1 is homogeneous, as was to be shown.

Let V be a variety defined over k by a prime ideal $\mathfrak{p}$ in $k[X]$. Let (x) be a generic point of V over k. We say that (x) is **homogeneous** (**over** k) if for t

transcendental over $k(x)$, the point (tx) is also a point of V, or in other words, (tx) is a specialization of (x). If this is the case, then we have an isomorphism

$$k[x_1, \ldots, x_n] \approx k[tx_1, \ldots, tx_n],$$

which is the identity on k and sends x_i on tx_i. It then follows from the preceding propositions that the following conditions are equivalent for a variety V over k:

V is homogeneous.
The prime ideal of V in $k[X]$ is homogeneous.
A generic point of V over k is homogeneous.

A homogeneous ideal always has a zero, namely the origin (0), which will be called the **trivial zero**. We shall want to know when a homogeneous algebraic set has a non-trivial zero (in some algebraically closed field). For this we introduce the terminology of projective space as follows. Let (x) be some point in $\mathbf{A}^n$ and λ an element of some field containing $k(x)$. Then we denote by (λx) the point $(\lambda x_1, \ldots, \lambda x_n)$. Two points $(x), (y) \in \mathbf{A}^n(K)$ for some field K are called equivalent if not all their coordinates are 0, and there exists some element $\lambda \in K$, $\lambda \neq 0$, such that $(\lambda x) = (y)$. The equivalence classes of such points in $\mathbf{A}^n(K)$ are called the points of **projective space** in K. We denote this projective space by $\mathbf{P}^{n-1}$, and the set of points of projective space in K by $\mathbf{P}^{n-1}(K)$. We define an **algebraic space in projective space** to be the non-trivial zeros of a homogeneous ideal, with two zeros identified if they differ by a common non-zero factor.

Algebraic spaces over rings

As we shall see in the next section, it is not sufficient to look only at ideals in $k[X]$ for some field k. Sometimes, even often, one wants to deal with polynomial equations over the integers $\mathbf{Z}$, for several reasons. In the example of the next sections, we shall find universal conditions over $\mathbf{Z}$ on the coefficients of a system of forms so that these forms have a non-trivial common zero. Furthermore, in number theory—diophantine questions—one wants to consider systems of equations with integer coefficients, and to determine solutions of these equations in the integers or in the rational numbers, or solutions obtained by reducing mod p for a prime p. Thus one is led to extend the notions of algebraic space and variety as follows. Even though the applications of the next section will be over $\mathbf{Z}$, we shall now give general definitions over an arbitrary commutative ring R.

Let $f(X) \in R[X] = R[X_1, \ldots, X_n]$ be a polynomial with coefficients in R. Let $R \to A$ be an R-algebra, by which for the rest of this chapter we mean a homomorphism of commutative rings. We obtain a corresponding homomorphism

$$R[X] \to A[X]$$

on the polynomial rings, denoted by $f \mapsto f_A$ whereby the coefficients of f_A are the images of the coefficients of f under the homomorphism $R \to A$. By a **zero** of f in A we mean a zero of f_A in A. Similarly, let S be a set of polynomials in $R[X]$. By a **zero** of S in A we mean a common zero in A of all polynomials $f \in S$. Let $\mathfrak{a}$ be the ideal generated by S in $R[X]$. Then a zero of S in A is also

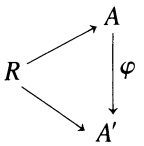
a zero of $\mathfrak{a}$ in A. We denote the set of zeros of S in A by $\mathfrak{Z}_S(A)$, so that we have

$$\mathfrak{Z}_S(A) = \mathfrak{Z}_{\mathfrak{a}}(A).$$

We call $\mathfrak{Z}_{\mathfrak{a}}(A)$ an **algebraic set** over R. Thus we have an association

$$\mathfrak{Z}_{\mathfrak{a}}: A \mapsto \mathfrak{Z}_{\mathfrak{a}}(A)$$

which to each R-algebra associates the set of zeros of $\mathfrak{a}$ in that algebra. We note that R-algebras form a category, whereby a morphism is a ring homomorphism $\varphi: A \to A'$ making the following diagram commutative:



Then it is immediately verified that $\mathfrak{Z}_{\mathfrak{a}}$ is a functor from the category of R-algebras to the category of sets. Again we call $\mathfrak{Z}_{\mathfrak{a}}$ an **algebraic space** over R.

If R is Noetherian, then $R[X]$ is also Noetherian (Chapter IV, Theorem 4.1), and so if $\mathfrak{a}$ is an ideal, then there is always some finite set of polynomials S generating the ideal, so $\mathfrak{Z}_S = \mathfrak{Z}_{\mathfrak{a}}$.

The notion of **radical** of $\mathfrak{a}$ is again defined as the set of polynomials $h \in R[X]$ such that $h^N \in \mathfrak{a}$ for some positive integer N. Then the following statement is immediate:

Suppose that R is entire. Then for every R-algebra $R \to K$ with a field K, we have

$$\mathfrak{Z}_{\mathfrak{a}}(K) = \mathfrak{Z}_{\mathrm{rad}(\mathfrak{a})}(K).$$

We can define **affine space** $\mathbf{A}^n$ over R. Its points consist of all n-tuples $(x_1, \ldots, x_n) = (x)$ with x_i in some R-algebra A. Thus $\mathbf{A}^n$ is again an association

$$A \mapsto \mathbf{A}^n(A)$$

from R-algebras to sets of points. Such points are in bijection with homormorphisms

$$R[X] \to A$$

from the polynomial ring over R into A. In the next section we shall limit ourselves to the case when $A = K$ is a field, and we shall consider only the functor $K \mapsto \mathbf{A}^n(K)$ for fields K. Furthermore, we shall deal especially with the case when $R = \mathbf{Z}$, so $\mathbf{Z}$ has a unique homomorphism into a field K. Thus a field K can always be viewed as a $\mathbf{Z}$-algebra.

Suppose finally that R is entire (for simplicity). We can also consider projective space over R. Let $\mathfrak{a}$ be an ideal in $R[X]$. We define $\mathfrak{a}$ to be homogeneous just as before. Then a homogeneous ideal in $R[X]$ can be viewed as defining an algebraic subset in projective space $\mathbf{P}^n(K)$ for each field K (as an R-algebra). If $R = \mathbf{Z}$,

then $\mathfrak{a}$ defines an algebraic subset in $\mathbf{P}^n(K)$ for every field K. Similarly, one can define the notion of a homogeneous algebraic space $\mathfrak{X}$ over R, and over the integers $\mathbf{Z}$ *a fortiori*. Propositions 2.6 and 2.7 and their proofs are also valid in this more general case, viewing $\mathfrak{X} = \mathfrak{X}_{\mathfrak{a}}$ as a functor from fields K to sets $\mathbf{P}^n(K)$.

If $\mathfrak{a}$ is a prime ideal $\mathfrak{p}$, then we call $\mathfrak{X}_{\mathfrak{p}}$ an R-**variety** V. If R is Noetherian, so $R[X]$ is Noetherian, it follows as before that an algebraic space $\mathfrak{X}$ over R is a finite union of R-varieties without inclusion relations. We shall carry this out in §5, in the very general context of commutative rings. Just as we did over a field, we may form the factor ring $\mathbf{Z}[X]/\mathfrak{p}$ and the image (x) of (X) in this factor ring is called a **generic point** of V.

§3. PROJECTIONS AND ELIMINATION

Let $(W) = (W_1, \ldots, W_m)$ and $(X) = (X_1, \ldots, X_n)$ be two sets of independent variables. Then ideals in $k[W, X]$ define algebraic spaces in the product space $\mathbf{A}^{m+n}$. Let $\mathfrak{a}$ be an ideal in $k[W, X]$. Let $\mathfrak{a}_1 = \mathfrak{a} \cap k[W]$. Let $\mathfrak{X}$ be the algebraic space of zeros of $\mathfrak{a}$ and let $\mathfrak{X}_1$ be the algebraic space of zeros of $\mathfrak{a}_1$. We have the projection

$$\mathrm{pr}: \mathfrak{X}^{m+n} \to \mathfrak{X}^m \quad \text{or} \quad \mathrm{pr}: \mathbf{A}^{m+n} \to \mathbf{A}^m$$

which maps a point (w, x) to its first set of coordinates (w). It is clear that $\mathrm{pr}\,\mathfrak{X} \subset \mathfrak{X}_1$. In general it is not true that $\mathrm{pr}\,\mathfrak{X} = \mathfrak{X}_1$. For example, the ideal $\mathfrak{p}$ generated by the single polynomial $W_1^2 - W_2X_1 = 0$ is prime. Its intersection with $k[W_1, W_2]$ is the zero ideal. But it is not true that every point in the affine (W_1, W_2)-space is the projection of a point in the variety $\mathfrak{X}_{\mathfrak{p}}$. For instance, the point $(1, 0)$ is not the projection of any zero of $\mathfrak{p}$. One says in such a case that the projection is **incomplete**. We shall now consider a situation when such a phenomenon does not occur.

In the first place, let $\mathfrak{p}$ be a prime ideal in $k[W, X]$ and let V be its variety of zeros. Let (w, x) be a generic point of V. Let $\mathfrak{p}_1 = \mathfrak{p} \cap k[W]$. Then (w) is a generic point of the variety V_1 which is the algebraic space zeros of $\mathfrak{p}_1$. This is immediate from the canonical injective homomorphism

$$k[W]/\mathfrak{p}_1 \to k[W, X]/\mathfrak{p}.$$

Thus the generic point (w) of V_1 is the projection of the generic point (w, x) of V. The question is whether a special point (w') of V_1 is the projection of a point of V.

In the subsequent applications, we shall consider ideals which are homogeneous only in the X-variables, and similarly algebraic subsets which are homogeneous in the second set of variables in $\mathbf{A}^n$.

An ideal $\mathfrak{a}$ in $k[W, X]$ which is homogeneous in (X) defines an algebraic space in $\mathbf{A}^m \times \mathbf{P}^{n-1}$. If V is an irreducible component of the algebraic set defined by $\mathfrak{a}$, then we may view V as a subvariety of $\mathbf{A}^m \times \mathbf{P}^{n-1}$. Let $\mathfrak{p}$ be the prime ideal associated with V. Then $\mathfrak{p}$ is homogeneous in (X). Let $\mathfrak{p}_1 = \mathfrak{p} \cap k[W]$. We shall see that the situation of an incomplete projection mentioned previously is eliminated when we deal with projective space.

We can also consider the product $\mathbf{A}^m \times \mathbf{P}^n$, defined by the zero ideal over $\mathbf{Z}$. For each field K, the set of points of $\mathbf{A}^m \times \mathbf{P}^n$ in K is $\mathbf{A}^m(K) \times \mathbf{P}^n(K)$. An ideal $\mathfrak{a}$ in $\mathbf{Z}[W, X]$, homogeneous in (X), defines an algebraic space $\mathfrak{Z} = \mathfrak{Z}_\mathfrak{a}$ in $\mathbf{A}^m \times \mathbf{P}^n$. We may form its projection $\mathfrak{Z}_1$ on the first factor. This applies in particular when $\mathfrak{a}$ is a prime ideal $\mathfrak{p}$, in which case we call $\mathfrak{Z}_\mathfrak{a}$ an **arithmetic subvariety** of $\mathbf{A}^m \times \mathbf{P}^n$. Its projection V_1 is an arithmetic subvariety of $\mathbf{A}^m$, associated with the prime ideal $\mathfrak{p}_1 = \mathfrak{p} \cap \mathbf{Z}[W]$.

Theorem 3.1. *Let $(W) = (W_1, \ldots, W_m)$ and $(X) = (X_1, \ldots, X_n)$ be independent families of variables. Let $\mathfrak{p}$ be a prime ideal in $k[W, X]$* (resp. $\mathbf{Z}[W, X]$) *and assume $\mathfrak{p}$ is homogeneous in (X). Let V be the corresponding irreducible algebraic space in $\mathbf{A}^m \times \mathbf{P}^{n-1}$. Let $\mathfrak{p}_1 = \mathfrak{p} \cap k[W]$* (resp. $\mathfrak{p} \cap \mathbf{Z}[W]$), *and let V_1 be the projection of V on the first factor. Then V_1 is the algebraic space of zeros of $\mathfrak{p}_1$ in $\mathbf{A}^m$.*

Proof. Let V have generic point (w, x). We have to prove that every zero (w') of $\mathfrak{p}_1$ in a field is the projection of some zero (w', x') of $\mathfrak{p}$ such that not all the coordinates of (x') are equal to 0. By assumption, not all the coordinates of (x) are equal to 0, since we viewed V as a subset of $\mathbf{A}^m \times \mathbf{P}^{n-1}$. For definiteness, say we are dealing with the case of a field k. By Chapter VII, Proposition 3.3, the homomorphism $k[w] \to k[w']$ can be extended to a place φ of $k(w, x)$. By Proposition 3.4 of Chapter VII, there is some coordinate x_j such that $\varphi(x_i/x_j) \neq \infty$ for all $i = 1, \ldots, n$. We let $x_i' = \varphi(x_i/x_j)$ for all i to conclude the proof. The proof is similar when dealing with algebraic spaces over $\mathbf{Z}$, replacing k by $\mathbf{Z}$.

Remarks. Given the point $(w') \in \mathbf{A}^m$, the point (w', x') in $\mathbf{A}^m \times \mathbf{P}^{n-1}$ may of course not lie in $k(w')$. The coordinates (x') could even be transcendental over $k(x')$. By any one of the forms of the Hilbert Nullstellensatz, say Corollary 1.3 of Theorem 1.1, we do know that (x') could be found algebraic over $k(w')$, however. In light of the various versions of the Nullstellensatz, if a set of forms has a non-trivial common zero in some field, then it has a non-trivial common zero in the algebraic closure of the field generated by the coefficients of the forms over the prime field. In a theorem such as Theorem 1.2 below, the conditions on the coefficients for the forms to have a non-trivial common zero (or a zero in projective space) are therefore also conditions for the forms to have such a zero in that algebraic closure.

We shall apply Theorem 3.1 to show that given a finite family of homogeneous polynomials, the property that they have a non-trivial common zero in some

algebraically closed field can be expressed in terms of a finite number of universal polynomial equations in their coefficients. We make this more precise as follows.

Consider a finite set of forms $(f) = (f_1, \ldots, f_r)$. Let $d_1, \ldots, d_r$ be their degrees. *We assume* $d_i \geqq 1$ *for* $i = 1, \ldots, r$. Each f_i can be written

$$f_i = \sum w_{i,(\nu)} M_{(\nu)}(X) \tag{1}$$

where $M_{(\nu)}(X)$ is a monomial in (X) of degree d_i, and $w_{i,(\nu)}$ is a coefficient. We shall say that (f) has a **non-trivial zero** (x) if $(x) \neq (0)$ and $f_i(x) = 0$ for all i. We let $(w) = (w)_f$ be the point obtained by arranging the coefficients $w_{i,(\nu)}$ of the forms in some definite order, and we consider this point as a point in some affine space $\mathbf{A}^m$, where m is the number of such coefficients. This integer m is determined by the given degrees $d_1, \ldots, d_r$. In other words, given such degrees, the set of all forms $(f) = (f_1, \ldots, f_r)$ with these degrees is in bijection with the points of $\mathbf{A}^m$.

Theorem 3.2. (Fundamental theorem of elimination theory.) *Given degrees* $d_1, \ldots, d_r$, *the set of all forms* $(f_1, \ldots, f_r)$ *in n variables having a non-trivial common zero is an algebraic subspace of* $\mathbf{A}^m$ *over* $\mathbf{Z}$.

Proof. Let $(W) = (W_{i,(\nu)})$ be a family of variables independent of (X). Let $(F) = (F_1, \ldots, F_r)$ be the family of polynomials in $\mathbf{Z}[W, X]$ given by

$$F_i(W, X) = \sum W_{i,(\nu)} M_{(\nu)}(X) \tag{2}$$

where $M_{(\nu)}(X)$ ranges over all monomials in (X) of degree d_i, so $(W) = (W)_F$. We call $F_1, \ldots, F_r$ **generic forms**. Let

$$\mathfrak{a} = \text{ideal in } \mathbf{Z}[W, X] \text{ generated by } F_1, \ldots, F_r.$$

Then $\mathfrak{a}$ is homogeneous in (X). Thus we are in the situation of Theorem 3.1, with $\mathfrak{a}$ defining an algebraic space $\mathfrak{A}$ in $\mathbf{A}^m \times \mathbf{P}^{n-1}$. Note that (w) is a specialization of (W), or, as we also say, (f) is a specialization of (F). As in Theorem 3.1, let $\mathfrak{A}_1$ be the projection of $\mathfrak{A}$ on the first factor. Then directly from the definitions, (f) has a non-trivial zero if and only if $(w)_f$ lies in $\mathfrak{A}_1$, so Theorem 3.2 is a special case of Theorem 3.1.

Corollary 3.3. *Let* (f) *be a family of n forms in n variables, and assume that* $(w)_f$ *is a generic point of* $\mathbf{A}^m$, *i.e. that the coefficients of these forms are algebraically independent. Then* (f) *does not have a non-trivial zero.*

Proof. There exists a specialization of (f) which has only the trivial zero, namely $f_1' = X_1^{d_1}, \ldots, f_n' = X_n^{d_n}$.

Next we follow van der Waerden in showing that $\mathfrak{A}$ and hence $\mathfrak{A}_1$ are irreducible.

Theorem 3.4. *The algebraic space* $\mathfrak{A}_1$ *of forms having a non-trivial common zero in Theorem 3.2 is actually a* $\mathbf{Z}$*-variety, i.e. it is irreducible. The prime ideal*

$\mathfrak{p}$ *in* $\mathbf{Z}[W, X]$ *associated with* $\mathfrak{A}$ *consists of all polynomials* $G(W, X) \in \mathbf{Z}[W, X]$ *such that for some index* j *there is an integer* $s \geqq 0$ *satisfying*

$(*)_j$ $\quad X_j^s G(W, X) \equiv 0 \bmod (F_1, \ldots, F_r)$; *that is,* $X_j^s G(W, X) \in \mathfrak{a}$.

If relation (*) *holds for one index* j, *then it holds for every* $j = 1, \ldots, n$. (*Of course, the integer* s *depends on* j.)

