Chapter 1

A Crash Course in Commutative Algebra

In this chapter we review some basics of commutative algebra which will be assumed in this book.

All rings will be commutative (with identity 1). The natural numbers, $\{0, 1, 2, \ldots\}$, will be denoted by $\mathbb{N}$. The positive integers, $\{1, 2, \ldots\}$, will be denoted by $\mathbb{Z}_+$. Throughout this book, k will be an algebraically closed field (of arbitrary characteristic) unless specified otherwise.

1.1. Basic algebra

The starting point of commutative algebra is the fact that every ring R has a maximal ideal and thus has at least one prime ideal [**13**, Theorem1.3].

We will say that a ring R is a local ring if R has a unique maximal ideal. We will denote the maximal ideal of the local ring R by m_R. If $\phi : R \to S$ is a ring homomorphism and I is an ideal in S, then $\phi^{-1}(I)$ is an ideal in R. If P is a prime ideal in S, then $\phi^{-1}(P)$ is a prime ideal in R. Suppose that R, S are local domains with maximal ideals m_R, m_S, respectively. We will say that S dominates R if $R \subset S$ and $m_S \cap R = m_R$. We will write $\mathrm{QF}(R)$ for the quotient field of a domain R.

A fundamental fact is the following theorem.

Lemma 1.1. *Let $\pi : R \to S$ be a surjective ring homomorphism, with kernel K.*

1) *Suppose that I is an ideal in S. Then $\pi^{-1}(I)$ is an ideal in R containing K.*

2) *Suppose that J is an ideal in R such that J contains K. Then $\pi(J)$ is an ideal in S.*
3) *The map $I \mapsto \pi^{-1}(I)$ is a 1-1 correspondence between the set of ideals in S and the set of ideals in R which contain K. The inverse map is $J \mapsto \pi(J)$.*
4) *The correspondence is order preserving: for ideals I_1, I_2 in S, $I_1 \subset I_2$ if and only if $\pi^{-1}(I_1) \subset \pi^{-1}(I_2)$.*
5) *For an ideal I in S, I is a prime ideal if and only if $\pi^{-1}(I)$ is a prime ideal in R.*
6) *For an ideal I in S, I is a maximal ideal if and only if $\pi^{-1}(I)$ is a maximal ideal in R.*

In the case when $S = R/K$ and $\pi : R \to R/K$ is the map $\pi(x) = x + K$ for $x \in R$, we have that $\pi(J) = J/K$ for J an ideal of R containing K.

Proof. [**84**, Theorem 2.6]. □

A ring S is an R-algebra if there is a given ring homomorphism $\phi : R \to S$. This gives us a multiplication $rs = \phi(r)s$ for $r \in R$ and $s \in S$. Suppose that S is an R-algebra by a homomorphism $\phi : R \to S$ and T is an R-algebra by a homomorphism $\psi : R \to T$. Then a ring homomorphism $\sigma : S \to T$ is an R-algebra homomorphism if $\sigma(\phi(r)) = \psi(r)$ for all $r \in R$.

A proof of the following universal property of polynomial rings can be found in [**84**, Theorem 2.11].

Theorem 1.2. *Suppose that R and S are rings and $R[x_1, \ldots, x_n]$ is a polynomial ring over R. Suppose that $\overline{\phi} : R \to S$ is a ring homomorphism and $t_1, \ldots, t_n \in S$. Then there exists a unique ring homomorphism $\Phi : R[x_1, \ldots, x_n] \to S$ such that $\Phi(r) = \overline{\phi}(r)$ for $r \in R$ and $\Phi(x_i) = t_i$ for $1 \leq i \leq n$.*

A polynomial ring over a ring R is naturally an R-algebra. With the notation of the previous theorem, S is an R-algebra by the homomorphism $\overline{\phi}$, making ϕ an R-algebra homomorphism.

Suppose that $R \subset S$ is a subring and $\Lambda \subset S$ is a subset. Then $R[\Lambda]$ is defined to be the smallest subring of S containing R and Λ. For $n \in \mathbb{N}$, letting $R[x_1, \ldots, x_n]$ be a polynomial ring, we have that

$$R[\Lambda] = \{f(t_1, \ldots, t_n) \mid t_1, \ldots, t_n \in \Lambda \text{ and } f \in R[x_1, \ldots, x_n]\}.$$

If $\Lambda = \{t_1, \ldots, t_n\}$, write $R[\Lambda] = R[t_1, \ldots, t_n]$.

Suppose that we have a surjective ring homomorphism $\Phi : R[x_1, \ldots, x_n] \to S$ from the polynomial ring $R[x_1, \ldots, x_n]$. Letting I be the kernel of Φ,

we have an induced isomorphism $R[x_1, \ldots, x_n]/I \cong S$. Letting $\overline{R} = \Phi(R) \cong R/I \cap R$, we have that $S = \overline{R}[t_1, \ldots, t_n]$ where $t_i = \Phi(x_i)$. More abstractly, if I is an ideal in the polynomial ring $R[x_1, \ldots, x_n]$, let $S = R[x_1, \ldots, x_n]/I$. Let $\overline{R} = R/(I \cap R) \subset S$ and $\overline{x}_i = x_i + I$ in S. Then $S = \overline{R}[\overline{x}_1, \ldots, \overline{x}_n]$.

An element $x \in R$ is a zero divisor if $x \neq 0$ and there exists $0 \neq y \in R$ such that $xy = 0$. An element $x \in R$ is nilpotent if $x \neq 0$ and there exists $n \in \mathbb{N}$ such that $x^n = 0$. The radical of an ideal I in R is

$$\sqrt{I} = \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N}\}.$$

A ring R is reduced if whenever $f \in R$ is such that $f^n = 0$ for some positive integer n, we have that $f = 0$. Suppose that I is an ideal in a ring R. The ring R/I is reduced if and only if $\sqrt{I} = I$.

An R-algebra A is finitely generated if A is generated by a finite number of elements as an R-algebra, so that A is a quotient of a polynomial ring over R in finitely many variables.

If A is nonzero and is generated by $u_1, \ldots, u_n$ as a R-algebra, then $\overline{R} = R1_A$ is a subring of A and $A = \overline{R}[u_1, \ldots, u_n]$. In particular, A is a quotient of a polynomial ring over R.

If K is a field and A is a nonzero K-algebra, then we can view K as a subring of A by identifying K with $K1_A$.

The following lemma will be useful in some of the problems in Chapter 2.

Lemma 1.3. *Suppose that K is a field, $K[x_1, \ldots, x_n, z]$ is a polynomial ring over K, and $f_1, \ldots, f_r, g \in K[x_1, \ldots, x_n]$. Then*

$$\begin{aligned} A &= K[x_1, \ldots, x_n, z]/(f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n), z - g(x_1, \ldots, x_n)) \\ &\cong K[x_1, \ldots, x_n]/(f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n)). \end{aligned}$$

Proof. Let $\overline{x}_1, \ldots, \overline{x}_n, \overline{z}$ be the classes of $x_1, \ldots, x_n, z$ in A. We have that A is generated by $\overline{x}_1, \ldots, \overline{x}_n$ and $\overline{z}$ as a K-algebra, and $\overline{z} = g(\overline{x}_1, \ldots, \overline{x}_n)$, so $A = K[\overline{x}_1, \ldots, \overline{x}_n]$ is generated by $\overline{x}_1, \ldots, \overline{x}_n$ as a K-algebra.

By the universal property of polynomial rings, we have a K-algebra homomorphism $\Phi : K[x_1, \ldots, x_n] \to A$ defined by $\Phi(x_i) = \overline{x}_i$ for $1 \leq i \leq n$. Since $A = K[\overline{x}_1, \ldots, \overline{x}_n]$, Φ is surjective.

We now compute the kernel of Φ. The elements $f_i(x_1, \ldots, x_n)$ are in Kernel(Φ) since $\Phi(f_i) = f_i(\overline{x}_1, \ldots, \overline{x}_n) = 0$. Suppose

$$h(x_1, \ldots, x_n) \in \text{Kernel}(\Phi).$$

Then $\Phi(h(x_1, \ldots, x_n)) = h(\overline{x}_1, \ldots, \overline{x}_n) = 0$ in A, and so $h(x_1, \ldots, x_n)$ is in the ideal

$$(f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n), z - g(x_1, \ldots, x_n))$$

of $K[x_1, \ldots, x_n, z]$ and so

$$\begin{aligned} &h(x_1, \ldots, x_n) \\ &\quad = a_1(x_1, \ldots, x_n, z) f_1(x_1, \ldots, x_n) + \cdots + a_r(x_1, \ldots, x_n, z) f_r(x_1, \ldots, x_n) \\ &\qquad + b(x_1, \ldots, x_n, z)(z - g(x_1, \ldots, x_n)) \end{aligned}$$

for some $a_i, b \in K[x_1, \ldots, x_n, z]$. Setting $z = g(x_1, \ldots, x_n)$, we have

$$\begin{aligned} h(x_1, \ldots, x_n) \;=\; & a_1(x_1, \ldots, x_n, g(x_1, \ldots, x_n)) f_1(x_1, \ldots, x_n) \\ & + \cdots + a_r(x_1, \ldots, x_n, g(x_1, \ldots, x_n)) f_r(x_1, \ldots, x_n). \end{aligned}$$

Thus h is in the ideal $(f_1, \ldots, f_r)$ in $K[x_1, \ldots, x_n]$, and so $\text{Kernel}(\Phi) = (f_1, \ldots, f_r)$. Thus $A \cong K[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. □

The following theorem justifies the common identification of polynomials and polynomial functions over an infinite field.

Theorem 1.4. *Suppose that L is an infinite field and $f \in L[x_1, \ldots, x_n]$ is a nonzero polynomial. Then there exist elements $a_1, \ldots, a_n \in L$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Proof. We prove the theorem by induction on n. A nonzero polynomial $f(x) \in L[x]$ has at most finitely many roots so, since L is infinite, there exists $a \in L$ such that $f(a) \neq 0$.