Proof. We construct a generic point of $\mathfrak{A}$. We select any one of the variables, say X_q, and rewrite the forms F_i as follows:

$$F_i(W, X) = F_i^* + Z_i X_q^{d_i}$$

where F_i^* is the sum of all monomials except the monomial containing $X_q^{d_i}$. The coefficients (W) are thereby split into two families, which we denote by (Y) and (Z), where $(Z) = (Z_1, \ldots, Z_r)$ are the coefficients of $(X_q^{d_1}, \ldots, X_q^{d_r})$ in $(F_1, \ldots, F_r)$, and (Y) is the remaining family of coefficients of $F_1^*, \ldots, F_r^*$. We have $(W) = (Y, Z)$, and we may write the polynomials F_i in the form

$$F_i(W, X) = F_i(Y, Z, X) = F_i^*(Y, X) + Z_i X_q^{d_i}.$$

Corresponding to the variables (Y, X) we choose quantities (y, x) algebraically independent over $\mathbf{Z}$. We let

$$z_i = -F_i^*(y, x)/x_q^{d_i} = -F_i^*(y, x/x_q). \tag{3}$$

We shall prove that (y, z, x) is a generic point of $\mathfrak{A}$.

From our construction, it is immediately clear that $F_i(y, z, x) = 0$ for all i, and consequently if $G(W, X) \in \mathbf{Z}[W, X]$ satisfies (*), then $G(y, z, x) = 0$.

Conversely, let $G(Y, Z, X) \in \mathbf{Z}[Y, Z, X] = \mathbf{Z}[W, X]$ satisfy $G(y, z, x) = 0$. From Taylor's formula in several variables we obtain

$$\begin{aligned} G(Y, Z, X) &= G(Y, \ldots, -F_i^*/X_q^{d_i} + Z_i + F_i^*/X_q^{d_i}, \ldots, X) \\ &= G(Y, -F_i^*/X_q^{d_i}, X) + \sum (Z_i + F_i^*/X_q^{d_i})^{\mu_i} H_{\mu_i}(Y, Z, X), \end{aligned}$$

where the sum is taken over terms having one factor $(Z_i + F_i^*/X_q^{d_i})$ to some power $\mu_i > 0$, and some factor H_{μ_i} in $\mathbf{Z}[Y, Z, X]$. From the way (y, z, x) was constructed, and the fact that $G(y, z, x) = 0$, we see that the first term vanishes, and hence

$$G(Y, Z, X) = \sum (Z_i + F_i^*/X_q^{d_i})^{\mu_i} H_{\mu_i}(Y, Z, X).$$

Clearing denominators of X_q, for some integer s we get

$$X_q^s G(Y, Z, X) \equiv 0 \bmod (F_i, \ldots, F_r),$$

or in other words, $(*)_q$ is satisfied. This concludes the proof of the theorem.

Remark. Of course the same statement and proof as in Theorem 3.4 holds with $\mathbf{Z}$ replaced by a field k. In that case, we denote by $\mathfrak{a}_k$ the ideal in $k[W, X]$ generated by the generic forms, and similarly by $\mathfrak{p}_k$ the associated prime

ideal. Then

$$\mathfrak{a}_{k,1} = \mathfrak{a}_k \cap k[W] \quad \text{and} \quad \mathfrak{p}_{k,1} = \mathfrak{p}_k \cap k[W].$$

The ideal $\mathfrak{p}$ in Theorem 3.4 will be called the **prime associated with the ideal of generic forms**. The intersection $\mathfrak{p}_1 = \mathfrak{p} \cap \mathbf{Z}[W]$ will be called the prime **elimination ideal** of these forms. If $\mathfrak{A}$ denotes as before the zeros of $\mathfrak{p}$ (or of $\mathfrak{a}$), and $\mathfrak{A}_1$ is its projection on the first factor, then $\mathfrak{p}_1$ is the prime associated with $\mathfrak{A}_1$. The same terminology will be used if instead of $\mathbf{Z}$ we work over a field k. (*Note*: homogeneous elements of $\mathfrak{p}_1$ have been called **inertia forms** in the classical literature, following Hurwitz. I am avoiding this terminology because the word "inertia" is now used in a standard way for inertia groups as in Chapter VII, §2.) The variety of zeros of $\mathfrak{p}_1$ will be called the **resultant variety**. It is determined by the given degrees $d_1, \ldots, d_n$, so we could denote it by $\mathfrak{A}_1(d_1, \ldots, d_n)$.

Exercise. Show that if $\mathfrak{p}$ is the prime associated with the ideal of generic forms, then $\mathfrak{p} \cap \mathbf{Z} = (0)$ is the zero ideal.

Theorem 3.5. *Assume $r = n$, so we deal with n forms in n variables. Then $\mathfrak{p}_1$ is principal, generated by a single polynomial, so $\mathfrak{A}_1$ is what one calls a hypersurface. If (w) is a generic point of $\mathfrak{A}_1$ over a field k, then the transcendence degree of $k(w)$ over k is $m - 1$.*

Proof. We prove the second statement first, and use the same notation as in the proof of Theorem 3.4. Let $u_j = x_j/x_n$. Then $u_n = 1$ and (y), $(u_1, \ldots, u_{n-1})$ are algebraically independent. By (3), we have $z_i = -F_i^*(y, u)$, so

$$k(w) = k(y, z) \subset k(y, u),$$

and so the transcendence degree of $k(w)$ over k is $\leqq m - 1$. We claim that this transcendence degree is $m - 1$. It will suffice to prove that $u_1, \ldots, u_{n-1}$ are algebraic over $k(w) = k(y, z)$. Suppose this is not the case. Then there exists a place φ of $k(w, u)$, which is the identity on $k(w)$ and maps some u_j on ∞. Select an index q such that $\varphi(u_i/u_q)$ is finite for all $i = 1, \ldots, n - 1$. Let $v_i = u_i/u_q$ and $v_i' = \varphi(u_i/u_q)$. Denote by Y_{iq} the coefficient of $X_q^{d_i}$ in F_i and let Y^* denote the variables (Y) from which $Y_{1q}, \ldots, Y_{nq}$ are deleted. By (3) we have for $i = 1, \ldots, n$:

$$\begin{aligned} 0 &= y_{iq} u_q^{d_i} + z_i + F_i^{**}(y^*, u) \\ &= y_{iq} + z_i/u_q^{d_i} + F_i^{**}(y^*, u/u_q). \end{aligned}$$

Applying the place yields

$$0 = y_{iq} + F_i^{**}(y^*, v').$$

In particular, $y_{iq} \in k(y^*, v')$ for each $i = 1, \ldots, n$. But the transcendence degree of $k(v')$ over k is at most $n - 1$, while the elements $(y_{1q}, \ldots, y_{nq}, y^*)$ are algebraically independent over k, which gives a contradiction proving the theorem.

Remark. There is a result (I learned it from [Jo 80]) which is more precise than Theorem 3.5. Indeed, let $\mathfrak{A}$ as in Theorem 3.5 be the variety of zeros of $\mathfrak{p}$, and $\mathfrak{A}_1$ its projection. Then this projection is birational in the following sense. Using the notation of the proof of Theorem 3.5, the result is not only that $k(w)$ has transcendence degree $m - 1$ over k, but actually we have

$$\mathbf{Q}(y, z) = \mathbf{Q}(w) = \mathbf{Q}(y, u).$$

Proof. Let $\mathfrak{p}_1 = (R)$, so R is the resultant, generating the principal ideal $\mathfrak{p}_1$. We shall need the following lemma.

Lemma 3.6. *There is a positive integer s with the following properties. Fix an index i with $1 \leqq i \leqq n - 1$. For each pair of n-tuples of integers $\geqq 0$*

$$(\alpha) = (\alpha_1, \ldots, \alpha_n) \quad \textit{and} \quad (\beta) = (\beta_1, \ldots, \beta_n)$$

with $|\alpha| = |\beta| = d_i$, we have

$$X_n^s\left(M_{(\alpha)}(X)\frac{\partial R}{\partial W_{i,(\beta)}} - M_{(\beta)}(X)\frac{\partial R}{\partial W_{i,(\alpha)}}\right) \equiv 0 \bmod (F_1, \ldots, F_n).$$

To see this, we use the fact from Theorem 3.4 that for some s,

$$X_n^s R(W) = Q_1F_1 + \cdots + Q_nF_n \text{ with } Q_j \in \mathbf{Z}[W, X].$$

Differentiating with respect to $W_{i,(\beta)}$ we get

$$X_n^s \frac{\partial R}{\partial W_{i,(\beta)}} \equiv Q_i M_{(\beta)}(X) \bmod (F_1, \ldots, F_n),$$

and similarly

$$X_n^s \frac{\partial R}{\partial W_{i,(\alpha)}} \equiv Q_i M_{(\alpha)}(X) \bmod (F_1, \ldots, F_n).$$

We multiply the first congruence by $M_{(\alpha)}(X)$ and the second by $M_{(\beta)}(X)$, and we subtract to get our lemma.

From the above we conclude that

$$M_{(\alpha)}(X)\frac{\partial R}{\partial W_{i,(\beta)}} - M_{(\beta)}(X)\frac{\partial R}{\partial W_{i,(\alpha)}}$$

vanishes on $\mathfrak{A}$, i.e. on the point (w, u), after we put $X_n = 1$. Then we select

$$M_{(\alpha)}(X) = X_i^{d_i} \quad \text{and} \quad M_{(\beta)}(X) = X_i^{d_i - 1}X_n \text{ for } i = 1, \ldots, n - 1,$$

and we see that we have the rational expression

$$u_i = \frac{\partial R/\partial W_{i,(\beta)}}{\partial R/\partial W_{i,(\alpha)}}\bigg|_{(W)=(w)}, \text{ for } i = 1, \ldots, n - 1,$$

thus showing that $\mathbf{Q}(u) \subset \mathbf{Q}(w)$, as asserted.

We note that the argument also works over the prime field of characteristic p. The only additional remark to be made is that there is some partial derivative $\partial R/\partial W_{i,(\alpha)}$ which does not vanish on (w). This is a minor technical matter, which we leave to the reader.

The above argument is taken from [Jo 80], Proposition 3.3.1. Jouanolou links old-time results as in Macaulay [Ma 16] with more recent techniques of commutative algebra, including the Koszul complex (which will be discussed in Chapter XXI). See also his monographs [Jo 90], [Jo 91].

Still following van der Waerden, we shall now give a fairly explicit determination of the polynomial generating the ideal in Theorem 3.5. We deal with the generic forms $F_i(W, X)$ $(i = 1, \ldots, n)$. According to Theorem 3.5, the ideal $\mathfrak{p}_1$ is generated by a single element. Because the units in $\mathbf{Z}[W]$ consist only of ± 1, it follows that this element is well defined up to a sign. Let

$$R(W) = R(F_1, \ldots, F_n)$$

be one choice of this element. Later we shall see how to pick in a canonical way one of these two possible choices. We shall prove various properties of this element, which will be called the **resultant** of $F_1, \ldots, F_n$.

For each $i = 1, \ldots, n$ we let D_i be the product of the degrees with d_i omitted; that is,

$$D_i = d_1 \cdots \overset{\wedge}{d_i} \cdots d_n.$$

We let d be the positive integer such that $d - 1 = \sum (d_i - 1)$.

Lemma 3.7. *Given one of the indices, say n, there is an element $R_n(W)$ lying in $\mathfrak{p}_1$, satisfying the following properties.*

(a) *For each i, $R_n(W)X_i^d \equiv 0 \bmod (F_1, \ldots, F_n)$ in $\mathbf{Z}[W, X]$.*
(b) *For each i, $R_n(W)$ is homogeneous in the set of variables $(W_{i,(\nu)})$, and is of degree D_n in $(W_{n,(\nu)})$,* i.e. *in the coefficient of F_n.*
(c) *As a polynomial in $\mathbf{Z}[W]$, $R_n(W)$ has content* 1, i.e. *is primitive.*

Proof. The polynomial $R_n(W)$ will actually be explicitly constructed. Let $M_\sigma(X)$ denote the monomials of degree $|\sigma| = d$. We partition the indexing set $S = \{\sigma\}$ into disjoint subsets as follows.

Let $S_1 = \{\sigma_1\}$ be the set of indices such that $M_{\sigma_1}(X)$ is divisible by $X_1^{d_1}$.

Let $S_2 = \{\sigma_2\}$ be the set of indices such that $M_{\sigma_2}(X)$ is divisible by $X_2^{d_2}$ but not by $X_1^{d_1}$.

...

Let $S_n = \{\sigma_n\}$ be the set of indices such that $M_{\sigma_n}(X)$ is divisible by $X_n^{d_n}$ but not by $X_1^{d_1}, \ldots, X_{n-1}^{d_{n-1}}$.

Then S is the disjoint union of $S_1, \ldots, S_n$. Write each monomial as follows:

$$\begin{aligned} M_{\sigma_1}(X) &= H_{\sigma_1}(X)X_1^{d_1} \quad \text{so} \quad \deg H_{\sigma_1} = d - d_1 \\ &\vdots \qquad\quad \vdots \\ M_{\sigma_1}(X) &= H_{\sigma_n}(X)X_n^{d_n} \quad \text{so} \quad \deg H_{\sigma_n} = d - d_n. \end{aligned}$$

Then the number of polynomials

$$H_{\sigma_1}F_1, \ldots, H_{\sigma_n}F_n \text{ (with } \sigma_1 \in S_1, \ldots, \sigma_n \in S_n)$$

is precisely equal to the number of monomials of degree d. We let R_n be the determinant of the coefficients of these polynomials, viewed as forms in (X) with coefficients in $\mathbf{Z}[W]$. Then $R_n = R_n(W) \in \mathbf{Z}[W]$. We claim that $R_n(W)$ satisfies the properties of the lemma.

First we note that if $\sigma_n \in S_n$, then $H_{\sigma_n}(X)$ is divisible by a power of X_i at most $d_i - 1$, for $i = 1, \ldots, n-1$. On the other hand, the degree of $H_{\sigma_n}(X)$ in X_n is determined by the condition that the total degree is $d - d_n$. Hence S_n has exactly D_n elements. It follows at once that $R_n(W)$ is homogeneous of degree D_n in the coefficients of F_n, i.e. in $(W_{n,(\nu)})$. From the construction it also follows that R_n is homogeneous in each set of variables $(W_{i,(\nu)})$ for each $i = 1, \ldots, n-1$.

If we specialize the forms F_i $(i = 1, \ldots, n)$ to $X_i^{d_i}$, then R_n specializes to 1, and hence $R_n \neq 0$ and R_n is primitive. For each σ_i we can write

$$H_{\sigma_i}F_i = \sum_{\sigma \in S} C_{\sigma,\sigma_i}(W)M_\sigma(X),$$

where $M_\sigma(X)$ $(\sigma \in S)$ ranges over all monomials of degree d in (X), and $C_{\sigma,\sigma_i}(W)$ is one of the variables (W). Then by definition

$$R_n(W) = \det(C_{\sigma,\sigma_1}(W)_{(\sigma_1 \in S_1)}, \ldots, C_{\sigma,\sigma_n}(W)_{(\sigma_n \in S_n)}) = \det(C).$$

where $\sigma_1 \in S_1, \ldots, \sigma_n \in S_n$ indexes the columns, and σ indexes the rows. Let $B = \tilde{C}$ be the matrix with components in $\mathbf{Z}[W, X]$ such that

$$BC = \det(C)I = R_n I.$$

(See Chapter XIII, Corollary 4.17.) Then for each σ, we have

$$R_n(W)M_\sigma(X) = \sum_i \sum_{\sigma_i \in S_i} B_{i,\sigma_i}F_i.$$

Given i, we take for σ the index such that $M_\sigma(X) = X_i^d$ in order to obtain the first relation in Lemma 3.7. By Theorem 3.4, we conclude that $R_n(W) \in \mathfrak{p}_1$. This concludes the proof of the lemma.

Of course, we picked an index n to fix ideas. For each i one has a polynomial R_i satisfying the analogous properties, and in particular homogeneous of degree D_i in the variables $(W_{i,(\nu)})$ which are the coefficients of the form F_i.

Theorem 3.8. *Let R be the resultant of the n generic forms F_i over $\mathbf{Z}$, in n variables. Then R satisfies the following properties.*

(a) *R is the greatest common divisor in $\mathbf{Z}[W]$ of the polynomials $R_1, \ldots, R_n$.*
(b) *R is homogeneous of degree D_i in the coefficients of F_i.*
(c) *Let $F_i = \ldots + W_{i,(d_i)}X_i^{d_i}$, so $W_{i,(d_i)}$ is the coefficient of $X_i^{d_i}$. Then R contains the monomial*

$$\pm \prod_{i=1}^{n} W_{i,(d_i)}^{D_i}.$$

Proof. The idea will be to specialize the forms $F_1, \ldots, F_n$ to products of generic linear forms, where we can tell what is going on. For that we need a lemma of a more general property eventually to be proved. We shall use the following notation. If $f_1, \ldots, f_n$ are forms with coefficients (w), then we write

$$R(f_1, \ldots, f_n) = R(w).$$

Lemma 3.9. *Let G, H be generic independent forms with $\deg(GH) = d_1$. Then $R(GH, F_2, \ldots, F_n)$ is divisible by $R(G, F_2, \ldots, F_n)R(H, F_2, \ldots, F_n)$.*

Proof. By Theorem 3.5, there is an expression

$$X_n^s R(F_1, \ldots, F_n) = Q_1F_1 + \cdots + Q_nF_n \text{ with } Q_i \in \mathbf{Z}[W, X].$$

Let $W_G, W_H, W_{F_2}, \ldots, W_{F_n}$ be the coefficients of $G, H, F_2, \ldots, F_n$ respectively, and let (w) be the coefficients of $GH, F_2, \ldots, F_n$. Then

$$R(w) = R(GH, F_2, \ldots, F_n),$$

and we obtain

$$X_n^s R(w) = Q_1(w, X)GH + Q_2(w, X)F_2 + Q_n(w, X)F_n.$$

Hence $R(GH, F_2, \ldots, F_n)$ belongs to the elimination ideal of $G, F_2, \ldots, F_n$ in the ring $\mathbf{Z}[W_G, W_H, W_{F_2}, \ldots, W_{F_n}]$, and similarly with H instead of G. Since W_H is a family of independent variables over $\mathbf{Z}[W_G, W_{F_2}, \ldots, W_{F_n}]$, it follows that $R(G, F_2, \ldots, F_n)$ divides $R(GH, F_2, \ldots, F_n)$ in that ring, and similarly for $R(H, F_2, \ldots, F_n)$. But (W_G) and (W_H) are independent sets of variables, and so $R(G, F_2, \ldots, F_n)$, $R(H, F_2, \ldots, F_n)$ are distinct prime elements in that ring, so their product divides $R(GH, F_2, \ldots, F_n)$ as stated, thus proving the lemma.

Lemma 3.9 applies to any specialized family of polynomials $g, h, f_1, \ldots, f_n$ with coefficients in a field k. Observe that for a system of n linear forms in n variables, the resultant is simply the determinant of the coefficients. Thus if $L_1, \ldots, L_n$ are generically independent linear forms in the variables $X_1, \ldots, X_n$, then their resultant $R(L_1, \ldots, L_n)$ is homogeneous of degree 1 in the coefficients of L_i for each i. We apply Lemma 3.9 to the case of forms $f_1, \ldots, f_{n-1}$, which are products of generically independent linear forms. By Lemma 3.9 we conclude that for this specialized family of form, their resultant has degree at least D_n in

the coefficients of F_n, so for the generic forms $F_1, \ldots, F_n$ their resultant has degree at least D_n in the coefficients of F_n. Similarly $R(F_1, \ldots, F_n)$ has degree at least D_i in the coefficients of F_i for each i. But R divides the n elements $R_1(W), \ldots, R_n(W)$ constructed in Lemma 3.7. Therefore we conclude that R has degree exactly D_i in the coefficients of F_i. By Theorem 3.5, we know that R divides each R_i. Let G be the greatest common divisor of $R_1, \ldots, R_n$ in $\mathbf{Z}[W]$. Then R divides G and has the same degree in each set of variables $(W_{i,(\nu)})$ for $i = 1, \ldots, n$. Hence there exists $c \in \mathbf{Z}$ such that $G = cR$. We must have $c = \pm 1$, because, say, R_n is primitive in $\mathbf{Z}[W]$. This proves (a) and (b) of the theorem.

As to the third part, we specialize the forms to $f_i = X_i^{d_i}$, $i = 1, \ldots, n$. Then R_n specializes to 1, and since R divides R_n it follows that R itself specializes to ± 1. Since all coefficients of the forms specialize to 0 except those which we denoted by $W_{i,(d_i)}$, it follows that $R(W)$ contains the monomial which is the product of these variables to the power D_i, up to the sign ± 1. This proves (c), and concludes the proof of Theorem 3.8.

We can now normalize the resultant by choosing the sign such that R contains the monomial

$$M = \prod_{i=1}^{n} W_{i,(d_i)}^{D_i},$$

with coefficient $+1$. This condition determines R uniquely, and we then denote R also by

$$R = \operatorname{Res}(F_1, \ldots, F_n).$$

Given forms $f_1, \ldots, f_n$ with coefficients (w) in a field K (actually any commutative ring), we can then define their **resultant**

$$\operatorname{Res}(f_1, \ldots, f_n) = R(w)$$

with the normalized polynomial R. With this normalization, we then have a stronger result than Lemma 3.9.

Theorem 3.10. *Let $f_1 = gh$ be a product of forms such that* $\deg(gh) = d_1$. *Let $f_2, \ldots, f_n$ be arbitrary forms of degrees $d_2, \ldots, d_n$. Then*

$$\operatorname{Res}(gh, f_2, \ldots, f_n) = \operatorname{Res}(g, f_2, \ldots, f_n)\operatorname{Res}(h, f_2, \ldots, f_n).$$

Proof. From the fact that the degrees have to add in a product of polynomials, together with Theorem 3.8(a) and (b), we now see in Lemma 3.9 that we must have the precise equality in what was only a divisibility before we knew the precise degree of R in each set of variables.

Theorem 3.10 is very useful in proving further properties of the determinant, because it allows a reduction to simple cases under factorization of polynomials.

For instance one has:

Theorem 3.11. *Let $F_1, \ldots, F_n$ be the generic forms in n variables, and let $\overline{F}_1, \ldots, \overline{F}_n$ be the forms obtained by substituting $X_n = 0$, so that $\overline{F}_1, \ldots, \overline{F}_{n-1}$ are the generic forms in $n-1$ variables. Let $n \geqq 2$. Then*

$$\mathrm{Res}(F_1, \ldots, F_{n-1}, X_n^{d_n}) = \mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1})^{d_n}.$$

Proof. By Theorem 3.10 it suffices to prove the assertion when $d_n = 1$. By Theorem 3.4, for each $i = 1, \ldots, n-1$ we have an expression

$$(*) \qquad X_i^s \mathrm{Res}(F_1, \ldots, F_{n-1}, X_n) = Q_1 F_1 + \cdots + Q_{n-1} F_{n-1} + Q_n X_n$$

with $Q_j \in \mathbf{Z}[W, X]$ (depending on the choice of i). The left-hand side can be written as a polynomial in the coefficients of $F_1, \ldots, F_{n-1}$ with the notation

$$X_i^s R(W_{F_1}, \ldots, W_{F_{n-1}}, 1_{X_n}) = X_i^s P(W_{F_1}, \ldots, W_{F_{n-1}}) = X_i^s P(W^{(n-1)}), \text{ say;}$$

thus in the generic linear form in $X_1, \ldots, X_n$ we have specialized all the coefficients to 0 except the coefficient of X_n, which we have specialized to 1. Substitute $X_n = 0$ in the right side of (*). By Theorem 3.4, we conclude that $P(W^{(n-1)})$ lies in the resultant ideal of $\overline{F}_1, \ldots, \overline{F}_{n-1}$, and therefore $\mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1})$ divides $P(W^{(n-1)})$. By Theorem 3.8 we know that $P(W^{(n-1)})$ has the same homogeneity degree in $W_{\overline{F}_i}$ $(i = 1, \ldots, n-1)$ as $\mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1})$. Hence there is $c \in \mathbf{Z}$ such that

$$c\mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1}) = \mathrm{Res}(F_1, \ldots, F_{n-1}, X_n).$$

One finds $c = 1$ by specializing $\overline{F}_1, \ldots, \overline{F}_{n-1}$ to $X_1^{d_1}, \ldots, X_{n-1}^{d_{n-1}}$ respectively, thus concluding the proof.

The next basic lemma is stated for the generic case, for instance in Macaulay [Ma 16], and is taken up again in [Jo 90], Lemma 5.6.

Lemma 3.12. *Let A be a commutative ring. Let $f_1, \ldots, f_n$, $g_1, \ldots, g_n$ be homogeneous polynomials in $A[X_1, \ldots, X_n]$. Assume that*

$$(g_1, \ldots, g_n) \subset (f_1, \ldots, f_n)$$

as ideals in $A[X]$. Then

$$\mathrm{Res}(f_1, \ldots, f_n) \text{ divides } \mathrm{Res}(g_1, \ldots, g_n) \text{ in } A.$$

Proof. Express each $g_i = \sum h_{ij} f_j$ with h_{ij} homogeneous in $A[X]$. By specialization, we may then assume that $g_i = \sum H_{ij} F_j$ where H_{ij} and F_j have algebraically independent coefficients over $\mathbf{Z}$. By Theorem 3.4, for each i we have a relation

$$X_i^s \mathrm{Res}(g_1, \ldots, g_n) = Q_1 g_1 + \cdots + Q_n g_n \text{ with some } Q_i \in \mathbf{Z}[W_H, W_F],$$

where W_H, W_F denote the independent variable coefficients of the polynomials H_{ij} and F_j respectively. In particular,

$$(*) \qquad X_i^s \operatorname{Res}(g_1, \ldots, g_n) \equiv 0 \bmod (F_1, \ldots, F_n)\mathbf{Z}[W_H, W_F, X].$$

Note that $\operatorname{Res}(g_1, \ldots, g_n) = P(W_H, W_F) \in \mathbf{Z}[W_H, W_F]$ is a polynomial with integer coefficients. If (w_F) is a generic point of the resultant variety $\mathfrak{A}_1$ over $\mathbf{Z}$, then $P(W_H, w_F) = 0$ by (*). Hence $\operatorname{Res}(F_1, \ldots, F_n)$ divides $P(W_H, W_F)$, thus proving the lemma.

Theorem 3.13. *Let A be a commutative ring and let $d_1, \ldots, d_n$ be integers $\geqq 1$ as usual. Let f_i be homogeneous of degree d_i in $A[X] = A[X_1, \ldots, X_n]$. Let d be an integer $\geqq 1$, and let $g_i, \ldots, g_n$ be homogeneous of degree d in $A[X]$. Then*

$$f_i \circ g = f_i(g_1, \ldots, g_n)$$

is homogeneous of degree dd_i, and

$$\operatorname{Res}(f_1 \circ g, \ldots, f_n \circ g) = \operatorname{Res}(g_1, \ldots, g_n)^{d_1 \cdots d_n} \operatorname{Res}(f_1, \ldots, f_n)^{d^{n-1}} \text{ in } A.$$

Proof. We start with the standard relation of Theorem 3.4:

$$(*) \qquad X_i^s \operatorname{Res}(F_1, \ldots, F_n) \equiv 0 \bmod (F_1, \ldots, F_n)\mathbf{Z}[W_F, X].$$

We let $G_1, \ldots, G_n$ be independent generic polynomials of degree d, and let W_G denote their independent variable coefficients. Substituting G_i for X_i in (*), we find

$$G_i^s \operatorname{Res}(F_1, \ldots, F_n) \equiv 0 \bmod (F_1 \circ G, \ldots, F_n \circ G)\mathbf{Z}[W_F, W_G, X].$$

Abbreviate $\operatorname{Res}(F_1, \ldots, F_n)$ by $R(F)$, and let $g_i = G_i^s R(F)$. By Lemma 3.12, it follows that

$$\operatorname{Res}(f_1 \circ G, \ldots, F_n \circ G) \text{ divides } \operatorname{Res}(G_1^s R(F), \ldots, G_n^s R(F)) \text{ in } \mathbf{Z}[W_F, W_G].$$

By Theorem 3.10 and the homogeneity of Theorem 3.8(b) we find that

$$\operatorname{Res}(G_1^s R(F), \ldots, G_n^s R(F)) = \operatorname{Res}(G_1, \ldots, G_n)^M \operatorname{Res}(F_1, \ldots, F_n)^N$$

with integers $M, N \geqq 0$. Since $\operatorname{Res}(G_1, \ldots, G_n)$ and $\operatorname{Res}(F_1, \ldots, F_n)$ are distinct prime elements in $\mathbf{Z}[W_G, W_F]$ (distinct because they involve independent variables), it follows that

$$(**) \qquad \operatorname{Res}(F_1 \circ G, \ldots, F_n \circ G) = \varepsilon \operatorname{Res}(G_1, \ldots, G_n)^a \operatorname{Res}(F_1, \ldots, F_n)^b$$

with integers $a, b \geqq 0$ and $\varepsilon = 1$ or -1. Finally, we specialize F_i to $W_i X_i^{d_i}$ and we specialize G_i to $U_i X_i^d$, with independent variables $(W_1, \ldots, W_n, U_1, \ldots, U_n)$.

Substituting in (**), we obtain

$$\operatorname{Res}(W_1U_1^{d_1}X_1^{dd_1}, \ldots, W_nU_n^{d_n}X_n^{dd_n}) = \varepsilon \operatorname{Res}(U_1X_1^d, \ldots, U_nX_n^d)^a \operatorname{Res}(W_1X_1^{d_1}, \ldots, W_nX_n^{d_n})^b.$$

By the homogeneity of Theorem 3.8(b) we get

$$\prod_i (W_iU^{d_i})^{d_1 \ldots \hat{d}_i \ldots d_n d^{n-1}} = \varepsilon \prod_i U_i^{d^{n-1}a} \prod_i W_i^{d_1 \ldots \hat{d}_i \ldots d_n b}.$$

From this we get at once $\varepsilon = 1$ and a, b are what they are stated to be in the theorem.

Corollary 3.14. *Let $C = (c_{ij})$ be a square matrix with coefficients in A. Let $f_i(X) = F_i(CX)$ (where CX is multiplication of matrices, viewing X as a column vector). Then*

$$\operatorname{Res}(f_1, \ldots, f_n) = \det(C)^{d_1 \ldots d_n} \operatorname{Res}(F_1, \ldots, F_n).$$

Proof. This is the case when $d = 1$ and g_i is a linear form for each i.

Theorem 3.15. *Let $f_1, \ldots, f_n$ be homogeneous in $A[X]$, and suppose $d_n \geqq d_i$ for all i. Let h_i be homogeneous of degree $d_n - d_i$ in $A[X]$. Then*

$$\operatorname{Res}(f_1, \ldots, f_{n-1}, f_n + \sum_{j=1}^{n-1} h_j f_j) = \operatorname{Res}(f_1, \ldots, f_n) \text{ in } A.$$

Proof. We may assume $f_i = F_i$ are the generic forms, H_i are forms generic independent from $F_1, \ldots, F_n$, and $A = \mathbf{Z}[W_F, W_H]$, where (W_F) and (W_H) are the coefficients of the respective polynomials. We note that the ideals $(F_1, \ldots, F_n)$ and $(F_1, \ldots, F_n + \sum_{j \neq n} H_jF_j)$ are equal. From Lemma 3.12 we conclude that the two resultants in the statement of the theorem differ by a factor of 1 or -1. We may now specialize H_{ij} to 0 to determine that the factor is $+1$, thus concluding the proof.

Theorem 3.16. *Let π be a permutation of $\{1, \ldots, n\}$, and let $\varepsilon(\pi)$ be its sign. Then*

$$\operatorname{Res}(F_{\pi(1)}, \ldots, F_{\pi(n)}) = \varepsilon(\pi)^{d_1 \ldots d_n} \operatorname{Res}(F_1, \ldots, F_n).$$

Proof. Again using Lemma 3.12 with the ideals $(F_1, \ldots, F_n)$ and $(F_{\pi(1)}, \ldots, F_{\pi(n)})$, which are equal, we conclude the desired equality up to a factor ± 1, in $\mathbf{Z}[W_F]$. We determine this sign by specializing F_i to $X_i^{d_i}$, and using the multiplicativity of Theorem 3.10. We are then reduced to the case when $F_i = X_i$, so a linear form; and we can apply Corollary 3.14 to conclude the proof.

The next theorem was an exercise in van der Waerden's *Moderne Algebra*.

Theorem 3.17. *Let $L_1, \ldots, L_{n-1}$, F be generic forms in n variables, such that $L_1, \ldots, L_{n-1}$ are of degree 1, and F has degree $d = d_n$. Let*

$$\Delta_j (j = 1, \ldots, n)$$

be $(-1)^{n-j}$ times the j-th minor determinant of the coefficient matrix of the forms $(L_1, \ldots, L_{n-1})$. Then

$$\operatorname{Res}(L_1, \ldots, L_{n-1}, F) = F(\Delta_1, \ldots, \Delta_n).$$

Proof. We first claim that for all $j = 1, \ldots, n$ we have the congruence

$$(*) \qquad X_n \Delta_j - X_j \Delta_n \equiv 0 \bmod (L_1, \ldots, L_{n-1})\mathbf{Z}[W, X],$$

where as usual, (W) are the coefficients of the forms $L_1, \ldots, L_{n-1}, F$. To see this, we consider the system of linear equations

$$\begin{aligned} W_{11}X_1 + \cdots + W_{1,n-1}X_{n-1} &= L_1(W, X) - W_{1,n}X_n \\ &\cdots\cdots \\ W_{n-1,1}X_1 + \cdots + W_{n-1,n-1}X_{n-1} &= L_{n-1}(W, X) - W_{n-1,n}X_n . \end{aligned}$$

If $C = (C^1, \ldots, C^{n-1})$ is a square matrix with columns C^j, then a solution of a system of linear equations $CX = C^n$ satisfies Cramer's rule

$$X_j \det(C^1, \ldots, C^{n-1}) = \det(C^1, \ldots, C^n, \ldots, C^{n-1}).$$

Using the fact that the determinant is linear in each column, (*) falls out.

Then from the congruence (*) it follows that

$$X_n^d F(\Delta_1, \ldots, \Delta_n) \equiv \Delta_n^d F(X_1, \ldots, X_n) \bmod (L_1, \ldots, L_{n-1})\mathbf{Z}[W, X],$$

whence

$$X_n^d F(\Delta_1, \ldots, \Delta_n) \equiv 0 \bmod (L_1, \ldots, L_{n-1}, F).$$

Hence by Theorem 3.4 and the fact that $\operatorname{Res}(L_1, \ldots, L_{n-1}, F) = R(W)$ generates the elimination ideal, it follows that there exists $c \in \mathbf{Z}[W]$ such that

$$F(\Delta_1, \ldots, \Delta_n) = c\operatorname{Res}(L_1, \ldots, L_{n-1}, F).$$

Since the left side is homogeneous of degree 1 in the coefficients W_F and homogeneous of degree d in the coefficients W_{L_i} for each $i = 1, \ldots, n-1$, it follows from Theorem 3.8 that $c \in \mathbf{Z}$. Specializing L_i to X_i and F to X_n^d makes Δ_j specialize to 0 if $j \neq n$ and Δ_n specializes to 1. Hence the left side specializes to 1, and so does the right side, whence $c = 1$. This concludes the proof.

Bibliography

[Jo 80] J. P. JOUANOLOU, Idéaux résultants, *Advances in Mathematics* **37** No. 3 (1980), pp. 212–238

[Jo 90] J. P. JOUANOLOU, Le formalisme du résultant, *Advances in Mathematics* **90** No. 2 (1991) pp. 117–263

[Jo 91] J. P. JOUANOLOU, *Aspects invariants de l'élimination*, Départment de Mathématiques, Université Louis Pasteur, Strasbourg, France (1991)

[Ma 16] F. MACAULAY, *The algebraic theory of modular systems*, Cambridge University Press, 1916

§4. RESULTANT SYSTEMS

The projection argument used to prove Theorem 3.4 has the advantage of constructing a generic point in a very explicit way. On the other hand, no explicit, or even effective, formula was given to construct a system of forms defining $\mathfrak{A}_1$. We shall now reformulate a version of Theorem 3.4 over $\mathbf{Z}$ and we shall prove it using a completely different technique which constructs effectively a system of generators for an ideal of definition of the arithmetic variety $\mathfrak{A}_1$ in Theorem 3.2.