Assume that $n > 1$ and the theorem is true for $n - 1$ indeterminates. Expand

$$f(x_1, \ldots, x_n) = B_0 + B_1 x_n + \cdots + B_d x_n^d$$

where $B_i \in L[x_1, \ldots, x_{n-1}]$ for all i and $B_d \neq 0$. By induction, there exist $a_i \in L$ such that $B_d(a_1, \ldots, a_{n-1}) \neq 0$. Thus

$$\begin{aligned} &f(a_1, \ldots, a_{n-1}, x_n) \\ &\quad = B_0(a_1, \ldots, a_{n-1}) + B_1(a_1, \ldots, a_{n-1}) x_n + \cdots + B_d(a_1, \ldots, a_{n-1}) x_n^d \end{aligned}$$

is a nonzero polyomial in $L[x_n]$. Hence we can choose $a_n \in L$ such that $f(a_1, \ldots, a_{n-1}, a_n) \neq 0$. □

Theorem 1.5 (Chinese remainder theorem)**.** *Let A be a ring and $I_1, \ldots, I_n$ be ideals in A such that $I_i + I_j = A$ for $i \neq j$ (I_i and I_j are coprime). Given elements $x_1, \ldots, x_n \in A$, there exists $x \in A$ such that $x \equiv x_i \bmod I_i$ for all i.*

Proof. [**95**, page 94]. □

Corollary 1.6. *Let A be a ring and $I_1, \ldots, I_n$ be ideals in A. Assume that $I_i + I_j = A$ for $i \neq j$. Let*

$$f : A \to \bigoplus_{i=1}^{n} A/I_i$$

be homomorphism induced by the canonical maps of A onto each factor A/I_i. Then the kernel of f is $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$ and f is surjective, so we have an isomorphism $A/\bigcap I_i \cong \prod A/I_i$.

Proof. [**95**, page 95]. □

Exercise 1.7. Suppose that R is a domain and $0 \neq f \in R$. Show that $R[x]/(xf - 1) \cong R[\frac{1}{f}]$. Hint: Start by using the universal property of polynomial rings to get an R-algebra homomorphism $\phi : R[x] \to K$ where K is the quotient field of R and $\phi(x) = \frac{1}{f}$.

Exercise 1.8. Let K be a field and $R = K[x, y]/(y^2 - x^3) = K[\overline{x}, \overline{y}]$ where $\overline{x}$, $\overline{y}$ are the classes of x and y in R. Show that R is a domain. Let R_1 be the subring $R_1 = R[\frac{\overline{y}}{\overline{x}}]$ of the quotient field of R. Show that $R_2 = R[t]/(\overline{x}t - \overline{y})$ is not a domain, so that the K-algebras R_1 and R_2 are not isomorphic.

Exercise 1.9. Let K be a field and $R = K[x, y]$ be a polynomial ring in the variables x and y. Let R_1 be the subring $R_1 = R[\frac{y}{x}]$ of the quotient field of R. Let $R_2 = R[t]/(xt - y)$. Show that the K-algebras R_1 and R_2 are isomorphic and that $R_1 = K[x, \frac{y}{x}]$ is a polynomial ring in the variables x and $\frac{y}{x}$.

Exercise 1.10. Suppose that R is a domain and $f, g \in R$ with $g \neq 0$. Show that $R[\frac{f}{g}] \cong R[t]/(tg - f)$ if and only if $(tg - f)$ is a prime ideal in $R[t]$.

Exercise 1.11. Let A be a ring and X be the set of all prime ideals in A. For each subset E of A, let $V(E)$ be the set of all prime ideals in A which contain E. Prove that:

a) If I is the ideal generated by E, then $V(E) = V(I) = V(\sqrt{I})$.

b) $V(0) = X$ and $V(1) = \emptyset$.

c) If $\{E_s\}_{s \in S}$ is any family of subsets of A, then

$$V\left(\bigcup_{s \in S} E_s\right) = \bigcap_{s \in S} V(E_s).$$

d) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideals I, J of A

This exercise shows that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. We call this topology on X the Zariski topology and write $\mathrm{Spec}(A)$ for this topological space.

Exercise 1.12. Suppose that R is a local ring and $f_1, \ldots, f_r \in R$ generate an ideal I of R. Suppose that I is a principal ideal. Show that there exists an index i such that $I = (f_i)$. Give an example to show that this is false in a polynomial ring $k[x]$.

Exercise 1.13. Let κ be a field, and define $\mathrm{Map}(\kappa^n, \kappa)$ to be the set of maps (of sets) from κ^n to κ. Since κ is a κ-algebra, $\mathrm{Map}(\kappa^n, \kappa)$ is a κ-algebra, with the operations $(\phi + \psi)(\alpha) = \phi(\alpha) + \psi(\alpha)$, $(\phi\psi)(\alpha) = \phi(\alpha)\psi(\alpha)$, and $(c\phi)(\alpha) = c\phi(\alpha)$ for $\phi, \psi \in \mathrm{Map}(\kappa^n, \kappa)$, $\alpha \in \kappa^n$, and $c \in \kappa$.

a) Let $\kappa[x_1, \ldots, x_n]$ be a polynomial ring over κ and define

$$\Lambda : \kappa[x_1, \ldots, x_n] \to \mathrm{Map}(\kappa^n, \kappa)$$

by $\Lambda(f)(\alpha) = f(\alpha)$ for $f \in k[x_1, \ldots, x_n]$ and $\alpha \in \kappa^n$. Show that Λ is a κ-algebra homomorphism. The image, $\Lambda(\kappa[x_1, \ldots, x_n])$, is a subring of $\mathrm{Map}(\kappa^n, \kappa)$ which is called the *ring of polynomial functions on* κ^n.

b) Show that Λ is an isomorphism onto the polynomial functions of κ^n if and only if κ is an infinite field.

1.2. Field extensions

Suppose that K is a field and A is a K-algebra. Suppose that Λ is a subset of A. The set Λ is said to be algebraically independent over K if whenever we have a relation

$$f(t_1, \ldots, t_n) = 0$$

for some distinct $t_1, \ldots, t_n \in \Lambda$ and a polynomial f in the polynomial ring $K[x_1, \ldots, x_n]$, we have that $f = 0$ (all the coefficients of f are zero).

Suppose that K is a subfield of a field L and Λ is a subset of L. The subfield $K(\Lambda)$ of L is the smallest subfield of L which contains K and Λ.

A subset Λ of L which is algebraically independent over K and is maximal with respect to inclusions is called a transcendence basis of L over K. Transcendence bases always exist. Any set of algebraically independent elements in L over K can be extended to a transcendence basis of L over K. Any two transcendence bases of L over K have the same cardinality ([**95**, Theorem 1.1, page 356] or [**160**, Theorem 25, page 99]). This cardinality is called the transcendence degree of the field L over K and is written as $\mathrm{trdeg}_K L$.

Suppose that $L \subset M \subset N$ is a tower of fields. Then

$$\mathrm{trdeg}_L N = \mathrm{trdeg}_M N + \mathrm{trdeg}_L M \tag{1.1}$$

by [**160**, Theorem 26, page 100].

An algebraic function field over a field K is a finitely generated field extension $L = K(y_1, \ldots, y_m)$ of K. After possibly permuting $y_1, \ldots, y_m$, there exists an integer r with $0 \leq r \leq m$ such that $y_1, \ldots, y_r$ is a transcendence basis of L over K. The field L is then said to be an r-dimensional algebraic function field. We have that L is finite over $K(y_1, \ldots, y_r)$. The field $K(y_1, \ldots, y_r)$ is isomorphic as a K-algebra to the quotient field of a polynomial ring over K in r variables, so $K(y_1, \ldots, y_r)$ is called a rational function field over K.

The field L is said to be separably generated over K if there exists a transcendence basis $z_1, \ldots, z_n$ of L over K such that L is separably algebraic over $K(z_1, \ldots, z_n)$. The set of elements $z_1, \ldots, z_n$ is then called a separating transcendence basis of L over K.

Theorem 1.14. *If K is a perfect field (K has characteristic 0, or K has characteristic $p > 0$ and all elements of K have a p-th root in K), then all finitely generated field extensions over K are separably generated over K.*

Proof. [**160**, Theorem 31, page 105]. □

In any algebraic extension of fields, there is a maximal separable extension.

Theorem 1.15. *Suppose that L is an algebraic extension of a field K. Then there exits a maximal subfield M of L which is separable algebraic over K and such that L is purely inseparable over M.*

Proof. [**95**, Theorem 4.5, page 241]. □

The M of the conclusions of Theorem 1.15 is called the separable closure of K in L. With the notation of the above theorem, we define

$$[L : K]_s = [M : K] \quad \text{and} \quad [L : K]_i = [L : M]. \tag{1.2}$$

The primitive element theorem gives a nice description of finite separable extensions.

Theorem 1.16 (Primitive element theorem)**.** *Suppose that L is finite extension field of a field K. There exists an element $\alpha \in L$ such that $L = K(\alpha)$ if and only if there exist only a finite number of fields F such that $K \subset F \subset L$. If L is separable over K then there exists such an element α.*

Proof. [**95**, Theorem 4.6, page 243]. □

Suppose that L is a finite extension field of a field K. We will write $\mathrm{Aut}(L/K)$ for the group of K-automorphisms of L. In the case that L is Galois over K, we will write $G(L/K)$ for the Galois group $\mathrm{Aut}(L/K)$.

Exercise 1.17. Suppose that κ is a perfect field of characteristic $p > 0$ and $L = \kappa(s,t)$ is a rational function field over κ. Let $K = \{f^p \mid f \in L\}$. Show that $K = \kappa(s^p, t^p)$, L is finite algebraic over K, and L is not a primitive extension of K.

1.3. Modules

[**13**, Chapter 2] and [**95**, Chapters III and X] are good introductions to the theory of modules over a ring.

An R-module M is a finitely generated R-module if there exist $n \in \mathbb{Z}_+$ and $f_1, \ldots, f_n \in M$ such that $M = \{r_1 f_1 + \cdots + r_n f_n \mid r_1, \ldots, r_n \in R\}$.

The following is Nakayama's lemma.

Lemma 1.18. *Suppose that R is a ring, I is an ideal of R which is contained in all maximal ideals of R, M is a finitely generated R-module, and N is a submodule. If $M = N + IM$, then $M = N$.*

Proof. [**95**, Chapter X, Section 4] or [**13**, Proposition 2.6]. □

We will use the following lemma to determine the minimal number of generators of an ideal.