Theorem 4.1. *Given degrees $d_1, \ldots, d_r \geqq 1$, and positive integers m, n. Let $(W) = (W_{i,(\nu)})$ be the variables as in* §3, (2) *viewed as algebraically independent elements over the integers $\mathbf{Z}$. There exists an effectively determinable finite number of polynomials $R_\rho(W) \in \mathbf{Z}[W]$ having the following property. Let (f) be as in* (1), *a system of forms of the given degrees with coefficients (w) in some field k. Then (f) has a non-trivial common zero if and only if $R_\rho(w) = 0$ for all ρ.*

A finite family $\{R_\rho\}$ having the property stated in Theorem 4.1 will be called a **resultant system** for the given degrees. According to van der Waerden (*Moderne Algebra*, first and second edition, §80), the following technique of proof using resultants goes back to Kronecker elimination, and to a paper of Kapferer (Über Resultanten und Resultantensysteme, *Sitzungsber. Bayer. Akad. München* 1929, pp. 179–200). The family of polynomials $\{R_\rho(W)\}$ is called a **resultant system**, because of the way they are constructed. They form a set of generators for an ideal $\mathfrak{b}_1$ such that the arithmetic variety $\mathfrak{A}_1$ is the set of zeros of $\mathfrak{b}_1$. I don't know how close the system constructed below is to being a set of generators for the prime ideal $\mathfrak{p}_1$ in $\mathbf{Z}[W]$ associated with $\mathfrak{A}_1$. Actually we shall not need the whole theory of Chapter IV, §10; we need only one of the characterizing properties of resultants.

Let p, q be positive integers. Let

$$f_v = v_0X_1^p + v_1X_1^{p-1}X_2 + \cdots + v_pX_2^p$$
$$g_w = w_0X_1^q + w_1X_1^{q-1}X_2 + \cdots + w_qX_2^q$$

be two generic homogeneous polynomials in $\mathbf{Z}[v, w, X_1, X_2] = \mathbf{Z}[v, \mathrm{w}][X]$. In Chapter IV, §10 we defined their resultant $\mathrm{Res}(f_v, g_w)$ in case $X_2 = 1$, but we find it now more appropriate to work with homogeneous polynomials. For our purposes here, we need only the fact that the resultant $R(v, w)$ is characterized by the following property. If we have a specialization (a, b) of (v, w) in a field K, and if f_a, f_b have a factorization

$$f_a = a_0 \prod_{i=1}^{p} (X_1 - \alpha_i X_2)$$

$$g_b = b_0 \prod_{j=1}^{q} (X_1 - \beta_j X_2)$$

then we have the symmetric expressions in terms of the roots:

$$R(a, b) = \mathrm{Res}(f_a, f_b) = a_0^q b_0^p \prod_{i,j} (\alpha_i - \beta_j)$$
$$= a_0^q \prod_i g_b(\alpha_i, 1) = (-1)^{pq} b_0^p \prod_j f_a(\beta_j, 1).$$

From the general theory of symmetric polynomials, it is *a priori* clear that $R(v, w)$ lies in $\mathbf{Z}[v, w]$, and Chapter IV, §10 gives an explicit representation

$$\varphi_{v,w} f_v + \psi_{v,w} g_w = X_2^{p+q-1} R(v, w)$$

where $\varphi_{v,w}$ and $\psi_{v,w} \in \mathbf{Z}[v, w, X]$. This representation will not be needed. The next property will provide the basic inductive step for elimination.

Proposition 4.2. *Let f_a, g_b be homogeneous polynomials with coefficients in a field K. Then $R(a, b) = 0$ if and only if the system of equations*

$$f_a(X) = 0, \quad g_b(X) = 0$$

has a non-trivial zero in some extension of K (which can be taken to be finite).

If $a_0 = 0$ then a zero of g_b is also a zero of f_a; and if $b_0 = 0$ then a zero of f_a is also a zero of g_b. If $a_0 b_0 \neq 0$ then from the expression of the resultant as a product of the difference of roots $(\alpha_i - \beta_j)$ the proposition follows at once.

We shall now prove Theorem 4.1 by using resultants. We do this by induction on n.

If $n = 1$, the theorem is obvious.

If $n = 2$, $r = 1$, the theorem is again obvious, taking the empty set for (R_ρ).

If $n = 2$, $r = 2$, then the theorem amounts to Proposition 4.2.

Assume now $n = 2$ and $r > 2$, so we have a system of homogeneous equations

$$0 = f_1(X) = f_2(X) = \ldots = f_r(X)$$

with $(X) = (X_1, X_2)$. Let d_i be the degree of f_i and let $d = \max d_i$. We replace the family $\{f_j(X)\}$ by the family of all polynomials

$$f_i(X)X_1^{d-d_i} \quad \text{and} \quad f_i(X)X_2^{d-d_i}, \; i = 1, \ldots, r.$$

These two families have the same sets of non-trivial zeros, so to prove Theorem 4.1 we may assume without loss of generality that all the polynomials $f_1, \ldots, f_r$ have the same degree d.

With $n = 2$, consider the generic system of forms of degree d in (X):

(4) $\quad F_i(W, X) = 0$ with $i = 1, \ldots, r$, in two variables $(X) = (X_1, X_2)$,

where the coefficients of F_i are $W_{i,0}, \ldots, W_{i,d}$ so that

$$(W) = (W_{1,0}, \ldots, W_{1,d}, \ldots, W_{r,0}, \ldots, W_{r,d}).$$

The next proposition is a special case of Theorem 4.1, but gives the first step of an induction showing how to get the analogue of Proposition 4.2 for such a larger system. Let $T_1, \ldots, T_r$ and $U_1, \ldots, U_r$ be independent variables over $\mathbf{Z}[W, X]$. Let $F_1, \ldots, F_r$ be the generic forms of §3, (2). Let

$$f = F_1(W, X)T_1 + \cdots + F_r(W, X)T_r$$
$$g = F_1(W, X)U_1 + \cdots + F_r(W, X)U_r$$

so $f, g \in \mathbf{Z}[W, T, U][X]$. Then f, g are polynomials in (X) with coefficients in $\mathbf{Z}[W, T, U]$. We may form their resultant

$$\mathrm{Res}(f, g) \in \mathbf{Z}[W, T, U].$$

Thus $\mathrm{Res}(f, g)$ is a polynomial in the variables (T, U) with coefficients in $\mathbf{Z}[W]$. We let $(Q_\mu(W))$ be the family of coefficients of this polynomial.

Proposition 4.3. *The system $\{Q_\mu(W)\}$ just constructed satisfies the property of Theorem 4.1,* i.e. *it is a resultant system for r forms of the same degree d.*

Proof. Suppose that there is a non-trivial solution of a special system $F_j(W, X) = 0$ with (w) in some field k. Then (w, T, U) is a common non-trivial zero of f, g, so $\mathrm{Res}(f, g) = 0$ and therefore $Q_\mu(w) = 0$ for all μ. Conversely, suppose that $Q_\mu(w) = 0$ for all μ. Let $f_i(X) = F_i(w, X)$. We want to show that $f_i(X)$ for $i = 1, \ldots, r$ have a common non-trivial zero in some extension of

k. If all f_i are 0 in $k[X_1, X_2]$ then they have a common non-trivial zero. If, say, $f_1 \neq 0$ in $k[X]$, then specializing $T_2, \ldots, T_r$ to 0 and T_1 to 1 in the resultant $\mathrm{Res}(f, g)$, we see that

$$\mathrm{Res}(f_1, f_2U_2 + \cdots + f_rU_r) = 0$$

as a polynomial in $k[U_2, \ldots, U_r]$. After making a finite extension of k if necessary, we may assume that $f_1(X)$ splits into linear factors. Let $\{\alpha_i\}$ be the roots of $f_1(X_1, 1)$. Then some $(\alpha_i, 1)$ must also be a zero of $f_2U_2 + \cdots + f_rU_r$, which implies that $(\alpha_i, 1)$ is a common zero of $f_1, \ldots, f_r$ since $U_2, \ldots, U_r$ are algebraically independent over k. This proves Proposition 4.3.

We are now ready to do the inductive step with $n > 2$. Again, let

$$f_i(X) = F_i(w, X) \text{ for } j = 1, \ldots, r$$

be polynomials with coefficients (w) in some fields k.

Remark 4.4. *There exists a non-trivial zero of the system*

$$f_i = 0 \ (i = 1, \ldots, r)$$

in some extension of k if and only if there exist

$$(x_1, \ldots, x_{n-1}) \neq (0, \ldots, 0) \text{ and } (x_n, t) \neq (0, 0)$$

in some extension of k such that

$$f_i(tx_1, \ldots, tx_{n-1}, x_n) = 0 \text{ for } i = 1, \ldots, r.$$

So we may now construct the system (R_ρ) inductively as follows.

Let T be a new variable, and let $X^{(n-1)} = (X_1, \ldots, X_{n-1})$. Let

$$g_i(W, X^{(n-1)}, S_n, T) = F_i(W, TX_1, \ldots, TX_{n-1}, X_n) \in \mathbf{Z}[W, X^{(n-1)}][X_n, T].$$

Then g_i is homogeneous in the two variables (X_n, T). By the theorem for two variables, there is a system of polynomials (Q_μ) in $\mathbf{Z}[W, X^{(n-1)}]$ having the property: *if $(w, x^{(n-1)})$ is a point in a field K, then*

$$g_i(w, x^{(n-1)}, X_n, T) \text{ *have a non-trivial common zero for* } i = 1, \ldots, r.$$
$$\Leftrightarrow Q_\mu(w, x^{(n-1)}) = 0 \text{ *for all* } \mu.$$

Viewing each Q_μ as a polynomial in the variables $(X^{(n-1)})$, we decompose each Q_μ as a sum of its homogeneous terms, and we let $(H_\lambda(W, X^{(n-1)}))$ be the family of these polynomials, homogeneous in $(X^{(n-1)})$. From the homogeneity property of the forms F_j in (X), it follows that if t is transcendental over K and $g_i(w, x^{(n-1)}, X_n, T)$ have a non-trivial common zero for $j = 1, \ldots, r$ then $g_i(w, tx^{(n-1)}, X_n, T)$ also have a non-trivial common zero. Therefore

$Q_\mu(w, tx^{(n-1)}) = 0$ for all μ, and so $H_\lambda(w, x^{(n-1)}) = 0$. Therefore we may use the family of polynomials (H_λ) instead of the family (Q_μ), and we obtain the property: *if* $(w, x^{(n-1)})$ *is a point in a field* K, *then*

$$g_i(w, x^{(n-1)}, X_n, T) \text{ have a non-trivial common zero for } i = 1, \ldots, r$$
$$\Leftrightarrow H_\lambda(w, x^{(n-1)}) = 0 \text{ for all } \lambda.$$

By induction on n, there exists a family $(R_\rho(W))$ of polynomials in $\mathbf{Z}[W]$ (actually homogeneous), having the property: *if* (w) *is a point in a field* K, *then*

$$H_\lambda(w, X^{(n-1)}) \text{ have a non-trivial common zero for all } \lambda$$
$$\Leftrightarrow R_\rho(w) = 0 \text{ for all } \rho.$$

In light of Remark 4.4, this concludes the proof of Theorem 4.1 by the resultant method.

§5. SPEC OF A RING

We shall extend the notions of §2 to arbitrary commutative rings.

Let A be a commutative ring. By spec(A) we mean the set of all prime ideals of A. An element of spec(A) is also called a **point** of spec(A).

If $f \in A$, we view the set of prime ideals $\mathfrak{p}$ of spec(A) containing f as the set of **zeros** of f. Indeed, it is the set of $\mathfrak{p}$ such that the image of f in the canonical homomorphism

$$A \to A/\mathfrak{p}$$

is 0. Let $\mathfrak{a}$ be an ideal, and let $\mathfrak{Z}(\mathfrak{a})$ (the set of **zeros** of $\mathfrak{a}$) be the set of all primes of A containing $\mathfrak{a}$. Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Then we have:

Proposition 5.1.

(i) $\mathfrak{Z}(\mathfrak{ab}) = \mathfrak{Z}(\mathfrak{a}) \cup \mathfrak{Z}(\mathfrak{b})$.

(ii) *If* $\{\mathfrak{a}_i\}$ *is a family of ideals, then* $\mathfrak{Z}(\sum \mathfrak{a}_i) = \bigcap \mathfrak{Z}(\mathfrak{a}_i)$.

(iii) *We have* $\mathfrak{Z}(\mathfrak{a}) \subset \mathfrak{Z}(\mathfrak{b})$ *if and only if* $\mathrm{rad}(\mathfrak{a}) \supset \mathrm{rad}(\mathfrak{b})$, *where* $\mathrm{rad}(\mathfrak{a})$, *the radical of* $\mathfrak{a}$, *is the set of all elements* $x \in A$ *such that* $x^n \in \mathfrak{a}$ *for some positive integer* n.

Proof. Exercise. See Corollary 2.3 of Chapter X.

A subset C of spec(A) is said to be **closed** if there exists an ideal $\mathfrak{a}$ of A such that C consists of those prime ideals $\mathfrak{p}$ such that $\mathfrak{a} \subset \mathfrak{p}$. The complement of a closed subset of spec(A) is called an **open subset** of spec(A). The following statements are then very easy to verify, and will be left to the reader.

Proposition 5.2. *The union of a finite number of closed sets is closed. The intersection of an arbitrary family of closed sets is closed.*

The intersection of a finite number of open sets is open. The union of an arbitrary family of open sets is open.

The empty set and spec(A) *itself are both open and closed.*

If S is a subset of A, then the set of prime ideals $\mathfrak{p} \in \operatorname{spec}(A)$ such that $S \subset \mathfrak{p}$ coincides with the set of prime ideals $\mathfrak{p}$ containing the ideal generated by S.

The collection of open sets as in Proposition 5.2 is said to be a **topology** on spec(A), called the **Zariski topology**.

Remark. In analysis, one considers a compact Hausdorff space S. "Hausdorff" means that given two points P, Q there exists disjoint open sets U_P, U_Q containing P and Q respectively. In the present algebraic context, the topology is not Hausdorff. In the analytic context, let R be the ring of complex valued continuous functions on S. Then the maximal ideals of R are in bijection with the points of S (Gelfand-Naimark theorem). To each point $P \in S$, we associate the ideal M_P of functions f such that $f(P) = 0$. The association $P \mapsto M_P$ gives the bijection. There are analogous results in the complex analytic case. For a non-trivial example, see Exercise 19 of Chapter XII.

Let A, B be commutative rings and $\varphi: A \to B$ a homomorphism. Then φ induces a map

$$\varphi^* = \operatorname{spec}(\varphi) = \varphi^{-1} : \operatorname{spec}(B) \to \operatorname{spec}(A)$$

by

$$\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

Indeed, it is immediately verified that $\varphi^{-1}(\mathfrak{p})$ is a prime ideal of A. Note however that the inverse image of a maximal ideal of B is not necessarily a maximal ideal of A. Example? The reader will verify at once that spec(φ) is continuous, in the sense that if U is open in spec(B), then $\varphi^{-1}(U)$ is open in spec(A).

We can then view spec as a contravariant functor from the category of commutative rings to the category of topological spaces.

By a **point** of spec(A) **in a field** L one means a mapping

$$\operatorname{spec}(\varphi) : \operatorname{spec}(L) \to \operatorname{spec}(A)$$

induced by a homomorphism $\varphi : A \to L$ of A into L.

For example, for each prime number p, we get a point of spec($\mathbf{Z}$), namely the point arising from the reduction map

$$\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}.$$

The corresponding point is given by the reversed arrow,

$$\operatorname{spec}(\mathbf{Z}) \leftarrow \operatorname{spec}(\mathbf{Z}/p\mathbf{Z}).$$

As another example, consider the polynomial ring $k[X_1, \ldots, X_n]$ over a field k. For each n-tuple $(c_1, \ldots, c_n)$ in $k^{a(n)}$ we get a homomorphism

$$\varphi : k[X_1, \ldots, X_n] \to k^a$$

such that φ is the identity on k, and $\varphi(X_i) = c_i$ for all i. The corresponding point is given by the reversed arrow

$$\operatorname{spec} k[X] \leftarrow \operatorname{spec}(k^a).$$

Thus we may identify the points in n-space $k^{a(n)}$ with the points of spec $k[X]$ (over k) in k^a.

However, one does not want to take points only in the algebraic closure of k, and of course one may deal with the case of an arbitrary variety V over k rather than all of affine n-space. Thus let $k[x_1, \ldots, x_n]$ be a finitely generated entire ring over k with a chosen family of generators. Let $V = \operatorname{spec} k[x]$. Let A be a commutative k-algebra, corresponding to a homomorphism $k \to A$. Then a point of V in A may be described either as a homomorphism

$$\varphi\colon k[x_1, \ldots, x_n] \to A,$$

or as the reversed arrow

$$\operatorname{spec}(A) \to \operatorname{spec}(k[x])$$

corresponding to this homomorphism. If we put $c_i = \varphi(x_i)$, then one may call $(c) = (c_1, \ldots, c_n)$ the **coordinates of the point in** A. By a **generic point** of V in a field K we mean a point such that the map $\varphi\colon k[x] \to K$ is injective, i.e. an isomorphism of $k[x]$ with some subring of K.

Let A be a commutative Noetherian ring. We leave it as an exercise to verify the following assertions, which translate the Noetherian condition into properties of closed sets in the Zariski topology.

Closed subsets of spec(A) satisfy the **descending chain condition**, i.e., if

$$C_1 \supset C_2 \supset C_3 \supset \cdots$$

is a descending chain of closed sets, then we have $C_n = C_{n+1}$ for all sufficiently large n. Equivalently, let $\{C_i\}_{i \in I}$ be a family of closed sets. Then there exists a relatively minimal element of this family, that is a closed set C_{i_0} in the family such that for all i, if $C_i \subset C_{i_0}$ then $C_i = C_{i_0}$. The proof follows at once from the corresponding properties of ideals, and the simple formalism relating unions and intersections of closed sets with products and sums of ideals.

A closed set C is said to be **irreducible** if it cannot be expressed as the union of two closed sets

$$C \neq C_1 \cup C_2$$

with $C_1 \neq C$ and $C_2 \neq C$.

Theorem 5.3. *Let A be a Noetherian commutative ring. Then every closed set C can be expressed as a finite union of irreducible closed sets, and this expression is unique if in the union*

$$C = C_1 \cup \cdots \cup C_r$$

of irreducible closed sets, we have $C_i \not\subset C_j$ if $i \neq j$.

Proof. We give the proof as an example to show how the version of Theorem 2.2 has an immediate translation in the more general context of spec(A). Suppose the family of closed sets which cannot be represented as a finite union of irreducible ones is not empty. Translating the Noetherian hypothesis in this case shows that there exists a minimal such set C. Then C cannot be irreducible, and we can write C as a union of closed sets

$$C = C' \cup C'',$$

with $C' \neq C$ and $C'' \neq C$. Since C' and C'' are strictly smaller than C, then we can express C' and C'' as finite unions of irreducible closed sets, thus getting a similar expression for C, and a contradiction which proves existence.