Lemma 1.19. *Suppose that R is a local ring with maximal ideal $\mathfrak{m}$ and M is a finitely generated R-module. Then the minimal number of elements $\mu(M)$ of M which generate M as an R-module is the $R/\mathfrak{m}$-vector space dimension*

$$\mu(M) = \dim_{R/m} M/\mathfrak{m}M.$$

Proof. Observe that $M/\mathfrak{m}M$ is an $R/\mathfrak{m}$-vector space by the well-defined map $R/\mathfrak{m} \times M/\mathfrak{m}M \to M/\mathfrak{m}M$ given by mapping the classes $[x]$ in $R/\mathfrak{m}$ of $x \in R$ and $[y] \in M/\mathfrak{m}M$ of $y \in M$ to the class $[xy]$ of xy in $M/\mathfrak{m}M$.

Suppose that $a_1, \ldots, a_r$ generate M as an R-module. Then the classes $[a_1], \ldots, [a_r] \in M/\mathfrak{m}M$ generate $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space. Thus

$$\dim_{R/\mathfrak{m}} M/\mathfrak{m}M \le \mu(M).$$

Suppose that $a_1, \ldots, a_r \in M$ are such that the classes $[a_1], \ldots, [a_r] \in M/\mathfrak{m}M$ generate $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space. Let N be the submodule of M generated by $a_1, \ldots, a_r$. Then $N + \mathfrak{m}M = M$ so $N = M$ by Lemma 1.18. Thus

$$\mu(M) \le \dim_{R/\mathfrak{m}} M/\mathfrak{m}M. \qquad \square$$

A chain of submodules of a module M is a sequence of submodules

$$0 = M_n \subset \cdots \subset M_1 \subset M_0 = M. \tag{1.3}$$

The length of (1.3) is n. If each module M_i/M_{i+1} has no submodules other than 0 and M_i/M_{i+1}, then (1.3) is called a composition series. If M has a

composition series, then every composition series of M has length n, and every chain of submodules of M can be extended to a composition series [**13**, Proposition 6.7]. We define the length $\ell_R(M)$ of an R-module M to be the length of a composition series if a composition series exists, and we define $\ell_R(M) = \infty$ if a composition series does not exist. If R is a local ring with maximal ideal m_R containing a field κ such that $R/m_R \cong \kappa$, then any R-module M is naturally a κ-vector space, and

$$\ell_R(M) = \dim_\kappa M.$$

1.4. Localization

A multiplicatively closed (multiplicative) subset S of a ring R is a subset of R such that $1 \in S$ and S is closed under multiplication. Define an equivalence relation $\equiv$ on $R \times S$ by

$$(a, s) \equiv (b, t) \text{ if and only if } (at - bs)u = 0$$

for some $u \in S$. The localization of R with respect to S, denoted by $S^{-1}R$, is the set of equivalence classes $R \times S/\equiv$. The equivalence class of (a, s) is denoted by $\frac{a}{s}$. The localization $S^{-1}R$ is a ring with addition defined by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

and multiplication defined by

$$\left(\frac{a}{s}\right)\left(\frac{b}{t}\right) = \frac{ab}{st}.$$

This definition extends to localization $S^{-1}M$ of R-modules M, in particular for ideals in R [**13**, page 38].

There is a natural ring homomorphism $\phi : R \to S^{-1}R$ defined by $\phi(r) = \frac{r}{1}$ for $r \in R$.

We summarize a few facts from [**13**, Proposition 3.11]. The ideals in $S^{-1}R$ are the ideals $S^{-1}I = I(S^{-1}R)$ such that I is an ideal of R. We have that $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \emptyset$. The prime ideals of $S^{-1}R$ are in 1-1 correspondence with the prime ideals of R which are disjoint from S.

Suppose that $f \in R$. Then $S = \{f^n \mid n \in \mathbb{N}\}$ is a multiplicatively closed set. The localization $S^{-1}R$ is denoted by R_f. Suppose that $\mathfrak{p}$ is a prime ideal in R. Then $S = R \setminus \mathfrak{p}$ is a multiplicatively closed set. The localization $S^{-1}R$ is denoted by $R_\mathfrak{p}$.

If $\mathfrak{p}$ is a prime ideal in a ring R, then $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$.

If R is a domain, the quotient field of R is defined as $\mathrm{QF}(R) = R_{\mathfrak{p}}$ where $\mathfrak{p}$ is the zero ideal of R.

More basic properties of localization and localization of homomorphisms are established in [**13**, Chapter 3].

Exercise 1.20. Suppose that R is a domain and I is an ideal in R. Let R_I be the subset of the quotient field of R defined by

$$R_I = \left\{ \frac{f}{g} \mid f \in R, g \in R \setminus I \right\}.$$

Show that R_I is a ring if and only if I is a prime ideal in R.

Exercise 1.21. Suppose that S is a multiplicative set in a ring R. Show that the kernel of the natural homomorphism $\phi : R \to S^{-1}R$ is the ideal

$$\{g \in R \mid gs = 0 \text{ for some } s \in S\}.$$

Give an example of a ring R and $0 \neq f \in R$ such that the kernel of $R \to R_f$ is nonzero.

Exercise 1.22. Suppose that S and T are multiplicatively closed subsets of a ring R. Let U be the image of T in $S^{-1}R$. Show that $(ST)^{-1}R \cong U^{-1}(S^{-1}R)$, where $ST = \{st \mid s \in S \text{ and } t \in T\}$.

Exercise 1.23. Suppose that R is a ring and P is a prime ideal in R. Show that R_P is a local ring with maximal ideal $PR_P = P_P$. Let $\Lambda : R \to R_P$ be the natural homomorphism defined by $\Lambda(f) = \frac{f}{1}$ for $f \in R$. Show that $\Lambda^{-1}(PR_P) = P$.

1.5. Noetherian rings and factorization

Noetherian rings enjoy many good properties. They are ubiquitous throughout algebraic geometry.

Definition 1.24. A ring R is Noetherian if every ascending chain of ideals

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

is stationary (there exists n_0 such that $I_n = I_{n_0}$ for $n \geq n_0$).

Proposition 1.25. *A ring R is Noetherian if and only if every ideal I in R is finitely generated; that is, there exist $f_1, \ldots, f_n \in I$ for some $n \in \mathbb{Z}_+$ such that*

$$I = (f_1, \ldots, f_n) = f_1 R + \cdots + f_n R.$$

Proof. [**13**, Proposition 6.3]. □

We have the following fundamental theorem.

Theorem 1.26 (Hilbert's basis theorem)**.** *If R is a Noetherian ring, then the polynomial ring $R[x]$ is Noetherian.*

Proof. [**13**, Theorem 7.5, page 81]. □

Corollary 1.27. *A polynomial ring over a field is Noetherian. A quotient of a Noetherian ring is Noetherian. A localization of a Noetherian ring is Noetherian.*

The following lemma will simplify some calculations.

Lemma 1.28. *Suppose that R is a Noetherian ring, $\mathfrak{m}$ is a maximal ideal of R, and N is an R-module such that $\mathfrak{m}^a N = 0$ for some positive integer a. Then $N_{\mathfrak{m}} \cong N$.*

Proof. Suppose that $f \in R \setminus \mathfrak{m}$. We will first prove that for any $r \in \mathbb{Z}_+$, there exists $e \in R$ such that $fe \equiv 1 \bmod \mathfrak{m}^r$.

The ring $R/\mathfrak{m}$ is a field, and the residue of f in $R/\mathfrak{m}$ is nonzero. Thus for any $h \in R$, there exists $g \in R$ such that $fg \equiv h \bmod \mathfrak{m}$. Taking $h = 1$, we obtain that there exists $e_0 \in R$ such that $fe_0 \equiv 1 \bmod \mathfrak{m}$.

Suppose that we have found $e \in R$ such that $fe \equiv 1 \bmod \mathfrak{m}^r$. Let $x_1, \ldots, x_n$ be a set of generators of $\mathfrak{m}$. There exists $h_{i_1,\ldots,i_n} \in R$ such that $fe - 1 = \sum_{i_1+\cdots+i_n=r} h_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$. There exist $g_{i_1,\ldots,i_n} \in R$ such that $fg_{i_1,\ldots,i_n} \equiv h_{i_1,\ldots,i_n} \bmod \mathfrak{m}$. Thus

$$\sum_{i_1+\cdots+i_n=r} fg_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \equiv \sum_{i_1+\cdots+i_n=r} h_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \bmod \mathfrak{m}^{r+1}.$$

Set $e' = e - \sum g_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ to get $fe' \equiv 1 \bmod \mathfrak{m}^{r+1}$.

Consider the natural homomorphism $\Phi : N \to N_{\mathfrak{m}}$ defined by $\Phi(n) = \frac{n}{1}$ for $n \in N$. We will show that Φ is an isomorphism. Suppose that $\Phi(n) = 0$. Then there exists $f \in R \setminus \mathfrak{m}$ such that $fn = 0$. By the first part of the proof, there exists $e \in R$ such that $fe \equiv 1 \bmod \mathfrak{m}^a$. Thus $n = efn = 0$. Suppose $\frac{n}{f} \in N_{\mathfrak{m}}$. Then there exists $e \in R \setminus \mathfrak{m}$ such that $ef = 1 + h$ with $h \in \mathfrak{m}^a$, and $\Phi(ne) = \frac{n}{f}$. □

Suppose R is a domain. A nonzero element $f \in R$ is called irreducible if f is not a unit and whenever we have a factorization $f = gh$ with g and h in R, then g is a unit or h is a unit.

Since every ascending chain of principal ideals is stationary in a Noetherian ring, we have the following proposition.

Proposition 1.29. *Suppose R is a Noetherian domain. Then every nonzero nonunit $f \in R$ has a factorization $f = g_1 \cdots g_r$ for some positive integer r and irreducible elements $g_1, \ldots, g_r \in R$.*

Suppose R is a domain. A nonzero element $f \in R$ is called a prime if the ideal $(f) \subset R$ is a prime ideal.

Proposition 1.30. *Suppose R is a domain and $f \in R$. Then:*

1) *If f is prime, then f is irreducible.*
2) *If R is a unique factorization domain (UFD), then f is a prime if and only if f is irreducible.*

Proof. [**84**, Theorem 2.21]. □

Proposition 1.31. *Suppose that A is a UFD. Let K be the quotient field of A. Then the ring of polynomials in n variables $A[x_1, \ldots, x_n]$ is a UFD. Its units are precisely the units of A, and its prime elements are either primes of A or polynomials which are irreducible in $K[x_1, \ldots, x_n]$ and have content 1 (the greatest common divisor of the coefficients in A of the polynomial is 1).*

Proof. [**95**, Corollary 2.4, page 183]. □

Suppose that R is a ring and $R[x_1, \ldots, x_n]$ is a polynomial ring over R. If $f \in R[x_1, \ldots, x_n]$, then f has a unique expansion

$$f = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

with $a_{i_1,\ldots,i_n} \in R$. If f is nonzero, the (total) degree $\deg f$ of f is defined to be

$$\deg f = \max\{i_1 + \cdots + i_n \mid a_{i_1,\ldots,i_n} \neq 0\}.$$

The polynomial f is homogeneous of degree d if $a_{i_1,\ldots,i_n} = 0$ if $i_1 + \cdots + i_n \neq d$.

Suppose that $A = K[x, y, z, w]$ is a polynomial ring over a field K. The units in A are the nonzero elements of K. Let $f = xy - zw \in A$. Suppose that $f = gh$ with $g, h \in A$ nonunits. Since f is homogeneous of degree 2, we have that g and h are both homogeneous of degree 1, so $g = a_0x + a_1y + a_2z + a_3w$ and $h = b_0x + b_1y + b_2z + b_3w$ with $a_0, \ldots, a_3, b_0, \ldots, b_3 \in K$. We verify by expanding gh that there do not exist $a_0, \ldots, a_3, b_0, \ldots, b_3 \in K$ such that $gh = f$. Thus $xy - zw$ is irreducible in A. Since A is a UFD, we have that (f) is a prime ideal in A, and thus $R = A/(f)$ is a domain. For $u \in A$, let $\overline{u}$ denote the class of u in R. Then $R = K[\overline{x}, \overline{y}, \overline{z}, \overline{w}]$ where $\overline{x}, \overline{y}, \overline{z}, \overline{w}$ are the classes of x, y, z, w. Since f is homogeneous, the function $\deg \overline{g} = \deg g$ if $0 \neq g$ is well-defined on R (we will see that R is graded in Section 3.1). The units of R are the nonzero elements of K (they have

degree 0) and since $\overline{x}, \overline{y}, \overline{z}, \overline{w}$ are all nonzero and they have degree 1, they must be irreducible in R. We have that the ideal $(f, x) = (zw, x)$ in A, so $R/(\overline{x}) \cong A/(zw, x) \cong K[y, z, w]/zw$ by Lemma 1.3, which is not a domain (the classes of z and w are zero divisors). In particular, $\overline{x}$ is an irreducible element of R which is not a prime. We see from Proposition 1.30 that R is not a UFD. We also have that

$$\overline{xy} = \overline{zw}$$

gives two factorizations in R by irreducible elements, none of which are associates, showing directly that R is not a UFD.

Exercise 1.32. Suppose that K is a field and $K[x_1, \ldots, x_n]$ is a polynomial ring over K. Let $f \in K[x_1, \ldots, x_n]$ be nonzero and homogeneous, and suppose that $g, h \in K[x_1, \ldots, x_n]$ are such that $f = gh$. Show that g and h are homogeneous and $\deg g + \deg h = \deg f$.

Exercise 1.33. Suppose that K is an algebraically closed field and $K[x_1, x_2]$ is a polynomial ring over K. Suppose that $f \in K[x_1, x_2]$ is homogeneous of positive degree. Show that f is a product of homogeneous polynomials of degree 1. Show that this is false if K is not algebraically closed.

Exercise 1.34. Let K be a field and $K[x, y, z]$ be a polynomial ring over K. Let $f = y^3 - x^3 + xz^2 \in K[x, y, z]$. Show that f is irreducible and that $R = K[x, y, z]/(f)$ is a domain. Show that R is not a UFD.

Exercise 1.35. Prove Euler's formula: Suppose that K is a field and F is a homogeneous polynomial of degree d in the polynomial ring $K[x_0, \ldots, x_n]$. Show that

$$\sum_{i=0}^{n} \frac{\partial F}{\partial x_i} x_i = dF.$$

1.6. Primary decomposition

Suppose that R is a ring. An ideal Q in R is primary if $Q \neq R$ and if for $x, y \in R$, $xy \in Q$ implies either $x \in Q$ or $y^n \in Q$ for some $n > 0$.

Proposition 1.36. *Let Q be a primary ideal in a ring R. Then $\sqrt{Q}$ is the smallest prime ideal of R containing Q.*

Proof. It suffices to show that $\sqrt{Q}$ is a prime ideal. Suppose $x, y \in R$ are such that $xy \in \sqrt{Q}$. Then $(xy)^n \in Q$ for some $n > 0$. Then either $x^n \in Q$ or $y^{mn} \in Q$ for some $m > 0$. Thus either $x \in \sqrt{Q}$ or $y \in \sqrt{Q}$. □

If $\mathfrak{p}$ is a prime ideal, an ideal Q is called $\mathfrak{p}$-primary if Q is primary and $\sqrt{Q} = \mathfrak{p}$.

Proposition 1.37. *If $\sqrt{I}$ is a maximal ideal $\mathfrak{m}$, then I is $\mathfrak{m}$-primary.*

Proof. [**13**, Proposition 4.2]. □

Lemma 1.38. *If the Q_i are $\mathfrak{p}$-primary, then $Q = \bigcap_{i=1}^n Q_i$ is $\mathfrak{p}$-primary.*

Proof. [**13**, Lemma 4.3]. □

A primary decomposition of an ideal I in R is an expression of I as a finite intersection of primary ideals,

$$I = \bigcap_{i=1}^{n} Q_i. \tag{1.4}$$

The ideal I is called decomposable if it has a primary decomposition. If I is decomposable, then I has a minimal (or irredundant) primary decomposition, that is, an expression (1.4) where the $\sqrt{Q_i}$ are all distinct and $\bigcap_{j\neq i} Q_j \not\subset Q_i$ for all i. By Lemma 1.38, every decomposable ideal I has a minimal primary decomposition.

Theorem 1.39. *In a Noetherian ring R, every ideal has a primary decomposition (and hence has a minimal primary decomposition).*

Proof. [**13**, Theorem 7.13]. □

Let M be an R-module. A prime ideal $\mathfrak{p}$ is an associated prime of M if $\mathfrak{p}$ is the annihilator

$$\mathrm{Ann}(x) = \{r \in R \mid rx = 0\}$$

for some $x \in M$. The set of associated primes of M is denoted by $\mathrm{Ass}(M)$ or $\mathrm{Ass}_R(M)$. In the case of an ideal I of R, it is traditional to abuse notation and call the associated primes of R/I the associated primes of I.

An element a in a ring R is called a zero divisor for an R-module M if there exists a nonzero $x \in M$ such that $ax = 0$. Otherwise, a is M-regular.

Theorem 1.40. *Let A be a Noetherian ring and M a nonzero A-module.*

1) *Every maximal element of the family of ideals $F = \{\mathrm{Ann}(x) \mid 0 \neq x \in M\}$ is an associated prime of M.*
2) *The set of zero divisors for M is the union of all the associated primes of M.*

Proof. 1) We must show that if $\mathrm{Ann}(x)$ is a maximal element of F, then it is prime. If $a, b \in A$ are such that $abx = 0$ but $bx \neq 0$, then by maximality, $\mathrm{Ann}(bx) = \mathrm{Ann}(x)$. Hence $ax = 0$.

2) If $ax = 0$ for some $x \neq 0$, then $a \in \mathrm{Ann}(x) \in F$. By 1), there is an associated prime of M containing $\mathrm{Ann}(x)$. □

Another important set of prime ideals associated to a module M is the support of M, which is

$$\mathrm{Supp}(M) = \{\text{prime ideals } \mathfrak{p} \text{ of } R \mid M_{\mathfrak{p}} \neq 0\}.$$

Theorem 1.41. *Let R be a Noetherian ring and M a finitely generated R-module. Then:*

1) $\mathrm{Ass}(M)$ *is a finite set.*
2) $\mathrm{Ass}(M) \subset \mathrm{Supp}(M)$.
3) *Any minimal element of* $\mathrm{Supp}(M)$ *is in* $\mathrm{Ass}(M)$.

Proof. [**107**, (7.G) on page 52] and [**107**, Theorem 9], or [**106**, Theorem 6.5]. □

The minimal elements of the set $\mathrm{Ass}(M)$ are called minimal or isolated prime ideals belonging to M. The others are called embedded primes. We have that a prime ideal P of R is a minimal prime of an ideal I (a minimal prime of R/I) if $I \subset P$, and if Q is a prime ideal of R such that $I \subset Q \subset P$, then $Q = P$.

Theorem 1.42. *Let I be a decomposable ideal and let $I = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition of I. Then:*

1)
$$\mathrm{Ass}(R/I) = \{\sqrt{Q_i} \mid 1 \leq i \leq n\}.$$
2) *The isolated primary components (the primary components Q_i corresponding to minimal prime ideals $\mathfrak{p}_i$) are uniquely determined by I.*

Proof. [**13**, Theorem 4.5 and Corollary 4.11]. □

Proposition 1.43. *Let S be a multiplicatively closed subset of a ring R and let I be a decomposable ideal. Let $I = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition of I. Let $\mathfrak{p}_i = \sqrt{Q_i}$ and suppose that the Q_i are indexed so that $S \cap \mathfrak{p}_i \neq \emptyset$ for $m < i \leq n$ and $S \cap \mathfrak{p}_i = \emptyset$ for $1 \leq i \leq m$. Then*

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i$$

is a minimal primary decomposition of $S^{-1}I$ in $S^{-1}R$, with $\sqrt{S^{-1}Q_i} = \mathfrak{p}_i S^{-1}R$.