As to uniqueness, let

$$C = C_1 \cup \cdots \cup C_r = Z_1 \cup \cdots \cup Z_s$$

be an expression of C as union of irreducible closed sets, without inclusion relations. For each Z_j we can write

$$Z_j = (Z_j \cap C_1) \cup \cdots \cup (Z_j \cap C_r).$$

Since each $Z_j \cap C_i$ is a closed set, we must have $Z_j = Z_j \cap C_i$ for some i. Hence $Z_j = C_i$ for some i. Similarly, C_i is contained in some Z_k. Since there is no inclusion relation among the Z_j's, we must have $Z_j = C_i = Z_k$. This argument can be carried out for each Z_j and each C_i. This proves that each Z_j appears among the C_i's and each C_i appears among the Z_j's, and proves the uniqueness of our representation. This proves the theorem.

Proposition 5.4. *Let C be a closed subset of* spec(A). *Then C is irreducible if and only if $C = \mathfrak{Z}(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$.*

Proof. Exercise.

More properties at the same basic level will be given in Exercises 14–19.

EXERCISES

Integrality

1. (Hilbert-Zariski) Let k be a field and let V be a homogeneous variety with generic point (x) over k. Let $\mathfrak{Z}$ be the algebraic set of zeros in k^a of a homogeneous ideal in $k[X]$ generated by forms $f_1, \ldots, f_r$ in $k[X]$. Prove that $V \cap \mathfrak{Z}$ has only the trivial zero if and only if each x_i is integral over the ring $k[f(x)] = k[f_1(x), \ldots, f_r(x)]$. (Compare with Theorem 3.7 of Chapter VII.)
2. Let $f_1, \ldots, f_r$ be forms in n variables and suppose $n > r$. Prove that these forms have a non-trivial common zero.
3. Let R be an entire ring. Prove that R is integrally closed if and only if the local ring $R_\mathfrak{p}$ is integrally closed for each prime ideal $\mathfrak{p}$.
4. Let R be an entire ring with quotient field K. Let t be transcendental over K. Let $f(t) = \sum a_i t^i \in K[t]$. Prove:
   (a) If $f(t)$ is integral over $R[t]$, then all a_i are integral over R.
   (b) If R is integrally closed, then $R[t]$ is integrally closed.

For the next exercises, we let $R = k[x] = k[X]/\mathfrak{p}$, where $\mathfrak{p}$ is a homogeneous prime ideal. Then (x) is a homogeneous generic point for a k-variety V. We let I be the integral closure of R in $k(x)$. We assume for simplicity that $k(x)$ is a regular extension of k.

5. Let $z = \sum c_i x_i$ with $c_i \in k$, and $z \neq 0$. If $k[x]$ is integrally closed, prove that $k[x/z]$ is integrally closed.
6. Define an element $f \in k(x)$ to be **homogeneous** if $f(tx) = t^d f(x)$ for t transcendental over $k(x)$ and some integer d. Let $f \in I$. Show that f can be written in the form $f = \sum f_i$ where each f_i is homogeneous of degree $i \geqq 0$, and where also $f_i \in I$. (Some f_i may be 0, of course.)

We let R_m denote the set of elements of R which are homogeneous of degree m. Similarly for I_m. We note that R_m and I_m are vector spaces over k, and that R (resp. I) is the direct sum of all spaces R_m (resp. I_m) for $m = 0, 1, \ldots$ This is obvious for R, and it is true for I because of Exercise 6.

7. Prove that I can be written as a sum $I = Rz_1 + \cdots + Rz_s$, where each z_i is homogeneous of some degree d_i.
8. Define an integer $m \geqq 1$ to be **well behaved** if $I_m^q = I_{qm}$ for all integers $q \geqq 1$. If $R = I$, then all m are well behaved. In Exercise 7, suppose $m \geqq \max d_i$. Show that m is well behaved.
9. (a) Prove that I_m is a finite dimensional vector space over k. Let $w_0, \ldots, w_M$ be a basis for I_m over k. Then $k[I_m] = k[w]$.
   (b) If m is well behaved, show that $k[I_m]$ is integrally closed.
   (c) Denote by $k((x))$ the field generated over k by all quotients x_i/x_j with $x_j \neq 0$, and similarly for $k((w))$. Show that $k((x)) = k((w))$.

(If you want to see Exercises 4–9 worked out, see my *Introduction to Algebraic Geometry*, Interscience 1958, Chapter V.)

Resultants

10. Prove that the resultant defined for n forms in n variables in §3 actually coincides with the resultant of Chapter IV, or §4 when $n = 2$.

11. Let $\mathfrak{a} = (f_1, \ldots, f_r)$ be a homogeneous ideal in $k[X_1, \ldots, X_n)$ (with k algebraically closed). Assume that the only zeros of $\mathfrak{a}$ consist of a finite number of points $(x^{(1)}), \ldots, (x^{(d)})$ in projective space $\mathbf{P}^{n-1}$, so the coordinates of each $x^{(j)}$ can be taken in k. Let $u_1, \ldots, u_n$ be independent variables and let

$$L_u(X) = u_1X_1 + \cdots + u_nX_n.$$

Let $R_1(u), \ldots, R_s(u) \in k[u]$ be a resultant system for $f_1, \ldots, f_r, L_u$.

(a) Show that the common non-trivial zeros of the system $R_i(u)$ $(i = 1, \ldots, s)$ in k are the zeros of the polynomial

$$\prod_j L_u(x^{(j)}) \in k[u].$$

(b) Let $D(u)$ be the greatest common divisor of $R_1(u), \ldots, R_s(u)$ in $k[u]$. Show that there exist integers $m_j \geqq 1$ such that (up to a factor in k)

$$D(u) = \prod_{j=1}^{d} L_u(x^{(j)})^{m_j}.$$

[See van der Waerden, *Moderne Algebra*, Second Edition, Volume II, §79.]

12. For forms in 2 variables, prove directly from the definition used in §4 that one has

$$\operatorname{Res}(fg, h) = \operatorname{Res}(f, h) \operatorname{Res}(g, h)$$

$$\operatorname{Res}(f, g) = (-1)^{(\deg f)(\deg g)} \operatorname{Res}(g, f).$$

13. Let k be a field and let $\mathbf{Z} \to k$ be the canonical homomorphism. If $F \in \mathbf{Z}[W, X]$, we denote by $\overline{F}$ the image of F in $k[W, X]$ under this homomorphism. Thus we get $\overline{R}$, the image of the resultant R.

(a) Show that $\overline{R}$ is a generator of the prime ideal $\mathfrak{p}_{k,1}$ of Theorem 3.5 over the field k. Thus we may denote $\overline{R}$ by R_k.

(b) Show that R is absolutely irreducible, and so is R_k. In other words, R_k is irreducible over the algebraic closure of k.

Spec of a ring

14. Let A be a commutative ring. Define spec(A) to be **connected** if spec(A) is not the union of two disjoint non-empty closed sets (or equivalently, spec(A) is not the union of two disjoint, non-empty open sets).

(a) Suppose that there are idempotents e_1, e_2 in A (that is $e_1^2 = e_1$ and $e_2^2 = e_2$), $\neq 0, 1$, such that $e_1e_2 = 0$ and $e_1 + e_2 = 1$. Show that spec(A) is not connected.

(b) Conversely, if spec(A) is not connected, show that there exist idempotents as in part (a).

In either case, the existence of the idempotents is equivalent with the fact that the ring A is a product of two non-zero rings, $A = A_1 \times A_2$.

15. Prove that the Zariski topology is **compact**, in other words: let $\{U_i\}_{i \in I}$ be a family of open sets such that

$$\bigcup_i U_i = \text{spec}(A).$$

Show that there is a finite number of open sets $U_{i_1}, \ldots, U_{i_n}$ whose union is spec(A). [*Hint*: Use closed sets, and use the fact that if a sum of ideals is the unit ideal, then 1 can be written as a finite sum of elements.]

16. Let f be an element of A. Let S be the multiplicative subset $\{1, f, f^2, f^3, \ldots\}$ consisting of the powers of f. We denote by A_f the ring $S^{-1}A$ as in Chapter II, §3. From the natural homomorphism $A \to A_f$ one gets the corresponding map $\text{spec}(A_f) \to \text{spec}(A)$.
    (a) Show that $\text{spec}(A_f)$ maps on the open set of points in spec(A) which are not zeros of f.
    (b) Given a point $\mathfrak{p} \in \text{spec}(A)$, and an open set U containing $\mathfrak{p}$, show that there exists f such that $\mathfrak{p} \in \text{spec}(A_f) \subset U$.

17. Let $U_i = \text{spec}(A_{f_i})$ be a finite family of open subsets of spec(A) covering spec(A). For each i, let $a_i/f_i \in A_{f_i}$. Assume that as functions on $U_i \cap U_j$ we have $a_i/f_i = a_j/f_j$ for all pairs i, j. Show that there exists a unique element $a \in A$ such that $a = a_i/f_i$ in A_{f_i} for all i.

18. Let k be a field and let $k[x_1, \ldots, x_n] = A \subset K$ be a finitely generated subring of some extension field K. Assume that $k(x_1, \ldots, x_n)$ has transcendence degree r. Show that every maximal chain of prime ideals

$$A \supset P_1 \supset P_2 \supset \ldots \supset P_m \supset \{0\},$$

with $P_1 \neq A$, $P_i \neq P_{i+1}$, $P_m \neq \{0\}$, must have $m = r$.

19. Let $A = \mathbf{Z}[x_1, \ldots, x_n]$ be a finitely generated entire ring over $\mathbf{Z}$. Show that every maximal chain of prime ideals as in Exercise 18 must have $m = r + 1$. Here, r = transcendence degree of $\mathbf{Q}(x_1, \ldots, x_n)$ over $\mathbf{Q}$.

CHAPTER X

Noetherian Rings and Modules

This chapter may serve as an introduction to the methods of algebraic geometry rooted in commutative algebra and the theory of modules, mostly over a Noetherian ring.

§1. BASIC CRITERIA

Let A be a ring and M a module (i.e., a left A-module). We shall say that M is **Noetherian** if it satisfies any one of the following three conditions:

(1) Every submodule of M is finitely generated.

(2) Every ascending sequence of submodules of M,

$$M_1 \subset M_2 \subset M_3 \subset \cdots,$$

such that $M_i \neq M_{i+1}$ is finite.

(3) Every non-empty set S of submodules of M has a maximal element (i.e., a submodule M_0 such that for any element N of S which contains M_0 we have $N = M_0$).

We shall now prove that the above three conditions are equivalent.

(1) $\Rightarrow$ (2) Suppose we have an ascending sequence of submodules of M as above. Let N be the union of all the M_i ($i = 1, 2, \ldots$). Then N is finitely generated, say by elements $x_1, \ldots, x_r$, and each generator is in some M_i. Hence there exists an index j such that

$$x_1, \ldots, x_r \in M_j.$$

S. Lang, *Algebra*
© Springer Science+Business Media LLC 2002

Then

$$\langle x_1, \ldots, x_r \rangle \subset M_j \subset N = \langle x_1, \ldots, x_r \rangle,$$

whence equality holds and our implication is proved.

(2) $\Rightarrow$ (3) Let N_0 be an element of S. If N_0 is not maximal, it is properly contained in a submodule N_1. If N_1 is not maximal, it is properly contained in a submodule N_2. Inductively, if we have found N_i which is not maximal, it is contained properly in a submodule N_{i+1}. In this way we could construct an infinite chain, which is impossible.

(3) $\Rightarrow$ (1) Let N be a submodule of M. Let $a_0 \in N$. If $N \neq \langle a_0 \rangle$, then there exists an element $a_1 \in N$ which does not lie in $\langle a_0 \rangle$. Proceeding inductively, we can find an ascending sequence of submodules of N, namely

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \cdots$$

where the inclusion each time is proper. The set of these submodules has a maximal element, say a submodule $\langle a_0, a_1, \ldots, a_r \rangle$, and it is then clear that this finitely generated submodule must be equal to N, as was to be shown.

Proposition 1.1. *Let M be a Noetherian A-module. Then every submodule and every factor module of M is Noetherian.*

Proof. Our assertion is clear for submodules (say from the first condition). For the factor module, let N be a submodule and $f: M \to M/N$ the canonical homomorphism. Let $\overline{M}_1 \subset \overline{M}_2 \subset \cdots$ be an ascending chain of submodules of M/N and let $M_i = f^{-1}(\overline{M}_i)$. Then $M_1 \subset M_2 \subset \cdots$ is an ascending chain of submodules of M, which must have a maximal element, say M_r, so that $M_i = M_r$ for $r \geqq i$. Then $f(M_i) = \overline{M}_i$ and our assertion follows.

Proposition 1.2. *Let M be a module, N a submodule. Assume that N and M/N are Noetherian. Then M is Noetherian.*

Proof. With every submodule L of M we associate the pair of modules

$$L \mapsto (L \cap N, (L + N)/N).$$

We contend: If $E \subset F$ are two submodules of M such that their associated pairs are equal, then $E = F$. To see this, let $x \in F$. By the hypothesis that $(E + N)/N = (F + N)/N$ there exist elements $u, v \in N$ and $y \in E$ such that $y + u = x + v$. Then

$$x - y = u - v \in F \cap N = E \cap N.$$

Since $y \in E$, it follows the $x \in E$ and our contention is proved. If we have an ascending sequence

$$E_1 \subset E_2 \subset \cdots$$

then the associated pairs form an ascending sequence of submodules of N and M/N respectively, and these sequences must stop. Hence our sequence $E_1 \subset E_2 \cdots$ also stops, by our preceding contention.

Propositions 1.1 and 1.2 may be summarized by saying that in an exact sequence $0 \to M' \to M \to M'' \to 0$, M is Noetherian if and only if M' and M'' are Noetherian.

Corollary 1.3. *Let M be a module, and let N, N' be submodules. If $M = N + N'$ and if both N, N' are Noetherian, then M is Noetherian. A finite direct sum of Noetherian modules is Noetherian.*

Proof. We first observe that the direct product $N \times N'$ is Noetherian since it contains N as a submodule whose factor module is isomorphic to N', and Proposition 1.2 applies. We have a surjective homomorphism

$$N \times N' \to M$$

such that the pair (x, x') with $x \in N$ and $x' \in N'$ maps on $x + x'$. By Proposition 1.1, it follows that M is Noetherian. Finite products (or sums) follow by induction.

A ring A is called **Noetherian** if it is Noetherian as a left module over itself. This means that every left ideal is finitely generated.

Proposition 1.4. *Let A be a Noetherian ring and let M be a finitely generated module. Then M is Noetherian.*

Proof. Let $x_1, \ldots, x_n$ be generators of M. There exists a homomorphism

$$f: A \times A \times \cdots \times A \to M$$

of the product of A with itself n times such that

$$f(a_1, \ldots, a_n) = a_1 x_1 + \cdots + a_n x_n.$$

This homomorphism is surjective. By the corollary of the preceding proposition, the product is Noetherian, and hence M is Noetherian by Proposition 1.1.

Proposition 1.5. *Let A be a ring which is Noetherian, and let $\varphi: A \to B$ be a surjective ring-homomorphism. Then B is Noetherian.*

Proof. Let $\mathfrak{b}_1 \subset \cdots \subset \mathfrak{b}_n \subset \cdots$ be an ascending chain of left ideals of B and let $\mathfrak{a}_i = \varphi^{-1}(\mathfrak{b}_i)$. Then the $\mathfrak{a}_i$ form an ascending chain of left ideals of A which must stop, say at $\mathfrak{a}_r$. Since $\varphi(\mathfrak{a}_i) = \mathfrak{b}_i$ for all i, our proposition is proved.

Proposition 1.6. *Let A be a commutative Noetherian ring, and let S be a multiplicative subset of A. Then $S^{-1}A$ is Noetherian.*

Proof. We leave the proof as an exercise.

Examples. In Chapter IV, we gave the fundamental examples of Noetherian rings, namely polynomial rings and rings of power series. The above propositions show how to construct other examples from these, by taking factor rings or modules, or submodules.

We have already mentioned that for applications to algebraic geometry, it is valuable to consider factor rings of type $k[X]/\mathfrak{a}$, where $\mathfrak{a}$ is an arbitrary ideal. For this and similar reasons, it has been found that the foundations should be laid in terms of modules, not just ideals or factor rings. Notably, we shall first see that the prime ideal associated with an irreducible algebraic set has an analogue in terms of modules. We shall also see that the decomposition of an algebraic set into irreducibles has a natural formulation in terms of modules, namely by expressing a submodule as an intersection or primary modules.

In §6 we shall apply some general notions to get the Hilbert polynomial of a module of finite length, and we shall make comments on how this can be interpreted in terms of geometric notions. Thus the present chapter is partly intended to provide a bridge between basic algebra and algebraic geometry.

§2. ASSOCIATED PRIMES

Throughout this section, we let A be a commutative ring. Modules and homomorphisms are A-modules and A-homomorphisms unless otherwise specified.

Proposition 2.1. *Let S be a multiplicative subset of A, and assume that S does not contain 0. Then there exists an ideal of A which is maximal in the set of ideals not intersecting S, and any such ideal is prime.*

Proof. The existence of such an ideal $\mathfrak{p}$ follows from Zorn's lemma (the set of ideals not meeting S is not empty, because it contains the zero ideal, and is clearly inductively ordered). Let $\mathfrak{p}$ be maximal in the set. Let $a, b \in A$, $ab \in \mathfrak{p}$, but $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. By hypothesis, the ideals $(a, \mathfrak{p})$ and $(b, \mathfrak{p})$ generated by a and $\mathfrak{p}$ (or b and $\mathfrak{p}$ respectively) meet S, and there exist therefore elements $s, s' \in S$, $c, c', x, x' \in A$, $p, p' \in \mathfrak{p}$ such that

$$s = ca + xp \quad \text{and} \quad s' = c'b + x'p'.$$

Multiplying these two expressions, we obtain

$$ss' = cc'ab + p''$$

with some $p'' \in \mathfrak{p}$, whence we see that ss' lies in $\mathfrak{p}$. This contradicts the fact that $\mathfrak{p}$ does not intersect S, and proves that $\mathfrak{p}$ is prime.

An element a of A is said to be **nilpotent** if there exists an integer $n \geqq 1$ such that $a^n = 0$.

Corollary 2.2. *An element a of A is nilpotent if and only if it lies in every prime ideal of A.*

Proof. If $a^n = 0$, then $a^n \in \mathfrak{p}$ for every prime $\mathfrak{p}$, and hence $a \in \mathfrak{p}$. If $a^n \neq 0$ for any positive integer n, we let S be the multiplicative subset of powers of a, namely $\{1, a, a^2, \ldots\}$, and find a prime ideal as in the proposition to prove the converse.