Proof. [**13**, Proposition 4.9]. □

Exercise 1.44. Let K be a field and $R = K[x, y]$ be a polynomial ring. Let $I = (x^2y, xy^2)$. Compute a minimal primary decomposition of I. Compute the set $\mathrm{Ass}(R/I)$. Identify the minimal and embedded primes. Compute $\sqrt{I}$ and compute a minimal primary decomposition of $\sqrt{I}$. Identify the minimal and embedded primes. Compute the set $\mathrm{Ass}(R/\sqrt{I})$. Compute minimal primary decompositions of $I_{\mathfrak{p}}$ and the set $\mathrm{Ass}(I_{\mathfrak{p}})$ when $\mathfrak{p} = (x)$ and when $\mathfrak{p} = (x, y)$. Identify the minimal and embedded primes.

Exercise 1.45. Let K be a field and $R = K[x, y, z]/(z^2 - xy) = K[\overline{x}, \overline{y}, \overline{z}]$. Compute a minimal primary decomposition of the ideal $(\overline{z})$.

Exercise 1.46. Suppose that I is an ideal in a Noetherian ring R and $\sqrt{I} = I$. Show that all elements of $\mathrm{Ass}(R/I)$ are minimal and the minimal primary decomposition of I is

$$I = \bigcap_{\{\text{minimal primes } \mathfrak{p} \text{ of } I\}} \mathfrak{p}.$$

Exercise 1.47. Suppose that R is a Noetherian ring and $I \subset J$ are ideals of R. Show that $I = J$ if and only if $I_{\mathfrak{m}} = J_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R.

1.7. Integral extensions

[**13**, Chapter 5], [**95**, Chapter VII, Section 1] and [**160**, Sections 1–4 of Chapter V] are good references for this section.

Definition 1.48. Suppose that R is a subring of a ring S. An element $u \in S$ is integral over R if u satisfies a relation

$$u^n + a_1u^{n-1} + \cdots + a_{n-1}u + a_n = 0$$

with $a_1, \ldots, a_n \in R$.

Theorem 1.49. *Suppose that R is a subring of a ring S and $u \in S$. The following are equivalent:*

1) *u is integral over R.*
2) *$R[u]$ is a finitely generated R-module.*
3) *$R[u]$ is contained in a subring T of S such that T is a finitely generated R-module.*

Proof. [**13**, Proposition 5.1]. □

We have the following immediate corollaries.

Corollary 1.50. *Let $u_1, \ldots, u_n$ be elements of S which are each integral over R. Then the subring $R[u_1, \ldots, u_n]$ of S is a finitely generated R-module.*

Corollary 1.51. *Suppose that R is a subring of a ring S. Let*

$$\overline{R} = \{u \in S \mid u \text{ is integral over } R\}.$$

Then $\overline{R}$ is a ring.

Proof. If $x, y \in \overline{R}$, then the subring $R[x, y]$ of S is a finitely generated R-module by Corollary 1.50. The elements $x+y$ and xy are in $R[x, y]$ so $x+y$ and xy are integral over R by Theorem 1.49. □

$\overline{R}$ is called the integral closure of R in S. This construction is particularly important when R is a domain and S is the quotient field of R. In this case, $\overline{R}$ is called the normalization of R. R is said to be normal if $\overline{R} = R$. If R is a domain and S is a field extension of the quotient field of R, then the integral closure of R in S is called the normalization of R in S.

We now state some theorems which will be useful.

Lemma 1.52. *Let $A \subset B$ be rings with B integral over A and let S be a multiplicatively closed subset of A. Then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof. Suppose $b \in B$ satisfies a relation

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0$$

with $a_1, a_2, \ldots, a_n \in A$ and $s \in S$. Then

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s} = 0. \qquad \square$$

Theorem 1.53 (Noether's normalization lemma)**.** *Let R be a finitely generated L-algebra, where L is a field. Then there exist $y_1, \ldots, y_r \in R$ such that the subring $L[y_1, \ldots, y_r]$ of R is a polynomial ring over L and R is integral over $L[y_1, \ldots, y_r]$.*

Proof. We give a proof with the assumption that L is an infinite field. For a proof when L is a finite field, we refer to [**161**, Theorem 25 on page 200]. Write $R = L[x_1, \ldots, x_n]$. Suppose that R is not a polynomial ring over L, so there exists a nonzero f in the polynomial ring $L[z_1, \ldots, z_n]$ over L such that $f(x_1, \ldots, x_n) = 0$. Let $d = \deg f$ and let f_d be the homogeneous part of f of degree d, so that

$$f_d = z_n^d f_d\left(\frac{z_1}{z_n}, \ldots, \frac{z_{n-1}}{z_n}, 1\right).$$

By Theorem 1.4, there exist $c_1, \ldots, c_{n-1} \in L$ such that $f_d(c_1, \ldots, c_{n-1}, 1) \neq 0$. Set $y_i = x_i - c_i x_n$ for $1 \leq i \leq n-1$. Then

$$\begin{aligned} 0 = f(x_1, \ldots, x_n) &= f(y_1 + c_1 x_n, \ldots, y_{n-1} + c_{n-1} x_n, x_n) \\ &= f_d(c_1, \ldots, c_{n-1}, 1) x_n^d + g_1 x_n^{d-1} + \cdots + g_d \end{aligned}$$

with all $g_i \in L[y_1, \ldots, y_{n-1}]$, so that x_n is integral over $L[y_1, \ldots, y_{n-1}]$. The theorem then follows by induction on n. □

Theorem 1.54. *Let R be a domain which is a finitely generated algebra over a field K. Let Q be the quotient field of R and let L be a finite algebraic extension of Q. Then the integral closure R' of R in L is a finitely generated R-module and is also a finitely generated K-algebra.*

Lemma 1.55. *Suppose that R is a Noetherian ring, M is a finitely generated R-module, and N is a submodule of M. Then N is a finitely generated R-module.*

Proof. This follows from (1) of the "basic criteria" for a module to be Noetherian of [**95**, page 413] and [**95**, Proposition 1.4, page 415]. □

Let B be a ring and A be a subring. Let P be a prime ideal of A and let Q be a prime ideal of B. We say that Q lies over P if $Q \cap A = P$.

Proposition 1.56. *Let A be a subring of a ring B, let P be a prime ideal of A, and assume B is integral over A. Then $PB \neq B$ and there exists a prime ideal Q of B lying over P.*

Proof. We first show that $PB \neq B$. By Lemma 1.52, it suffices to show that $PS \neq S$ where $S = B_P$. Suppose that $PS = S$. Then there is a relation

$$1 = a_1 b_1 + \cdots + a_n b_n$$

with $a_i \in P$ and $b_i \in S$. Let $R = A_P$ and $S_0 = R[b_1, \ldots, b_n]$. Then $PS_0 = S_0$ and S_0 is a finitely generated R-module by Corollary 1.50, and so $S_0 = 0$ by Nakayama's lemma, Lemma 1.18, a contradiction.

Thus we have that PB_P is contained in a maximal ideal m of B_P. Then $PA_P \subset m \cap A_P$. But PA_P is the maximal ideal of A_P so $m \cap A_P = PA_P$. Let Q be the inverse image of m in B. We have that $P \subset Q \cap A$. Suppose $f \in Q \cap A$. Then $\frac{f}{1} \in m \cap A_P = PA_P$ and so $f \in P$. Thus $P = Q \cap A$. □

We will further develop the theory of integral extensions in Section 21.2.

Exercise 1.57. Suppose that R is a domain which is contained in a field K of characteristic $p > 0$. Suppose that $f \in K$ is such that $f^p \in R$. Let $S = R[f]$. Suppose that Q is a prime ideal in R. Show that $\sqrt{QS}$ is a prime ideal.

Exercise 1.58. Suppose that K is a field and A is a subring of K. Let B be the integral closure of A in K. Let S be a multiplicatively closed subset of A. Show that $S^{-1}B$ is the integral closure of $S^{-1}A$ in K.

Exercise 1.59. Let K be a field and R be a polynomial ring over K. Show that R is integrally closed in its quotient field.

1.8. Dimension

In this section we define the height of an ideal and the dimension (Krull dimension) of a ring.

Definition 1.60. The height, $\mathrm{ht}(P)$, of a prime ideal P in a ring R is the supremum of all natural numbers n such that there exists a chain

$$P_0 \subset P_1 \subset \cdots \subset P_n = P \tag{1.5}$$

of distinct prime ideals. The dimension $\dim R$ of R is the supremum of the heights of all prime ideals in R.

If P is a prime ideal in a ring R, then $\dim R_P = \mathrm{ht}(P)$ by Proposition 1.43.

A chain (1.5) is maximal if the chain cannot be lengthened by adding an additional prime ideal somewhere in the chain.

Definition 1.61. The height of an ideal I in a ring R is

$$\mathrm{ht}(I) = \inf\{\mathrm{ht}(P) \mid P \text{ is a prime ideal of } R \text{ and } I \subset P\}.$$

Theorem 1.62. *Let B be a Noetherian ring and let A be a Noetherian subring over which B is integral. Then* $\dim A = \dim B$.

Proof. [**107**, Theorem 20, page 81]. □

Theorem 1.63. *Let K be a field and A be a finitely generated K-algebra which is a domain. Let L be the quotient field of A. Then* $\dim A = \mathrm{trdeg}_K L$, *the transcendence degree of L over K.*

Proof. The dimension of a polynomial ring over K in n variables is n by [**107**, Theorem 22]. The proof of the theorem now follows from Theorem 1.53 (Noether's normalization lemma) and Theorem 1.62. □

An example of a Noetherian ring which has infinite dimension is given in [**121**, Example 1 of Appendix A1, page 203]. Rings which are finitely generated K-algebras have the following nice property.

Theorem 1.64. *Let K be a field and A be a finitely generated K-algebra which is a domain. For any prime ideal $\mathfrak{p}$ in A we have that*

$$\mathrm{ht}(\mathfrak{p}) + \dim A/\mathfrak{p} = \dim A.$$

Proof. [**28**, Theorem A.16] or [**13**, Chapter 11]. □

There are Noetherian rings which do not satisfy the equality of Theorem 1.64 [**121**, Example 2, Appendix A1].

The following theorem is of fundamental importance.