Let $\mathfrak{a}$ be an ideal of A. The **radical** of $\mathfrak{a}$ is the set of all $a \in A$ such that $a^n \in \mathfrak{a}$ for some integer $n \geqq 1$, (or equivalently, it is the set of elements $a \in A$ whose image in the factor ring $A/\mathfrak{a}$ is nilpotent). We observe that the radical of $\mathfrak{a}$ is an ideal, for if $a^n = 0$ and $b^m = 0$ then $(a + b)^k = 0$ if k is sufficiently large: In the binomial expansion, either a or b will appear with a power at least equal to n or m.

Corollary 2.3. *An element a of A lies in the radical of an ideal $\mathfrak{a}$ if and only if it lies in every prime ideal containing $\mathfrak{a}$.*

Proof. Corollary 2.3 is equivalent to Corollary 2.2 applied to the ring $A/\mathfrak{a}$.

We shall extend Corollary 2.2 to modules. We first make some remarks on localization. Let S be a multiplicative subset of A. If M is a module, we can define $S^{-1}M$ in the same way that we defined $S^{-1}A$. We consider equivalence classes of pairs (x, s) with $x \in M$ and $s \in S$, two pairs (x, s) and (x', s') being equivalent if there exists $s_1 \in S$ such that $s_1(s'x - sx') = 0$. We denote the equivalence class of (x, s) by x/s, and verify at once that the set of equivalence classes is an additive group (under the obvious operations). It is in fact an A-module, under the operation

$$(a, x/s) \mapsto ax/s.$$

We shall denote this module of equivalence classes by $S^{-1}M$. (We note that $S^{-1}M$ could also be viewed as an $S^{-1}A$-module.)

If $\mathfrak{p}$ is a prime ideal of A, and S is the complement of $\mathfrak{p}$ in A, then $S^{-1}M$ is also denoted by $M_{\mathfrak{p}}$.

It follows trivially from the definitions that if $N \to M$ is an injective homomorphism, then we have a natural injection $S^{-1}N \to S^{-1}M$. In other words, if N is a submodule of M, then $S^{-1}N$ can be viewed as a submodule of $S^{-1}M$. If $x \in N$ and $s \in S$, then the fraction x/s can be viewed as an element of $S^{-1}N$ or $S^{-1}M$. If $x/s = 0$ in $S^{-1}M$, then there exists $s_1 \in S$ such that $s_1 x = 0$, and this means that x/s is also 0 in $S^{-1}N$. Thus if $\mathfrak{p}$ is a prime ideal and N is a submodule of M, we have a natural inclusion of $N_{\mathfrak{p}}$ in $M_{\mathfrak{p}}$. We shall in fact identify $N_{\mathfrak{p}}$ as a submodule of $M_{\mathfrak{p}}$. In particular, we see that $M_{\mathfrak{p}}$ is the sum of its submodules $(Ax)_{\mathfrak{p}}$, for $x \in M$ (but of course not the direct sum).

Let $x \in M$. The **annihilator** $\mathfrak{a}$ of x is the ideal consisting of all elements $a \in A$ such that $ax = 0$. We have an isomorphism (of modules)

$$A/\mathfrak{a} \xrightarrow{\approx} Ax$$

under the map

$$a \to ax.$$

Lemma 2.4. *Let x be an element of a module M, and let $\mathfrak{a}$ be its annihilator. Let $\mathfrak{p}$ be a prime ideal of A. Then $(Ax)_{\mathfrak{p}} \neq 0$ if and only if $\mathfrak{p}$ contains $\mathfrak{a}$.*

Proof. The lemma is an immediate consequence of the definitions, and will be left to the reader.

Let a be an element of A. Let M be a module. The homomorphism

$$x \mapsto ax, \qquad x \in M$$

will be called the **principal homomorphism** associated with a, and will be denoted by a_M. We shall say that a_M is **locally nilpotent** if for each $x \in M$ there exists an integer $n(x) \geqq 1$ such that $a^{n(x)}x = 0$. This condition implies that for every finitely generated submodule N of M, there exists an integer $n \geqq 1$ such that $a^n N = 0$: We take for n the largest power of a annihilating a finite set of generators of N. Therefore, *if M is finitely generated, a_M is locally nilpotent if and only if it is nilpotent.*

Proposition 2.5. *Let M be a module, $a \in A$. Then a_M is locally nilpotent if and only if a lies in every prime ideal $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$.*

Proof. Assume that a_M is locally nilpotent. Let $\mathfrak{p}$ be a prime of A such that $M_{\mathfrak{p}} \neq 0$. Then there exists $x \in M$ such that $(Ax)_{\mathfrak{p}} \neq 0$. Let n be a positive integer such that $a^n x = 0$. Let $\mathfrak{a}$ be the annihilator of x. Then $a^n \in \mathfrak{a}$, and hence we can apply the lemma, and Corollary 4.3 to conclude that a lies in every prime $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$. Conversely, suppose a_M is not locally nilpotent, so there exists $x \in M$ such that $a^n x = 0$ for all $n \geqq 0$. Let $S = \{1, a, a^2, \ldots\}$, and using Proposition 2.1 let $\mathfrak{p}$ be a prime not intersecting S. Then $(Ax)_{\mathfrak{p}} \neq 0$, so $M_{\mathfrak{p}} \neq 0$ and $a \notin \mathfrak{p}$, as desired.

Let M be a module. A prime ideal $\mathfrak{p}$ of A will be said to be **associated** with M if there exists an element $x \in M$ such that $\mathfrak{p}$ is the annihilator of x. In particular, since $\mathfrak{p} \neq A$, we must have $x \neq 0$.

Proposition 2.6. *Let M be a module $\neq 0$. Let $\mathfrak{p}$ be a maximal element in the set of ideals which are annihilators of elements $x \in M, x \neq 0$. Then $\mathfrak{p}$ is prime.*

Proof. Let $\mathfrak{p}$ be the annihilator of the element $x \neq 0$. Then $\mathfrak{p} \neq A$. Let $a, b \in A$, $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$. Then $ax \neq 0$. But the ideal $(b, \mathfrak{p})$ annihilates ax, and contains $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, it follows that $b \in \mathfrak{p}$, and hence $\mathfrak{p}$ is prime.

Corollary 2.7. *If A is Noetherian and M is a module $\neq 0$, then there exists a prime associated with M.*

Proof. The set of ideals as in Proposition 2.6 is not empty since $M \neq 0$, and has a maximal element because A is Noetherian.

Corollary 2.8. *Assume that both A and M are Noetherian, $M \neq 0$. Then there exists a sequence of submodules*

$$M = M_1 \supset M_2 \supset \cdots \supset M_r = 0$$

such that each factor module M_i/M_{i+1} is isomorphic to $A/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$.

Proof. Consider the set of submodules having the property described in the corollary. It is not empty, since there exists an associated prime $\mathfrak{p}$ of M, and if $\mathfrak{p}$ is the annihilator of x, then $Ax \approx A/\mathfrak{p}$. Let N be a maximal element in the set. If $N \neq M$, then by the preceding argument applied to M/N, there exists a submodule N' of M containing N such that N'/N is isomorphic to $A/\mathfrak{p}$ for some $\mathfrak{p}$, and this contradicts the maximality of N.

Proposition 2.9. *Let A be Noetherian, and $a \in A$. Let M be a module. Then a_M is injective if and only if a does not lie in any associated prime of M.*

Proof. Assume that a_M is not injective, so that $ax = 0$ for some $x \in M$, $x \neq 0$. By Corollary 2.7, there exists an associated prime $\mathfrak{p}$ of Ax, and a is an element of $\mathfrak{p}$. Conversely, if a_M is injective, then a cannot lie in any associated prime because a does not annihilate any non-zero element of M.

Proposition 2.10. *Let A be Noetherian, and let M be a module. Let $a \in A$. The following conditions are equivalent:*

(i) *a_M is locally nilpotent.*

(ii) *a lies in every associated prime of M.*

(iii) *a lies in every prime $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$.*

If $\mathfrak{p}$ is a prime such that $M_{\mathfrak{p}} \neq 0$, then $\mathfrak{p}$ contains an associated prime of M.

Proof. The fact that (i) implies (ii) is obvious from the definitions, and does not need the hypothesis that A is Noetherian. Neither does the fact that (iii) implies (i), which has been proved in Proposition 2.5. We must therefore prove that (ii) implies (iii) which is actually implied by the last statement. The latter is proved as follows. Let $\mathfrak{p}$ be a prime such that $M_{\mathfrak{p}} \neq 0$. Then there exists $x \in M$ such that $(Ax)_{\mathfrak{p}} \neq 0$. By Corollary 2.7, there exists an associated prime $\mathfrak{q}$ of $(Ax)_{\mathfrak{p}}$ in A. Hence there exists an element y/s of $(Ax)_{\mathfrak{p}}$, with $y \in Ax$, $s \notin \mathfrak{p}$, and $y/s \neq 0$, such that $\mathfrak{q}$ is the annihilator of y/s. It follows that $\mathfrak{q} \subset \mathfrak{p}$, for otherwise, there exists $b \in \mathfrak{q}$, $b \notin \mathfrak{p}$, and $0 = by/s$, whence $y/s = 0$, contradiction. Let $b_1, \ldots, b_n$ be generators for $\mathfrak{q}$. For each i, there exists $s_i \in A$, $s_i \notin \mathfrak{p}$, such that $s_i b_i y = 0$ because $b_i y/s = 0$. Let $t = s_1 \cdots s_n$. Then it is trivially verified that $\mathfrak{q}$ is the annihilator of ty in A. Hence $\mathfrak{q} \subset \mathfrak{p}$, as desired.

Let us define the **support** of M by

$\operatorname{supp}(M)$ = set of primes $\mathfrak{p}$ such that $M_{\mathfrak{p}} \neq 0$.

We also have the **annihilator** of M,

$$\operatorname{ann}(M) = \text{set of elements } a \in A \text{ such that } aM = 0.$$

We use the notation

$$\operatorname{ass}(M) = \text{set of associated primes of } M.$$

For any ideal $\mathfrak{a}$ we have its **radical**,

$$\operatorname{rad}(\mathfrak{a}) = \text{set of elements } a \in A \text{ such that } a^n \in \mathfrak{a} \text{ for some integer } n \geqq 1.$$

Then for *finitely generated* M, we can reformulate Proposition 2.10 by the following formula:

$$\operatorname{rad}(\operatorname{ann}(M)) = \bigcap_{\mathfrak{p} \in \operatorname{supp}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \operatorname{ass}(M)} \mathfrak{p}.$$

Corollary 2.11. *Let A be Noetherian, and let M be a module. The following conditions are equivalent:*

(i) *There exists only one associated prime of M.*

(ii) *We have $M \neq 0$, and for every $a \in A$, the homomorphism a_M is injective, or locally nilpotent.*

If these conditions are satisfied, then the set of elements $a \in A$ such that a_M is locally nilpotent is equal to the associated prime of M.

Proof. Immediate consequence of Propositions 2.9 and 2.10.

Proposition 2.12. *Let N be a submodule of M. Every associated prime of N is associated with M also. An associated prime of M is associated with N or with M/N.*

Proof. The first assertion is obvious. Let $\mathfrak{p}$ be an associated prime of M, and say $\mathfrak{p}$ is the annihilator of the element $x \neq 0$. If $Ax \cap N = 0$, then Ax is isomorphic to a submodule of M/N, and hence $\mathfrak{p}$ is associated with M/N. Suppose $Ax \cap N \neq 0$. Let $y = ax \in N$ with $a \in A$ and $y \neq 0$. Then $\mathfrak{p}$ annihilates y. We claim $\mathfrak{p} = \operatorname{ann}(y)$. Let $b \in A$ and $by = 0$. Then $ba \in \mathfrak{p}$ but $a \notin \mathfrak{p}$, so $b \in \mathfrak{p}$. Hence $\mathfrak{p}$ is the annihilator of y in A, and therefore is associated with N, as was to be shown.

§3. PRIMARY DECOMPOSITION

We continue to assume that A is a commutative ring, and that modules (resp. homomorphisms) are A-modules (resp. A-homomorphisms), unless otherwise specified.

Let M be a module. A submodule Q of M is said to be **primary** if $Q \neq M$, and if given $a \in A$, the homomorphism $a_{M/Q}$ is either injective or nilpotent. Viewing A as a module over itself, we see that an ideal $\mathfrak{q}$ is **primary** if and only if it satisfies the following condition:

Given $a, b \in A$, $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, then $b^n \in \mathfrak{q}$ for some $n \geqq 1$.

Let Q be primary. Let $\mathfrak{p}$ be the ideal of elements $a \in A$ such that $a_{M/Q}$ is nilpotent. Then $\mathfrak{p}$ is prime. Indeed, suppose that $a, b \in A$, $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$. Then $a_{M/Q}$ is injective, and consequently $a^n_{M/Q}$ is injective for all $n \geqq 1$. Since $(ab)_{M/Q}$ is nilpotent, it follows that $b_{M/Q}$ must be nilpotent, and hence that $b \in \mathfrak{p}$, proving that $\mathfrak{p}$ is prime. We shall call $\mathfrak{p}$ the prime **belonging** to Q, and also say that Q is $\mathfrak{p}$-primary.

We note the corresponding property for a primary module Q with prime $\mathfrak{p}$:

Let $b \in A$ and $x \in M$ be such that $bx \in Q$. If $x \notin Q$ then $b \in \mathfrak{p}$.

Examples. Let $\mathfrak{m}$ be a maximal ideal of A and let $\mathfrak{q}$ be an ideal of A such that $\mathfrak{m}^k \subset \mathfrak{q}$ for some positive integer k. Then $\mathfrak{q}$ is primary, and $\mathfrak{m}$ belongs to $\mathfrak{q}$. We leave the proof to the reader.

The above conclusion is not always true if $\mathfrak{m}$ is replaced by some prime ideal $\mathfrak{p}$. For instance, let R be a factorial ring with a prime element t. Let A be the subring of polynomials $f(X) \in R[X]$ such that

$$f(X) = a_0 + a_1 X + \dots$$

with a_1 divisible by t. Let $\mathfrak{p} = (tX, X^2, X^3)$. Then $\mathfrak{p}$ is prime but

$$\mathfrak{p}^2 = (t^2X^2, tX^3, X^4)$$

is not primary, as one sees because $X^2 \notin \mathfrak{p}^2$ but $t^k \notin \mathfrak{p}^2$ for all $k \geqq 1$, yet $t^2X^2 \in \mathfrak{p}^2$.

Proposition 3.1. *Let M be a module, and $Q_1, \dots, Q_r$ submodules which are $\mathfrak{p}$-primary for the same prime $\mathfrak{p}$. Then $Q_1 \cap \dots \cap Q_r$ is also $\mathfrak{p}$-primary.*

Proof. Let $Q = Q_1 \cap \dots \cap Q_r$. Let $a \in \mathfrak{p}$. Let n_i be such that $(a_{M/Q_i})^{n_i} = 0$ for each $i = 1, \dots, r$ and let n be the maximum of $n_1, \dots, n_r$. Then $a^n_{M/Q} = 0$, so that $a_{M/Q}$ is nilpotent. Conversely, suppose $a \notin \mathfrak{p}$. Let $x \in M$, $x \notin Q_j$ for some j. Then $a^n x \notin Q_j$ for all positive integers n, and consequently $a_{M/Q}$ is injective. This proves our proposition.

Let N be a submodule of M. When N is written as a finite intersection of primary submodules, say

$$N = Q_1 \cap \cdots \cap Q_r,$$

we shall call this a **primary decomposition** of N. Using Proposition 3.1, we see that by grouping the Q_i according to their primes, we can always obtain from a given primary decomposition another one such that the primes belonging to the primary ideals are all distinct. A primary decomposition as above such that the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ belonging to $Q_1, \ldots, Q_r$ respectively are distinct, and such that N cannot be expressed as an intersection of a proper subfamily of the primary ideals $\{Q_1, \ldots, Q_r\}$ will be said to be **reduced**. By deleting some of the primary modules appearing in a given decomposition, we see that if N admits some primary decomposition, then it admits a reduced one. We shall prove a result giving certain uniqueness properties of a reduced primary decomposition.

Let N be a submodule of M and let $x \mapsto \bar{x}$ be the canonical homomorphism. Let $\overline{Q}$ be a submodule of $\overline{M} = M/N$ and let Q be its inverse image in M. Then directly from the definition, one sees that $\overline{Q}$ is primary if and only if Q is primary; and if they are primary, then the prime belonging to Q is also the prime belonging to $\overline{Q}$. Furthermore, if $N = Q_1 \cap \ldots \cap Q_r$ is a primary decomposition of N in M, then

$$(0) = \overline{Q}_1 \cap \ldots \cap \overline{Q}_r$$

is a primary decomposition of (0) in $\overline{M}$, as the reader will verify at once from the definitions. In addition, the decomposition of N is reduced if and only if the decomposition of (0) is reduced since the primes belonging to one are the same as the primes belonging to the other.

Let $Q_1 \cap \cdots \cap Q_r = N$ be a reduced primary decomposition, and let $\mathfrak{p}_i$ belong to Q_i. If $\mathfrak{p}_i$ does not contain $\mathfrak{p}_j$ $(j \neq i)$ then we say that $\mathfrak{p}_i$ is **isolated**. The isolated primes are therefore those primes which are minimal in the set of primes belonging to the primary modules Q_i.

Theorem 3.2. *Let N be a submodule of M, and let*

$$N = Q_1 \cap \cdots \cap Q_r = Q'_1 \cap \cdots \cap Q'_s$$

be a reduced primary decomposition of N. Then $r = s$. The set of primes belonging to $Q_1, \ldots, Q_r$ and $Q'_1, \ldots, Q'_r$ is the same. If $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ is the set of isolated primes belonging to these decompositions, then $Q_i = Q'_i$ for $i = 1, \ldots, m$, in other words, the primary modules corresponding to isolated primes are uniquely determined.

Proof. The uniqueness of the number of terms in a reduced decomposition and the uniqueness of the family of primes belonging to the primary components will be a consequence of Theorem 3.5 below.

There remains to prove the uniqueness of the primary module belonging to an isolated prime, say $\mathfrak{p}_1$. By definition, for each $j = 2, \ldots, r$ there exists $a_j \in \mathfrak{p}_j$ and $a_j \notin \mathfrak{p}_1$. Let $a = a_2 \cdots a_r$ be the product. Then $a \in \mathfrak{p}_j$ for all $j > 1$, but $a \notin \mathfrak{p}_1$. We can find an integer $n \geqq 1$ such that $a^n_{M/Q_j} = 0$ for $j = 2, \ldots, r$. Let

$$N_1 = \text{set of } x \in M \text{ such that } a^n x \in N.$$

We contend that $Q_1 = N_1$. This will prove the desired uniqueness. Let $x \in Q_1$. Then $a^n x \in Q_1 \cap \cdots \cap Q_r = N$, so $x \in N_1$. Conversely, let $x \in N_1$, so that $a^n x \in N$, and in particular $a^n x \in Q_1$. Since $a \notin \mathfrak{p}_1$, we know by definition that a_{M/Q_1} is injective. Hence $x \in Q_1$, thereby proving our theorem.

Theorem 3.3. *Let M be a Noetherian module. Let N be a submodule of M. Then N admits a primary decomposition.*

Proof. We consider the set of submodules of M which do not admit a primary decomposition. If this set is not empty, then it has a maximal element because M is Noetherian. Let N be this maximal element. Then N is not primary, and there exists $a \in A$ such that $a_{M/N}$ is neither injective nor nilpotent. The increasing sequence of modules

$$\operatorname{Ker} a_{M/N} \subset \operatorname{Ker} a^2_{M/N} \subset \operatorname{Ker} a^3_{M/N} \subset \cdots$$

stops, say at $a^r_{M/N}$. Let $\varphi : M/N \to M/N$ be the endomorphism $\varphi = a^r_{M/N}$. Then $\operatorname{Ker} \varphi^2 = \operatorname{Ker} \varphi$. Hence $0 = \operatorname{Ker} \varphi \cap \operatorname{Im} \varphi$ in M/N, and neither the kernel nor the image of φ is 0. Taking the inverse image in M, we see that N is the intersection of two submodules of M, unequal to N. We conclude from the maximality of N that each one of these submodules admits a primary decomposition, and therefore that N admits one also, contradiction.

We shall conclude our discussion by relating the primes belonging to a primary decomposition with the associated primes discussed in the previous section.

Proposition 3.4. *Let A and M be Noetherian. A submodule Q of M is primary if and only if M/Q has exactly one associated prime $\mathfrak{p}$, and in that case, $\mathfrak{p}$ belongs to Q, i.e. Q is $\mathfrak{p}$-primary.*

Proof. Immediate consequence of the definitions, and Corollary 2.11.

Theorem 3.5. *Let A and M be Noetherian. The associated primes of M are precisely the primes which belong to the primary modules in a reduced primary decomposition of 0 in M. In particular, the set of associated primes of M is finite.*

Proof. Let

$$0 = Q_1 \cap \cdots \cap Q_r$$

be a reduced primary decomposition of 0 in M. We have an injective homomorphism

$$M \to \bigoplus_{i=1}^{r} M/Q_i.$$

By Proposition 2.12 and Proposition 3.4, we conclude that every associated prime of M belongs to some Q_i. Conversely, let $N = Q_2 \cap \cdots \cap Q_r$. Then $N \neq 0$ because our decomposition is reduced. We have

$$N = N/(N \cap Q_1) \approx (N + Q_1)/Q_1 \subset M/Q_1.$$

Hence N is isomorphic to a submodule of M/Q_1, and consequently has an associated prime which can be none other than the prime $\mathfrak{p}_1$ belonging to Q_1. This proves our theorem.

Theorem 3.6. *Let A be a Noetherian ring. Then the set of divisors of zero in A is the set-theoretic union of all primes belonging to primary ideals in a reduced primary decomposition of* 0.

Proof. An element of $a \in A$ is a divisor of 0 if and only if a_A is not injective. According to Proposition 2.9, this is equivalent to a lying in some associated prime of A (viewed as module over itself). Applying Theorem 3.5 concludes the proof.

§4. NAKAYAMA'S LEMMA

We let A denote a commutative ring, but not necessarily Noetherian.

When dealing with modules over a ring, many properties can be obtained first by localizing, thus reducing problems to modules over local rings. In practice, as in the present section, such modules will be finitely generated. This section shows that some aspects can be reduced to vector spaces over a field by reducing modulo the maximal ideal of the local ring. Over a field, a module always has a basis. We extend this property as far as we can to modules finite over a local ring. The first three statements which follow are known as **Nakayama's lemma**.

Lemma 4.1. *Let $\mathfrak{a}$ be an ideal of A which is contained in every maximal ideal of A. Let E be a finitely generated A-module. Suppose that $\mathfrak{a}E = E$. Then $E = \{0\}$.*

Proof. Induction on the number of generators of E. Let $x_1, \ldots, x_s$ be generators of E. By hypothesis, there exist elements $a_1, \ldots, a_s \in \mathfrak{a}$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s,$$

so there is an element a (namely a_s) in $\mathfrak{a}$ such that $(1 + a)x_s$ lies in the module generated by the first $s - 1$ generators. Furthermore $1 + a$ is a unit in A, otherwise $1 + a$ is contained in some maximal ideal, and since a lies in all maximal ideals, we conclude that 1 lies in a maximal ideal, which is not possible. Hence x_s itself lies in the module generated by $s - 1$ generators, and the proof is complete by induction.

Lemma 4.1 applies in particular to the case when A is a local ring, and $\mathfrak{a} = \mathfrak{m}$ is its maximal ideal.

Lemma 4.2. *Let A be a local ring, let E be a finitely generated A-module, and F a submodule. If $E = F + \mathfrak{m}E$, then $E = F$.*

Proof. Apply Lemma 4.1 to E/F.

Lemma 4.3. *Let A be a local ring. Let E be a finitely generated A-module. If $x_1, \ldots, x_n$ are generators for $E \bmod \mathfrak{m}E$, then they are generators for E.*

Proof. Take F to be the submodule generated by $x_1, \ldots, x_n$.

Theorem 4.4. *Let A be a local ring and E a finite projective A-module. Then E is free. In fact, if $x_1, \ldots, x_n$ are elements of E whose residue classes $\bar{x}_1, \ldots, \bar{x}_n$ are a basis of $E/\mathfrak{m}E$ over $A/\mathfrak{m}$, then $x_1, \ldots, x_n$ are a basis of E over A. If $x_1, \ldots, x_r$ are such that $\bar{x}_1, \ldots, \bar{x}_r$ are linearly independent over $A/\mathfrak{m}$, then they can be completed to a basis of E over A.*

Proof. I am indebted to George Bergman for the following proof of the first statement. Let F be a free module with basis $e_1, \ldots, e_n$, and let $f\colon F \to E$ be the homomorphism mapping e_i to x_i. We want to prove that f is an isomorphism. By Lemma 4.3, f is surjective. Since E is projective, it follows that f splits, i.e. we can write $F = P_0 \oplus P_1$, where $P_0 = \operatorname{Ker} f$ and P_1 is mapped isomorphically onto E by f. Now the linear independence of $x_1, \ldots, x_n \bmod \mathfrak{m}E$ shows that

$$P_0 \subset \mathfrak{m}F = \mathfrak{m}P_0 \oplus \mathfrak{m}P_1.$$

Hence $P_0 \subset \mathfrak{m}P_0$. Also, as a direct summand in a finitely generated module, P_0 is finitely generated. So by Lemma 4.3, $P_0 = (0)$ and f is an isomorphism, as was to be proved.

As to the second statement, it is immediate since we can complete a given

sequence $x_1, \ldots, x_r$ with $\bar{x}_1, \ldots, \bar{x}_r$ linearly independent over $A/\mathfrak{m}$, to a sequence $x_1, \ldots, x_n$ with $\bar{x}_1, \ldots, \bar{x}_n$ linearly independent over $A/\mathfrak{m}$, and then we can apply the first part of the proof. This concludes the proof of the theorem.

Let E be a module over a local ring A with maximal ideal $\mathfrak{m}$. We let $E(\mathfrak{m}) = E/\mathfrak{m}E$. If $f: E \to F$ is a homomorphism, then f induces a homomorphism

$$f_{(\mathfrak{m})}: E(\mathfrak{m}) \to F(\mathfrak{m}).$$

If f is surjective, then it follows trivially that $f_{(\mathfrak{m})}$ is surjective.

Proposition 4.5. *Let $f: E \to F$ be a homomorphism of modules, finite over a local ring A. Then:*

(i) *If $f_{(\mathfrak{m})}$ is surjective, so is f.*

(ii) *Assume f is injective. If $f_{(\mathfrak{m})}$ is surjective, then f is an isomorphism.*

(iii) *Assume that E, F are free. If $f_{(\mathfrak{m})}$ is injective (resp. an isomorphism) then f is injective (resp. an isomorphism).*

Proof. The proofs are immediate consequences of Nakayama's lemma and will be left to the reader. For instance, in the first statement, consider the exact sequence

$$E \to F \to F/\mathrm{Im} f \to 0$$

and apply Nakayama to the term on the right. In (iii), use the lifting of bases as in Theorem 4.4.

§5. FILTERED AND GRADED MODULES

Let A be a commutative ring and E a module. By a **filtration** of E one means a sequence of submodules

$$E = E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_n \supset \cdots$$

Strictly speaking, this should be called a descending filtration. We don't consider any other.

Example. Let $\mathfrak{a}$ be an ideal of a ring A, and E an A-module. Let

$$E_n = \mathfrak{a}^n E.$$

Then the sequence of submodules $\{E_n\}$ is a filtration.

More generally, let $\{E_n\}$ be any filtration of a module E. We say that it is an **$\mathfrak{a}$-filtration** if $\mathfrak{a}E_n \subset E_{n+1}$ for all n. The preceding example is an $\mathfrak{a}$-filtration.

We say that an $\mathfrak{a}$-filtration is **$\mathfrak{a}$-stable**, or **stable** if we have $\mathfrak{a}E_n = E_{n+1}$ for all n sufficiently large.

Proposition 5.1. *Let $\{E_n\}$ and $\{E'_n\}$ be stable $\mathfrak{a}$-filtrations of E. Then there exists a positive integer d such that*

$$E_{n+d} \subset E'_n \quad \text{and} \quad E'_{n+d} \subset E_n$$

for all $n \geqq 0$.

Proof. It suffices to prove the proposition when $E'_n = \mathfrak{a}^n E$. Since $\mathfrak{a}E_n \subset E_{n+1}$ for all n, we have $\mathfrak{a}^n E \subset E_n$. By the stability hypothesis, there exists d such that

$$E_{n+d} = \mathfrak{a}^n E_d \subset \mathfrak{a}^n E,$$

which proves the proposition.

A ring A is called **graded** (by the natural numbers) if one can write A as a direct sum (as abelian group),

$$A = \bigoplus_{n=0}^{\infty} A_n,$$

such that for all integers $m, n \geqq 0$ we have $A_n A_m \subset A_{n+m}$. It follows in particular that A_0 is a subring, and that each component A_n is an A_0-module.

Let A be a graded ring. A module E is called a **graded module** if E can be expressed as a direct sum (as abelian group)

$$E = \bigoplus_{n=0}^{\infty} E_n,$$

such that $A_n E_m \subset E_{n+m}$. In particular, E_n is an A_0-module. Elements of E_n are then called **homogeneous of degree** n. By definition, any element of E can be written uniquely as a finite sum of homogeneous elements.

Example. Let k be a field, and let $X_0, \ldots, X_r$ be independent variables. The polynomial ring $A = k[X_0, \ldots, X_r]$ is a graded algebra, with $k = A_0$. The homogeneous elements of degree n are the polynomials generated by the monomials in $X_0, \ldots, X_r$ of degree n, that is

$$X_0^{d_0} \cdots X_r^{d_r} \quad \text{with} \quad \sum_{i=0}^{r} d_i = n.$$

An ideal I of A is called homogeneous if it is graded, as an A-module. If this is the case, then the factor ring A/I is also a graded ring.

Proposition 5.2. *Let A be a graded ring. Then A is Noetherian if and only if A_0 is Noetherian, and A is finitely generated as A_0-algebra.*

Proof. A finitely generated algebra over a Noetherian ring is Noetherian, because it is a homomorphic image of the polynomial ring in finitely many variables, and we can apply Hilbert's theorem.

Conversely, suppose that A is Noetherian. The sum

$$A^+ = \bigoplus_{n=1}^{\infty} A_n$$

is an ideal of A, whose residue class ring is A_0, which is thus a homomorphic image of A, and is therefore Noetherian. Furthermore, A^+ has a finite number of generators $x_1, \ldots, x_s$ by hypothesis. Expressing each generator as a sum of homogeneous elements, we may assume without loss of generality that these generators are homogeneous, say of degrees $d_1, \ldots, d_s$ respectively, with all $d_i > 0$. Let B be the subring of A generated over A_0 by $x_1, \ldots, x_s$. We claim that $A_n \subset B$ for all n. This is certainly true for $n = 0$. Let $n > 0$. Let x be homogeneous of degree n. Then there exist elements $a_i \in A_{n-d_i}$ such that

$$x = \sum_{i=1}^{s} a_i x_i.$$

Since $d_i > 0$ by induction, each a_i is in $A_0[x_1, \ldots, x_s] = B$, so this shows $x \in B$ also, and concludes the proof.

We shall now see two ways of constructing graded rings from filtrations.

First, let A be a ring and $\mathfrak{a}$ an ideal. We view A as a filtered ring, by the powers $\mathfrak{a}^n$. We define the **first associated graded ring** to be

$$S_{\mathfrak{a}}(A) = S = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n.$$

Similarly, if E is an A-module, and E is filtered by an $\mathfrak{a}$-filtration, we define

$$E_S = \bigoplus_{n=0}^{\infty} E_n.$$

Then it is immediately verified that E_S is a graded S-module.

Observe that if A is Noetherian, and $\mathfrak{a}$ is generated by elements $x_1, \ldots, x_s$ then S is generated as an A-algebra also by $x_1, \ldots, x_s$, and is therefore also Noetherian.

Lemma 5.3. *Let A be a Noetherian ring, and E a finitely generated module, with an $\mathfrak{a}$-filtration. Then E_S is finite over S if and only if the filtration of E is $\mathfrak{a}$-stable.*

Proof. Let

$$F_n = \bigoplus_{i=0}^{n} E_i,$$

and let

$$G_n = E_0 \oplus \cdots \oplus E_n \oplus \mathfrak{a}E_n \oplus \mathfrak{a}^2E_n \oplus \mathfrak{a}^3E_n \oplus \cdots$$

Then G_n is an S-submodule of E_S, and is finite over S since F_n is finite over A. We have

$$G_n \subset G_{n+1} \quad \text{and} \quad \bigcup G_n = E_S.$$

Since S is Noetherian, we get:

$$\begin{aligned} E_S \text{ is finite over } S &\Leftrightarrow E_S = G_N \text{ for some } N \\ &\Leftrightarrow E_{N+m} = \mathfrak{a}^m E_N \text{ for all } m \geqq 0 \\ &\Leftrightarrow \text{the filtration of } E \text{ is } \mathfrak{a}\text{-stable.} \end{aligned}$$

This proves the lemma.

Theorem 5.4. (Artin-Rees). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal, E a finite A-module with a stable $\mathfrak{a}$-filtration. Let F be a submodule, and let $F_n = F \cap E_n$. Then $\{F_n\}$ is a stable $\mathfrak{a}$-filtration of F.*

Proof. We have

$$\mathfrak{a}(F \cap E_n) \subset \mathfrak{a}F \cap \mathfrak{a}E_n \subset F \cap E_{n+1},$$

so $\{F_n\}$ is an $\mathfrak{a}$-filtration of F. We can then form the associated graded S-module F_S, which is a submodule of E_S, and is finite over S since S is Noetherian. We apply Lemma 5.3 to conclude the proof.

We reformulate the Artin-Rees theorem in its original form as follows.

Corollary 5.5. *Let A be a Noetherian ring, E a finite A-module, and F a submodule. Let $\mathfrak{a}$ be an ideal. There exists an integer s such that for all integers $n \geqq s$ we have*

$$\mathfrak{a}^n E \cap F = \mathfrak{a}^{n-s}(\mathfrak{a}^s E \cap F).$$

Proof. Special case of Theorem 5.4 and the definitions.

Theorem 5.6. (Krull). *Let A be a Noetherian ring, and let $\mathfrak{a}$ be an ideal contained in every maximal ideal of A. Let E be a finite A-module. Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n E = 0.$$

Proof. Let $F = \bigcap \mathfrak{a}^n E$ and apply Nakayama's lemma to conclude the proof.

Corollary 5.7. *Let* $\mathfrak{o}$ *be a local Noetherian ring with maximal ideal* $\mathfrak{m}$. *Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0.$$

Proof. Special case of Theorem 5.6 when $E = A$.

The second way of forming a graded ring or module is done as follows. Let A be a ring and $\mathfrak{a}$ an ideal of A. We define the **second associated graded ring**

$$\mathrm{gr}_{\mathfrak{a}}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}.$$

Multiplication is defined in the obvious way. Let $a \in \mathfrak{a}^n$ and let $\bar{a}$ denote its residue class mod $\mathfrak{a}^{n+1}$. Let $b \in \mathfrak{a}^m$ and let $\bar{b}$ denote its residue class mod $\mathfrak{a}^{m+1}$. We define the product $\bar{a}\bar{b}$ to be the residue class of ab mod $\mathfrak{a}^{m+n+1}$. It is easily verified that this definition is independent of the choices of representatives and defines a multiplication on $\mathrm{gr}_{\mathfrak{a}}(A)$ which makes $\mathrm{gr}_{\mathfrak{a}}(A)$ into a graded ring.

Let E be a filtered A-module. We define

$$\mathrm{gr}(E) = \bigoplus_{n=0}^{\infty} E_n/E_{n+1}.$$

If the filtration is an $\mathfrak{a}$-filtration, then $\mathrm{gr}(E)$ is a graded $\mathrm{gr}_{\mathfrak{a}}(A)$-module.

Proposition 5.8. *Assume that* A *is Noetherian, and let* $\mathfrak{a}$ *be an ideal of* A. *Then* $\mathrm{gr}_{\mathfrak{a}}(A)$ *is Noetherian. If* E *is a finite* A*-module with a stable* $\mathfrak{a}$*-filtration, then* $\mathrm{gr}(E)$ *is a finite* $\mathrm{gr}_{\mathfrak{a}}(A)$*-module.*

Proof. Let $x_1, \ldots, x_s$ be generators of $\mathfrak{a}$. Let $\bar{x}_i$ be the residue class of x_i in $\mathfrak{a}/\mathfrak{a}^2$. Then

$$\mathrm{gr}_{\mathfrak{a}}(A) = (A/\mathfrak{a})[\bar{x}_1, \ldots, \bar{x}_s]$$

is Noetherian, thus proving the first assertion. For the second assertion, we have for some d,

$$E_{d+m} = \mathfrak{a}^m E_d \qquad \text{for all } m \geqq 0.$$

Hence $\mathrm{gr}(E)$ is generated by the finite direct sum

$$\mathrm{gr}(E)_0 \oplus \cdots \oplus \mathrm{gr}(E)_d.$$

But each $\mathrm{gr}(E)_n = E_n/E_{n+1}$ is finitely generated over A, and annihilated by $\mathfrak{a}$, so is a finite $A/\mathfrak{a}$-module. Hence the above finite direct sum is a finite $A/\mathfrak{a}$-module, so $\mathrm{gr}(E)$ is a finite $\mathrm{gr}_{\mathfrak{a}}(A)$-module, thus concluding the proof of the proposition.