Theorem 1.65 (Krull's principal ideal theorem)**.** *Let A be a Noetherian ring, and let $f \in A$ be an element which is neither a zero divisor nor a unit. Then every minimal prime ideal $\mathfrak{p}$ containing f has height* 1*.*

Proof. [**13**, Corollary 11.17]. □

Proposition 1.66. *A Noetherian domain A is a UFD if and only if every prime ideal of height* 1 *in A is principal.*

Proof. [**106**, Theorem 20.1] or [**23**, Chapter 7, Section 3] or [**50**, Proposition 3.11]. □

1.9. Depth

Let R be a ring and M be an R-module. Elements $x_1, \ldots, x_r \in R$ are said to be an M-regular sequence if

1) for each $1 \leq i \leq r$, x_i is a nonzero divisor on $M/(x_1, \ldots, x_{i-1})M$ ($x_i y \neq 0$ for all nonzero $y \in M/(x_1, \ldots, x_{i-1})M$) and
2) $M \neq (x_1, \ldots, x_r)M$.

Definition 1.67. Let R be a Noetherian ring, I be an ideal in R, and M be a finitely generated R-module. We define $\operatorname{depth}_I M$ to be the maximal length of an M-regular sequence $x_1, \ldots, x_r$ with all $x_i \in I$.

Definition 1.68. A Noetherian ring R is said to be Cohen-Macaulay if $\operatorname{depth}_I R = \operatorname{ht}(I)$ for every maximal ideal I of R.

We give some examples of Cohen-Macaulay rings in the following theorem and proposition.

Theorem 1.69. *Let A be a Cohen-Macaulay ring. Then the polynomial ring $A[x_1, \ldots, x_n]$ is a Cohen-Macaulay ring. In particular, a polynomial ring over a field is Cohen-Macaulay.*

Proof. [**107**, Theorem 33]. □

Proposition 1.70. *Let A be a Cohen-Macaulay ring and $J = (a_1, \ldots, a_r)$ be an ideal of height r. Then A/J^v is Cohen-Macaulay for every $v > 0$.*

Proof. [**107**, Proposition, page 112]. □

A proof of the following theorem is given in [**50**, Corollary 18.14] or [**107**, Theorem 32].

Theorem 1.71 (Unmixedness theorem)**.** *Let R be a Cohen-Macaulay ring. If $I = (x_1, \ldots, x_n)$ is an ideal such that $\operatorname{ht}(I) = n$, then all associated primes of I are minimal primes of I and have height n.*

Lemma 1.72. *Suppose that R is a ring and $I, P_1, \ldots, P_r$ are ideals in R such that the P_i are prime ideals. Suppose that $I \not\subset P_i$ for each i. Then $I \not\subset \bigcup_i P_i$.*

Proof. We may omit the P_i which are contained in some other P_j and suppose that $P_i \not\subset P_j$ if $i \neq j$. We prove the lemma by induction on r. Suppose $r = 2$ and $I \subset P_1 \cup P_2$. Choose $x \in I \setminus P_2$ and $y \in I \setminus P_1$. Then $x \in P_1$ so $y + x \notin P_1$. Thus y and $y + x \in P_2$ so $x \in P_2$, a contradiction.

Now suppose $r > 2$. Then $IP_1 \cdots P_{r-1} \not\subset P_r$ since P_r is a prime ideal. Choose $x \in IP_1 \cdots P_{r-1} \setminus P_r$. Let $S = I \setminus (P_1 \cup \cdots \cup P_{r-1})$. By induction, $S \neq \emptyset$. Suppose $I \subset P_1 \cup \cdots \cup P_r$. Then $S \subset P_r$. Suppose $s \in S$. Then $s + x \in S$ and thus both s and $s + x$ are in P_r, and so $x \in P_r$, a contradiction. □

Lemma 1.73. *Suppose that R is a Noetherian ring, $\mathfrak{m}$ is a maximal ideal of R, and M is a finite R-module. Then $\operatorname{depth}_{\mathfrak{m}} M = 0$ if and only if $\mathfrak{m} \in \operatorname{Ass}_R(M)$.*

Proof. If $\mathfrak{m}$ is an associated prime for M, then there exists $x \in M$ such that $\mathfrak{m} = \operatorname{Ann}(x)$. Thus $\operatorname{depth}_{\mathfrak{m}} M = 0$.

Suppose $\operatorname{depth}_{\mathfrak{m}} M = 0$. Then all elements of $\mathfrak{m}$ are zero divisors for M. Now the set of all zero divisors for M is the union of the finitely many associated primes of R by Theorems 1.40 and 1.41. Thus $\mathfrak{m}$ is an associated prime of M by Lemma 1.72. □

A proof of the following lemma is given in [**50**, Corollary 18.6].

Lemma 1.74. *Let R be a Noetherian ring, $\mathfrak{m}$ be a maximal ideal of R, and*

$$0 \to N' \to N \to N'' \to 0$$

be a short exact sequence of nonzero finitely generated R-modules. Then

1) $\operatorname{depth}_{\mathfrak{m}} N'' \geq \min\{\operatorname{depth}_{\mathfrak{m}} N, \operatorname{depth}_{\mathfrak{m}} N' - 1\}$,
2) $\operatorname{depth}_{\mathfrak{m}} N' \geq \min\{\operatorname{depth}_{\mathfrak{m}} N, \operatorname{depth}_{\mathfrak{m}} N'' + 1\}$.

Example 1.75. There exists a domain A and a nonzero element $f \in A$ such that the ideal fA has an embedded prime.

We now construct such an example. Let K be a field. We will first show that the two-dimensional domain

$$R = K[s^4, s^3t, st^3, t^4]$$

which is a subring of the polynomial ring $K[s,t]$ has $\text{depth}_m(R) = 1$ where $m = (s^4, s^3t, st^3, t^4)$ (so R is not Cohen-Macaulay). Let

$$S = K[s^4, s^3t, s^2t^2, st^3, t^4].$$

The domain S contains R as a subring, realizing $S = R + s^2t^2R$ as a finitely generated R-module. We have a short exact sequence of R-modules

$$0 \to R \to S \to M \to 0$$

where $M = S/R$. We have that $\text{depth}_m S \geq 1$ since S is a domain which is not a field. Let a be the class of s^2t^2 in M. Consider the surjective R-module homomorphism $\phi : R \to M$ defined by $\phi(f) = fa$ for $f \in R$. Since $ma = 0$, ϕ induces an isomorphism of R-modules $M \cong R/m$. By Lemma 1.74 we have that $\text{depth}_m R \leq 1$, so that $\text{depth}_m R = 1$ since R is a domain which is not a field.

Thus R has the following attribute: For every nonzero $f \in m$,

$$\text{depth}_m R/(f) = 0,$$

so by Lemma 1.73, m is an embedded prime for the ideal (f); that is, a minimal primary decomposition of fR_m is

$$fR_m = Q_1 \cap \cdots \cap Q_t \cap Q_0 \tag{1.6}$$

where the Q_i are P_i-primary for a height 1 prime P_i in R_m (a minimal prime of fR_m) and Q_0 is a nontrivial m_m-primary ideal.

The following theorem will be useful.

Theorem 1.76. *Suppose that R is a Cohen-Macaulay ring and $J = (g_1, \ldots, g_s)$ is an ideal in R such that $g_1, \ldots, g_s$ is an R-regular sequence. Then*

$$\text{gr}_J(R) = \bigoplus_{i \geq 0} J^i/J^{i+1} = R/J[\overline{g}_1, \ldots, \overline{g}_s]$$

is a polynomial ring over R/J in $\overline{g}_1, \ldots, \overline{g}_s$, where $\overline{g}_i$ is the class of g_i in J/J^2.

Proof. This follows from [**107**, Theorem27, page 98] and the equivalence (***) on page 98 of [**107**]. □

1.10. Normal rings and regular rings

Normal and regular rings play an important role in algebraic geometry. In normal rings, the concepts of zeros and poles of a function are well-defined, and regular rings correspond to nonsingular spaces.

We begin this section with some properties of normal rings which we will use. A normal ring is defined in Section 1.7.

Lemma 1.77. *Suppose that A is a domain with quotient field K. Then*

$$A = \bigcap_P A_P$$

where the intersection in K is over all maximal ideals P of A.

Proof. Suppose $x \in K$. Let $D = \{a \in A \mid ax \in A\}$. The element x is in A if and only if $D = A$, and x is in A_P if and only if $D \not\subset P$. Thus if $x \notin A$, there exists a maximal ideal P of A such that $D \subset P$, and so $x \notin A_P$. □

Corollary 1.78. *Suppose that A is a domain. Then A is normal if and only if A_P is normal for all maximal ideals P of A.*

Proof. If A is normal, then $S^{-1}A$ is normal for every multiplicatively closed subset of A not containing 0. Since $A = \bigcap A_P$ by Lemma 1.77, where the intersection is over all maximal ideals P of A, the domain A is normal if and only if A_P is normal for all maximal ideals P. □

A stronger intersection theorem holds for height 1 primes.

Theorem 1.79. *Let A be a Noetherian normal domain. Then:*

1) *All associated primes of a nonzero principal ideal have height* 1.
2) $$A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$$
where the intersection in K is over all height 1 *prime ideals $\mathfrak{p}$ of A.*

Proof. [**107**, Theorem 38] or [**106**, Theorem 11.5]. □

We now develop some concepts to define a regular local ring.

Definition 1.80. Suppose that R is a local ring with maximal ideal m_R. The associated graded ring of R is

$$\mathrm{gr}_{m_R}(R) = \bigoplus_{i \geq 0} m_R^i / m_R^{i+1}.$$

Theorem 1.81. *Suppose that R is a Noetherian local ring with maximal ideal m_R. Then:*

1) $\dim \mathrm{gr}_{m_R}(R) = \dim R$.
2) $\dim_{R/m_R} m_R/m_R^2 \geq \dim R$.

Proof. Equation 1) is proven in [**107**, Theorem 17] or [**106**, Theorem 13.9], using the theory of Hilbert polynomials. Equation 2) follows from [**160**, Theorem 30, page 240, and Theorem 31, page 241] or [**107**, (12.J)]. □

If A is a local ring with maximal ideal m_A and residue field $\kappa = A/m_A$, then the tangent space of A is defined as

$$T(A) = \mathrm{Hom}_\kappa(m_A/m_A^2, \kappa). \tag{1.7}$$

Definition 1.82. A Noetherian local ring R with maximal ideal m_R is a regular local ring if $\dim_{R/m_R} m_R/m_R^2 = \dim R$.

Since $\dim_\kappa T(R) = \dim_\kappa m_R/m_R^2$, we always have that $\dim_\kappa T(R) \geq \dim R$ and R is regular if and only if $\dim_\kappa T(R) = \dim R$.

We now state some useful properties of regular local rings and their relation to normal rings.

Theorem 1.83. *Let A be a ring such that for every prime ideal P of A the localization A_P is regular. Then the polynomial ring $A[x_1, \ldots, x_n]$ has the same property. In particular, every local ring of a polynomial ring over a field is a regular local ring.*

Proof. [**107**, Theorem40] □

Theorem 1.84. *Suppose that R is a regular local ring. Then R is a Cohen-Macaulay normal domain.*

Proof. This follows from [**161**, Corollary 1 on page 302] and [**107**, Theorem 36]. □

The proofs of the following theorems are through homological algebra.

Theorem 1.85. *A Noetherian ring A is normal if and only if it satisfies the following two condtions:*

1) *For every prime ideal $\mathfrak{p} \subset A$ of height 1, $A_\mathfrak{p}$ is regular.*
2) *For every prime ideal $\mathfrak{p} \subset A$ of height ≥ 2, we have $\operatorname{depth} A_\mathfrak{p} \geq 2$.*

Proof. [**107**, Theorem 39, page 125]. □

Corollary 1.86. *Suppose that R is a regular local ring and $f \in R$ is nonzero and is not a unit. Then $R/(f)$ is normal if and only if $(R/(f))_\mathfrak{p}$ is regular for all prime ideals $\mathfrak{p}$ of $R/(f)$ of height 1.*

Proof. Let $A = R/(f)$. We must show that condition 2) of Theorem 1.85 holds. We have that R is a Cohen-Macaulay domain by Theorem 1.84. Since f is R-regular, we have that A_P is Cohen-Macaulay for all prime ideals P of A by [**107**, Theorem 30], and so

$$\operatorname{depth}(A_P) = \dim A_P = \mathrm{ht}(P). \qquad \square$$

Theorem 1.87. *Suppose that R is a normal Noetherian local ring of dimension 1. Then R is a regular local ring.*

Proof. This follows from Theorem 1.85. □

Theorem 1.88. *Suppose that R is a regular local ring and P is a prime ideal in R. Then R_P is a regular local ring.*

Proof. [**107**, Corollary, page 139] or [**106**, Theorem 19.3]. □

Theorem 1.89 (Auslander and Buchsbaum)**.** *Suppose that R is a regular local ring. Then R is a UFD.*

Proof. [**15**] or [**107**, Theorem 48] or [**106**, Theorem 20.3]. □

Chapter 18

Curves

In this chapter we consider the geometry of nonsingular projective curves.

In Sections 18.1–18.3, we prove the Riemann-Roch theorem on a nonsingular projective curve X, Theorem 18.13, which gives a formula for the dimension of the vector space $\Gamma(X, \mathcal{O}_X(D))$ of functions whose poles are bounded by a given divisor D on X in terms of the genus g of X, the degree $\deg D$ of D, and the dimension $h^0(X, \mathcal{O}_X(K_X - D))$, where K_X is a canonical divisor on X. The Riemann-Roch theorem follows from the Riemann-Roch inequality, Theorem 18.2 and Corollary 18.3, proven in Section 18.1 and from Serre duality, Corollary 18.10, proven in Section 18.2.

The Riemann-Roch inequality, Theorem 18.2 and Corollary 18.3, give a lower bound for $h^0(X, \mathcal{O}_X(D))$, which is only in terms of g and $\deg D$ and which is an equality if and only if $h^1(X, \mathcal{O}_X(D)) = 0$. Clifford's theorem, Theorem 18.20, gives an upper bound for $h^0(X, \mathcal{O}_X(D))$ which only depends on $\deg D$ if $h^1(X, \mathcal{O}_X(D)) > 0$.

As a consequence of the Riemann-Roch theorem, we show in Theorem 18.21 that if $\deg D \geq 2g + 1$, then D is very ample and the complete linear system $|D|$ induces a closed embedding of X into a projective space. We deduce in Theorem 18.22 a subdivision of curves by Kodaira dimension: the curves of genus larger than 1, for which K_X is ample; the elliptic curves (genus 1), for which $K_X \sim 0$; and $\mathbb{P}^1$ (genus 0), for which $-K_X$ is ample. The theory of Kodaira dimension generalizes to higher-dimensional varieties [**18**], [**91**], [**112**], [**113**], [**114**], and [**20**].

In Section 18.4, we consider the Riemann-Roch problem, which is the problem of computing the function $h^0(X, \mathcal{O}_X(nD))$ for large n, where X is a nonsingular projective variety and D is a divisor on X.

In Sections 18.5 and Section 18.6, we consider regular maps $f : X \to Y$ of nonsingular projective curves and find formulas relating the genus of X, the genus of Y, and the ramification of f.

We work out the basic geometric theory of elliptic curves in Section 18.7, study the topology of complex curves in Section 18.8, and introduce the theory of Abelian varieties and Jacobians of curves in Section 18.9.

18.1. The Riemann-Roch inequality

Suppose that X is a nonsingular projective curve. The genus of X is

$$g = g(X) = h^0(X, \mathcal{O}_X(K_X)).$$

We have that

$$g(X) = h^1(X, \mathcal{O}_X) \tag{18.1}$$

as follows from Serre duality (Corollary 18.10) which will be established in Section 18.2. Recall the definition of the degree of a divisor on a curve from Section 13.5. If D_1 and D_2 are linearly equivalent divisors on X, then $\deg D_1 = \deg D_2$ by Corollary 13.19.

Lemma 18.1. *Let D be a divisor on X. If $h^0(X, \mathcal{O}_X(D)) > 0$, then* $\deg(D) \geq 0$. *If $h^0(X, \mathcal{O}_X(D)) > 0$ and $\deg D = 0$, then $D \sim 0$.*

Proof. If $h^0(X, \mathcal{O}_X(D)) > 0$, then there exists $0 \neq f \in \Gamma(X, \mathcal{O}_X(D))$. Then $E = (f) + D$ is an effective divisor, so that $\deg E \geq 0$. We have $\deg D = \deg E \geq 0$ by Corollary 13.19. If $\deg D = 0$, then D is linearly equivalent to an effective divisor of degree 0. The only such divisor is 0. □

For a coherent sheaf $\mathcal{F}$ on X, we have

$$\chi(\mathcal{F}) = h^0(X, \mathcal{F}) - h^1(X, \mathcal{F})$$

by Theorem 17.5.

Theorem 18.2. *Let D be a divisor on a nonsingular projective curve X of genus g. Then*

$$\chi(\mathcal{O}_X(D)) = h^0(X, \mathcal{O}_X(D)) - h^1(X, \mathcal{O}_X(D)) = \deg D + 1 - g.$$

Proof. We must show that

$$\chi(\mathcal{O}_X(D)) = \deg D + 1 - g \tag{18.2}$$

for every divisor D on X. The formula is true for $D = 0$ by Theorem 3.35, the definition of genus, and equation (18.1).

Let D be any divisor, and let $p \in X$ be a point. We will show that the formula is true for D if and only if it is true for $D + p$. Since any divisor

on X can be obtained by a finite sequence of addition and subtraction of points, this will establish the formula (18.2) and prove the theorem.

Let $\mathcal{I}(p)$ be the ideal sheaf of the point $p \in X$. Using the fact that $\mathcal{I}(p) = \mathcal{O}_X(-p)$ (a point is a divisor on a curve), we have a short exact sequence of sheaves of $\mathcal{O}_X$-modules

$$0 \to \mathcal{O}_X(-p) \to \mathcal{O}_X \to \mathcal{O}_X/\mathcal{I}(p) \to 0.$$

Now tensor with $\mathcal{O}_X(D+p)$ to get a short exact sequence

$$0 \to \mathcal{O}_X(D) \to \mathcal{O}_X(D+p) \to \mathcal{O}_X/\mathcal{I}(p) \to 0. \tag{18.3}$$

The sequence is short exact since $\mathcal{O}_X(D+p)$ is a locally free (and thus flat) $\mathcal{O}_X$-module (in fact, locally, this is just like tensoring with $\mathcal{O}_X$). The support of $\mathcal{O}_X/\mathcal{I}(p)$ is just the point p, so that $(\mathcal{O}_X/\mathcal{I}(p)) \otimes_{\mathcal{O}_X} \mathcal{O}_X(D+p) \cong \mathcal{O}_X/\mathcal{I}(p)$. Taking the long exact cohomology sequence associated to (18.3) and using Corollary 17.6, we get an exact sequence

$$\begin{aligned} 0 \to H^0(X, \mathcal{O}_X(D)) \to H^0(X, \mathcal{O}_X(D+p)) \to H^0(X, \mathcal{O}_X/\mathcal{I}(p)) \cong k \\ \to H^1(X, \mathcal{O}_X(D)) \to H^1(X, \mathcal{O}_X(D+p)) \to H^1(X, \mathcal{O}_X/\mathcal{I}(p)) = 0. \end{aligned}$$

Thus

$$\chi(\mathcal{O}_X(D+p)) = \chi(\mathcal{O}_X(D)) + 1.$$

Since $\deg(D+p) = \deg(D) + 1$, we obtain the formula (18.2). □

Corollary 18.3 (The Riemann-Roch inequality)**.** *Suppose that D is a divisor on a nonsingular projective curve X of genus g. Then*

$$h^0(X, \mathcal{O}_X(D)) \geq \deg(D) + 1 - g.$$

18.2. Serre duality

The proof in this section follows Serre [**134**].

We continue to assume that X is a nonsingular projective curve. For a divisor $D = \sum a_i p_i$ on X where p_i are distinct points of X and $a_i \in \mathbb{Z}$, we define for a point $q \in X$

$$\nu_q(D) = \begin{cases} a_i & \text{if } q = p_i, \\ 0 & \text{if } q \neq p_i \text{ for all } i. \end{cases}$$

A répartition r is a family $\{r_p\}_{p \in X}$ of elements of $k(X)$ such that $r_p \in \mathcal{O}_{X,p}$ for all but finitely many $p \in X$. The set of all répartitions is an algebra R over k. Suppose that D is a divisor on X. Then define $R(D)$ to be the k-subspace of R consisting of all $r = \{r_p\}$ such that $\nu_p(r_p) \geq -\nu_p(D)$ for all $p \in X$.