§6. THE HILBERT POLYNOMIAL

The main point of this section is to study the lengths of certain filtered modules over local rings, and to show that they are polynomials in appropriate cases. However, we first look at graded modules, and then relate filtered modules to graded ones by using the construction at the end of the preceding section.

We start with a graded Noetherian ring together with a finite graded A-module E, so

$$A = \bigoplus_{n=0}^{\infty} A_n \quad \text{and} \quad E = \bigoplus_{n=0}^{\infty} E_n.$$

We have seen in Proposition 5.2 that A_0 is Noetherian, and that A is a finitely generated A_0-algebra. The same type of argument shows that E has a finite number of homogeneous generators, and E_n is a finite A_0-module for all $n \geqq 0$.

Let φ be an Euler-Poincaré $\mathbf{Z}$-valued function on the class of all finite A_0-modules, as in Chapter III, §8. We define the **Poincaré series** with respect to φ to be the power series

$$P_\varphi(E, t) = \sum_{n=0}^{\infty} \varphi(E_n)t^n \in \mathbf{Z}[[t]].$$

We write $P(E, t)$ instead of $P_\varphi(E, t)$ for simplicity.

Theorem 6.1. (Hilbert-Serre). *Let s be the number of generators of A as A_0-algebra. Then $P(E, t)$ is a rational function of type*

$$P(E, t) = \frac{f(t)}{\prod_{i=1}^{s} (1 - t^{d_i})}$$

with suitable positive integers d_i, and $f(t) \in \mathbf{Z}[t]$.

Proof. Induction on s. For $s = 0$ the assertion is trivially true. Let $s \geqq 1$. Let $A = A_0[x_1, \ldots, x_s]$, deg. $x_i = d_i \geqq 1$. Multiplication by x_s on E gives rise to an exact sequence

$$0 \to K_n \to E_n \xrightarrow{x_s} E_{n+d_s} \to L_{n+d_s} \to 0.$$

Let

$$K = \bigoplus K_n \quad \text{and} \quad L = \bigoplus L_n.$$

Then K, L are finite A-modules (being submodules and factor modules of E), and are annihilated by x_s, so are in fact graded $A_0[x_1, \ldots, x_{s-1}]$-modules. By definition of an Euler-Poincaré function, we get

$$\varphi(K_n) - \varphi(E_n) + \varphi(E_{n+d_s}) - \varphi(L_{n+d_s}) = 0.$$

Multiplying by t^{n+d_s} and summing over n, we get

$$(1 - t^{d_s})P(E, t) = P(L, t) - t^{d_s}P(K, t) + g(t),$$

where $g(t)$ is a polynomial in $\mathbf{Z}[t]$. The theorem follows by induction.

Remark. In Theorem 6.1, if $A = A_0[x_1, \ldots, x_s]$ then $d_i = \deg x_i$ as shown in the proof. The next result shows what happens when all the degrees are equal to 1.

Theorem 6.2. *Assume that A is generated as an A_0-algebra by homogeneous elements of degree 1. Let d be the order of the pole of $P(E, t)$ at $t = 1$. Then for all sufficiently large n, $\varphi(E_n)$ is a polynomial in n of degree $d - 1$. (For this statement, the zero polynomial is assumed to have degree -1.)*

Proof. By Theorem 6.1, $\varphi(E_n)$ is the coefficient of t^n in the rational function

$$P(E, t) = f(t)/(1 - t)^s.$$

Cancelling powers of $1 - t$, we write $P(E, t) = h(t)/(1 - t)^d$, and $h(1) \neq 0$, with $h(t) \in \mathbf{Z}[t]$. Let

$$h(t) = \sum_{k=0}^{m} a_k t^k.$$

We have the binomial expansion

$$(1 - t)^{-d} = \sum_{k=0}^{\infty} \binom{d + k - 1}{d - 1} t^k.$$

For convenience we let $\binom{n}{-1} = 0$ for $n \geqq 0$ and $\binom{n}{-1} = 1$ for $n = -1$. We then get

$$\varphi(E_n) = \sum_{k=0}^{m} a_k \binom{d + n - k - 1}{d - 1} \qquad \text{for all } n \geqq m.$$

The sum on the right-hand side is a polynomial in n with leading term

$$(\sum a_k) \frac{n^{d-1}}{(d - 1)!} \neq 0.$$

This proves the theorem.

The polynomial of Theorem 6.2 is called the **Hilbert polynomial** of the graded module E, with respect to φ.

We now put together a number of results of this chapter, and give an application of Theorem 6.2 to certain filtered modules.

Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal. Then $A/\mathfrak{q}$ is also Noetherian and local. Since some power of $\mathfrak{m}$ is contained in $\mathfrak{q}$, it follows that $A/\mathfrak{q}$ has only one associated prime, viewed as module over itself, namely $\mathfrak{m}/\mathfrak{q}$ itself. Similarly, if M is a finite $A/\mathfrak{q}$-module, then M has only one associated prime, and the only simple $A/\mathfrak{q}$-module is in fact an $A/\mathfrak{m}$-module which is one-dimensional. Again since some power of $\mathfrak{m}$ is contained in $\mathfrak{q}$, it follows that $A/\mathfrak{q}$ has finite length, and M also has finite length. We now use the length function as an Euler-Poincaré function in applying Theorem 6.2.

Theorem 6.3. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal, and let E be a finitely generated A-module, with a stable $\mathfrak{q}$-filtration. Then:*

(i) *E/E_n has finite length for $n \geqq 0$.*

(ii) *For all sufficiently large n, this length is a polynomial $g(n)$ of degree $\leqq s$, where s is the least number of generators of $\mathfrak{q}$.*

(iii) *The degree and leading coefficient of $g(n)$ depend only on E and $\mathfrak{q}$, but not on the chosen filtration.*

Proof. Let

$$G = \mathrm{gr}_{\mathfrak{q}}(A) = \bigoplus \mathfrak{q}^n/\mathfrak{q}^{n+1}.$$

Then $\mathrm{gr}(E) = \bigoplus E_n/E_{n+1}$ is a graded G-module, and $G_0 = A/\mathfrak{q}$. By Proposition 5.8, G is Noetherian and $\mathrm{gr}(E)$ is a finite G-module. By the remarks preceding the theorem, E/E_n has finite length, and if φ denotes the length, then

$$\varphi(E/E_n) = \sum_{j=1}^{n} \varphi(E_{j-1}/E_j).$$

If $x_1, \ldots, x_s$ generate $\mathfrak{q}$, then the images $\bar{x}_1, \ldots, \bar{x}_s$ in $\mathfrak{q}/\mathfrak{q}^2$ generate G as $A/\mathfrak{q}$-algebra, and each $\bar{x}_i$ has degree 1. By Theorem 6.2 we see that

$$\varphi(E_n/E_{n+1}) = h(n)$$

is a polynomial in n of degree $\leqq s - 1$ for sufficiently large n. Since

$$\varphi(E/E_{n+1}) - \varphi(E/E_n) = h(n),$$

it follows by Lemma 6.4 below that $\varphi(E/E_n)$ is a polynomial $g(n)$ of degree $\leqq s$ for all large n. The last statement concerning the independence of the degree

of g and its leading coefficient from the chosen filtration follows immediately from Proposition 5.1, and will be left to the reader. This concludes the proof.

From the theorem, we see that there is a polynomial $\chi_{E,\mathfrak{q}}$ such that

$$\chi_{E,\mathfrak{q}}(n) = \text{length}(E/\mathfrak{q}^n E)$$

for all sufficiently large n. If $E = A$, then $\chi_{A,\mathfrak{q}}$ is usually called the **characteristic polynomial** of $\mathfrak{q}$. In particular, we see that

$$\chi_{A,\mathfrak{q}}(n) = \text{length}(A/\mathfrak{q}^n)$$

for all sufficiently large n.

For a continuation of these topics into dimension theory, see [AtM 69] and [Mat 80].

We shall now study a particularly important special case having to do with polynomial ideals. Let k be a field, and let

$$A = k[X_0, \ldots, X_N]$$

be the polynomial ring in $N + 1$ variable. Then A is graded, the elements of degree n being the homogeneous polynomials of degree n. We let $\mathfrak{a}$ be a homogeneous ideal of A, and for an integer $n \geqq 0$ we define:

$$\varphi(n) = \dim_k A_n$$

$$\varphi(n, \mathfrak{a}) = \dim_k \mathfrak{a}_n$$

$$\chi(n, \mathfrak{a}) = \dim_k A_n/\mathfrak{a}_n = \dim_k A_n - \dim_k \mathfrak{a}_n = \varphi(n) - \varphi(n, \mathfrak{a}).$$

As earlier in this section, A_n denotes the k-space of homogeneous elements of degree n in A, and similarly for $\mathfrak{a}_n$. Then we have

$$\varphi(n) = \binom{N + n}{N}.$$

We shall consider the **binomial polynomial**

$$\binom{T}{d} = \frac{T(T-1)\cdots(T-d+1)}{d!} = \frac{T^d}{d!} + \text{lower terms.} \tag{1}$$

If f is a function, we define the **difference function** Δf by

$$\Delta f(T) = f(T + 1) - f(T).$$

Then one verifies directly that

$$\Delta\binom{T}{d} = \binom{T}{d-1}. \tag{2}$$

Lemma 6.4. *Let $P \in \mathbf{Q}[T]$ be a polynomial of degree d with rational coefficients.*

(a) *If $P(n) \in \mathbf{Z}$ for all sufficiently large integers n, then there exist integers $c_0, \ldots, c_d$ such that*

$$P(T) = c_0\binom{T}{d} + c_1\binom{T}{d-1} + \ldots + c_d.$$

In particular, $P(n) \in \mathbf{Z}$ for all integers n.

(b) *If $f\colon \mathbf{Z} \to \mathbf{Z}$ is any function, and if there exists a polynomial $Q(T) \in \mathbf{Q}[T]$ such that $Q(\mathbf{Z}) \subset \mathbf{Z}$ and $\Delta f(n) = Q(n)$ for all n sufficiently large, then there exists a polynomial P as in (a) such that $f(n) = P(n)$ for all n sufficiently large.*

Proof. We prove (a) by induction. If the degree of P is 0, then the assertion is obvious. Suppose deg $P \geqq 1$. By (1) there exist rational numbers $c_0, \ldots, c_d$ such that $P(T)$ has the expression given in (a). But ΔP has degree strictly smaller than deg P. Using (2) and induction, we conclude that $c_0, \ldots, c_{d-1}$ must be integers. Finally c_d is an integer because $P(n) \in \mathbf{Z}$ for n sufficiently large. This proves (a).

As for (b), using (a), we can write

$$Q(T) = c_0\binom{T}{d-1} + \ldots + c_{d-1}$$

with integers $c_0, \ldots, c_{d-1}$. Let P_1 be the "integral" of Q, that is

$$P_1(T) = c_0\binom{T}{d} + \ldots + c_{d-1}\binom{T}{1}, \quad \text{so} \quad \Delta P_1 = Q.$$

Then $\Delta(f - P_1)(n) = 0$ for all n sufficiently large. Hence $(f - P_1)(n)$ is equal to a constant c_d for all n sufficiently large, so we let $P = P_1 + c_d$ to conclude the proof.

Proposition 6.5. *Let $\mathfrak{a}, \mathfrak{b}$ be homogeneous ideals in A. Then*

$$\varphi(n, \mathfrak{a}+\mathfrak{b}) = \varphi(n, \mathfrak{a}) + \varphi(n, \mathfrak{b}) - \varphi(n, \mathfrak{a} \cap \mathfrak{b})$$
$$\chi(n, \mathfrak{a}+\mathfrak{b}) = \chi(n, \mathfrak{a}) + \chi(n, \mathfrak{b}) - \chi(n, \mathfrak{a} \cap \mathfrak{b}).$$

Proof. The first is immediate, and the second follows from the definition of χ.

Theorem 6.6. *Let F be a homogeneous polynomial of degree d. Assume that F is not a divisor of zero mod $\mathfrak{a}$, that is: if $G \in A$, $FG \in \mathfrak{a}$, then $G \in \mathfrak{a}$. Then*

$$\chi\big(n, \mathfrak{a} + (F)\big) = \chi(n, \mathfrak{a}) - \chi(n - d, \mathfrak{a}).$$

Proof. First observe that trivially

$$\varphi(n, (F)) = \varphi(n - d),$$

because the degree of a product is the sum of the degrees. Next, using the hypothesis that F is not divisor of 0 mod $\mathfrak{a}$, we conclude immediately

$$\varphi(n, \mathfrak{a} \cap (F)) = \varphi(n - d, \mathfrak{a}).$$

Finally, by Proposition 6.5 (the formula for χ), we obtain:

$$\begin{aligned}
\chi(n, \mathfrak{a} + (F)) &= \chi(n, \mathfrak{a}) + \chi(n, (F)) - \chi(n, \mathfrak{a} \cap (F)) \\
&= \chi(n, \mathfrak{a}) + \varphi(n) - \varphi(n, (F)) - \varphi(n) + \varphi(n, \mathfrak{a} \cap (F)) \\
&= \chi(n, \mathfrak{a}) - \varphi(n - d) + \varphi(n - d, \mathfrak{a}) \\
&= \chi(n, \mathfrak{a}) - \chi(n - d, \mathfrak{a})
\end{aligned}$$

thus proving the theorem.

We denote by $\mathfrak{m}$ the maximal ideal $\mathfrak{m} = (X_0, \ldots, X_N)$ in A. We call $\mathfrak{m}$ the **irrelevant prime ideal**. An ideal is called **irrelevant** if some positive power of $\mathfrak{m}$ is contained in the ideal. In particular, a primary ideal $\mathfrak{q}$ is irrelevant if and only if $\mathfrak{m}$ belongs to $\mathfrak{q}$. Note that by the Hilbert nullstellensatz, the condition that some power of $\mathfrak{m}$ is contained in $\mathfrak{a}$ is equivalent with the condition that the only zero of $\mathfrak{a}$ (in some algebraically closed field containing k) is the trivial zero.

Proposition 6.7. *Let $\mathfrak{a}$ be a homogeneous ideal.*

(a) *If $\mathfrak{a}$ is irrelevant, then $\chi(n, \mathfrak{a}) = 0$ for n sufficiently large.*

(b) *In general, there is an expression $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ as a reduced primary decomposition such that all $\mathfrak{q}_i$ are homogeneous.*

(c) *If an irrelevant primary ideal occurs in the decomposition, let $\mathfrak{b}$ be the intersection of all other primary ideals. Then*

$$\chi(n, \mathfrak{a}) = \chi(n, \mathfrak{b})$$

for all n sufficiently large.

Proof. For (a), by assumption we have $A_n = \mathfrak{a}_n$ for n sufficiently large, so the assertion (a) is obvious. We leave (b) as an exercise. As to (c), say $\mathfrak{q}_s$ is irrelevant, and let $\mathfrak{b} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{s-1}$. By Proposition 6.5, we have

$$\chi(n, \mathfrak{b} + \mathfrak{q}_s) = \chi(n, \mathfrak{b}) + \chi(n, \mathfrak{q}_s) - \chi(n, \mathfrak{a}).$$

But $\mathfrak{b} + \mathfrak{q}_s$ is irrelevant, so (c) follows from (a), thus concluding the proof.

We now want to see that for any homogeneous ideal $\mathfrak{a}$ the function f such that

$$f(n) = \chi(n, \mathfrak{a})$$

satisfies the conditions of Lemma 6.4(b). First, we observe that if we change the ground field from k to an algebraically closed field K containing k, and we let $A_K = K[X_0, \ldots, X_N]$, $\mathfrak{a}_K = K\mathfrak{a}$, then

$$\dim_k A_n = \dim_K A_{K,n} \qquad \text{and} \qquad \dim_k \mathfrak{a}_n = \dim_K \mathfrak{a}_{K,n}.$$

Hence we can assume that k is algebraically closed.

Second, we shall need a geometric notion, that of dimension. Let V be a variety over k, say affine, with generic point $(x) = (x_1, \ldots, x_N)$. We define its **dimension** to be the transcendence degree of $k(x)$ over k. For a projective variety, defined by a homogeneous prime ideal $\mathfrak{p}$, we define its dimension to be the dimension of the homogeneous variety defined by $\mathfrak{p}$ minus 1.

We now need the following lemma.

Lemma 6.8. *Let V, W be varieties over a field k.*

If $V \supset W$ and $\dim V = \dim W$, *then $V = W$.*

Proof. Say V, W are in affine space $\mathbf{A}^N$. Let $\mathfrak{p}_V$ and $\mathfrak{p}_W$ be the respective prime ideals of V and W in $k[X]$. Then we have a canonical homomorphism

$$k[X]/\mathfrak{p}_V \approx k[x] \to k[y] \approx k[X]/\mathfrak{p}_W$$

from the affine coordinate ring of V onto the affine coordinate ring of W. If the transcendence degree of $k(x)$ is the same as that of $k(y)$, and say $y_1, \ldots, y_r$ form a transcendence basis of $k(y)$ over k, then $x_1, \ldots, x_r$ is a transcendence basis of $k(x)$ over k, the homomorphism $k[x] \to k[y]$ induces an isomorphism

$$k[x_1, \ldots, x_r] \xrightarrow{\sim} k[y_1, \ldots, y_r],$$

and hence an isomorphism on the finite extension $k[x]$ to $k[y]$, as desired.

Theorem 6.9. *Let $\mathfrak{a}$ be a homogeneous ideal in A. Let r be the maximum dimension of the irreducible components of the algebraic space in projective space defined by $\mathfrak{a}$. Then there exists a polynomial $P \in \mathbf{Q}[T]$ of degree $\leqq r$, such that $P(\mathbf{Z}) \subset \mathbf{Z}$, and such that*

$$P(n) = \chi(n, \mathfrak{a})$$

for all n sufficiently large.