To every $f \in k(X)$, we associate the répartition $\{r_p\}$ such that $r_p = f$ for every $p \in X$, giving an injection of $k(X)$ into R. We may then view $k(X)$ as a subring of R.

Proposition 18.4. *Suppose that D is a divisor on X. Then the k-vector space $I(D) = H^1(X, \mathcal{O}_X(D))$ is canonically isomorphic to $R/(R(D)+k(X))$.*

Proof. For $p \in X$ and $r \in R$, let $[r_p]$ be the class of r_p in $k(X)/\mathcal{O}_X(D)_p$. Define a k-vector space homomorphism $\Lambda : R \to \bigoplus_{p\in X} k(X)/\mathcal{O}_X(D)_p$ by $r \mapsto \{[r_p]\}$. Here Λ is well-defined since $r_p \in \mathcal{O}_X(D)_p$ for all but finitely many $p \in X$. We have that $\Lambda(r) = 0$ if and only if $r_p \in \mathcal{O}_X(D)_p$ for all $p \in X$ which holds if and only if $\nu_p(r_p) \geq -\nu_p(D)$ for all $p \in X$. Thus Λ induces an isomorphism

$$R/R(D) \cong \bigoplus_{p\in X} k(X)/\mathcal{O}_X(D)_p. \tag{18.4}$$

Let $\mathcal{A}$ be the sheaf $k(X)/\mathcal{O}_X(D)$. By Lemma 17.15, we have natural exact sequences

$$0 \to \Gamma(V, \mathcal{O}_X(D)) \to \Gamma(V, k(X)) = k(X) \to \Gamma(V, \mathcal{A})$$

for all open subsets V of X.

Suppose that U is a neighborhood of a point $p \in X$ and $s \in \mathcal{A}(U)$. There exists $t \in k(X)$ such that the image of t in $\mathcal{A}_p$ is equal to s_p. Let t' be the image of t in $\mathcal{A}(U)$. Then the germ of $s - t'$ in $\mathcal{A}_p$ is zero. Since $\mathcal{A}_p$ is the limit of $\mathcal{A}(V)$ over open sets V containing p, we have that there exists an open neighborhood V of p in U such that the restriction of $s - t'$ in $\mathcal{A}(V)$ is zero.

Then replacing U with V and s with its restriction to V, we have that s is the class of $t \in k(X)$, which is necessarily in $\mathcal{O}_X(D)_q$ for all but finitely many $q \in U$. Thus there exists a neighborhood U' of p such that $s = 0$ on $U' \setminus \{p\}$. In particular, every $s \in H^0(X, \mathcal{A})$ has finite support, so

$$\Phi : H^0(X, \mathcal{A}) \to \bigoplus_{p\in X} \mathcal{A}_p \tag{18.5}$$

defined by $s \mapsto \{s_p\}$ is a well-defined homomorphism. By the sheaf axioms, every element $\{\alpha_p\} \in \bigoplus \mathcal{A}_p$ lifts to a section of $H^0(X, \mathcal{A})$, and the kernel of Φ is zero. Thus Φ is an isomorphism.

We have that $\mathcal{A}_p = k(X)/\mathcal{O}_X(D)_p$ for $p \in X$ so (18.4) and (18.5) give us an isomorphism

$$R/R(D) \cong H^0(X, \mathcal{A}). \tag{18.6}$$

The sheaf $\mathcal{O}_X(D)$ is a subsheaf of the constant sheaf $k(X)$, so there is an exact sequence

$$0 \to \mathcal{O}_X(D) \to k(X) \to k(X)/\mathcal{O}_X(D) \to 0.$$

By Lemma 17.15, we have that $H^0(X, k(X)) = k(X)$ and $H^1(X, k(X)) = 0$ so we have an exact sequence of cohomology modules

$$k(X) \to H^0(X, \mathcal{A}) \to H^1(X, \mathcal{O}_X(D)) \to 0.$$

Now using the isomorphism (18.6), we have the desired isomorphism

$$H^1(X, \mathcal{O}_X(D)) \cong R/(R(D) + k(X)). \qquad \square$$

From now on, we identify $H^1(X, \mathcal{O}_X(D))$ and $R/(R(D) + k(X))$ which we will denote by $I(D)$.

Let $J(D)$ be the dual of the k-vector space $I(D) = R/(R(D) + k(X))$. An element of $J(D)$ is thus a linear form on R which vanishes on $k(X)$ and $R(D)$. Suppose that $D' \geq D$. Then $R(D') \supset R(D)$ so that $J(D) \supset J(D')$. The union of the $J(D)$ for D running through the divisors of X will be denoted by J.

Let $f \in k(X)$ and $\alpha \in J$. The map $r \mapsto \alpha(fr)$ is a linear form on R vanishing on $k(X)$, which we will denote by $f\alpha$. If $\alpha \in J$, then $f\alpha \in J$. This follows since if $\alpha \in J(D)$ and $f \in \Gamma(X, \mathcal{O}_X(\Delta))$, then the linear form $f\alpha$ vanishes on $R(D - \Delta)$ and thus belongs to $J(D - \Delta)$. The operator $(f, \alpha) \mapsto f\alpha$ gives J the structure of a vector space over $k(X)$.

Proposition 18.5. *The dimension of J as a $k(X)$-vector space is ≤ 1.*

Proof. Suppose that $\alpha, \alpha' \in J$ are linearly independent over $k(X)$. There exists a divisor D such that $\alpha \in J(D)$ and $\alpha' \in J(D)$. Let $d = \deg(D)$. For every integer $n \geq 0$, let Δ_n be a divisor of degree n (for example, $\Delta_n = np$, where p is a fixed point of X).

Suppose that $f, g \in \Gamma(X, \mathcal{O}_X(\Delta_n))$. Then $f\alpha, g\alpha' \in J(D - \Delta_n)$. Since α, α' are linearly independent over $k(X)$, any relation $f\alpha + g\alpha' = 0$ implies $f = g = 0$. Thus the map $(f, g) \mapsto f\alpha + g\alpha'$ is an injective k-vector space homomorphism

$$\Gamma(X, \mathcal{O}_X(\Delta_n)) \oplus \Gamma(X, \mathcal{O}_X(\Delta_n)) \to J(D - \Delta_n),$$

so we have the inequality

$$\dim_k J(D - \Delta_n) \geq 2 \dim_k \Gamma(X, \mathcal{O}_X(\Delta_n)) \tag{18.7}$$

for all n. We will now show that (18.7) leads to a contradiction as $n \to \infty$. The left-hand side is

$$\begin{aligned} \dim_k I(D - \Delta_n) &= h^1(X, \mathcal{O}_X(D - \Delta_n)) \\ &= -\deg(D - \Delta_n) + g - 1 + h^0(X, \mathcal{O}_X(D - \Delta_n)) \\ &= n + (g - 1 - d) + h^0(D, \mathcal{O}_X(D - \Delta_n)) \end{aligned}$$

by Theorem 18.2.

When $n > d$, $\deg(D-\Delta_n) < 0$ so that $h^0(X, \mathcal{O}_X(D-\Delta_n)) = 0$ by Lemma 18.1. Thus for large n, the left-hand side of (18.7) is equal to $n + A_0$, A_0 a constant. The right-hand side of (18.7) is equal to $2h^0(X, \mathcal{O}_X(\Delta_n))$. By Theorem 18.2,

$$h^0(X, \mathcal{O}_X(\Delta_n)) \geq \deg(\Delta_n) + 1 - g = n + 1 - g.$$

Thus the right-hand side of (18.7) is $\geq 2n + A_1$ for some constant A_1, giving a contradiction for large n. □

The sheaf $\Omega_{X/k}$ is a subsheaf of $\Omega_{k(X)/k}$. If $p \in X$ and t is a regular parameter in $\mathcal{O}_{X,p}$, then $\Omega_{X/k,p} = \mathcal{O}_{X,p}dt$ by Proposition 14.15. We further have that $\Omega_{k(X)/k} = k(X)dt$. We define $\nu_p(\omega) = \nu_p(f)$ if $\omega = f dt \in k(X)dt$. Recall (Section 14.3) that the divisor (ω) of $\omega \in \Omega_{k(X)/k}$ is

$$(\omega) = \sum_{p \in X} \nu_p(\omega) p.$$

Thus $\nu_p(\omega) = \nu_p(K)$ where $(\omega) = K$ is the divisor of ω. The quotient field of $\hat{\mathcal{O}}_{X,p} = k[[t]]$ (Proposition 21.41) is the field of Laurent series $k((t))$. Identifying f with its image in $k((t))$ by the inclusion $k(X) \to k((t))$ induced by the inclusion $\mathcal{O}_{X,p} \to k[[t]]$, we have an expression

$$f = \sum_{n \gg -\infty} a_n t^n$$

with all $a_n \in k$ ($n \gg -\infty$ in the summation means that $a_n = 0$ for $n \ll 0$). The coefficient a_{-1} of t^{-1} in f is called the residue of $\omega = f dt$ at p, denoted by $\mathrm{Res}_p(\omega)$. The following proposition shows that the definition is well-defined.

Proposition 18.6 (Invariance of the residue)**.** *The preceding definition is independent of the choice of regular parameter t in $\mathcal{O}_{X,p}$.*

Proposition 18.6 is proven in [**134**, Section 11 of Chapter II].

Proposition 18.7 (Residue formula)**.** *For every $\omega \in \Omega_{k(X)/k}$,*

$$\sum_{p \in X} \mathrm{Res}_p(\omega) = 0.$$

Proposition 18.7 is proven in [**134**, Sections 12 and 13 of Chapter II]. The proof is by taking a projection to $\mathbb{P}^1$ and showing that it reduces to verifying the formula for $\mathbb{P}^1$.

Given a divisor D on X, let $\Omega_{X/k}(D)$ be the subsheaf of $\Omega_{k(X)/k}$ defined by

$$\Gamma(U, \Omega_{X/k}(D)) = \{\omega \in \Omega_{k(X)/k} \mid (\omega) \cap U \geq D \cap U\}$$

for U an open subset of X.

Let ω_0 be a nonzero rational differential form, and let $K = (\omega_0)$. Every rational differential form ω can be written as $\omega = f\omega_0$ for some $f \in k(X)$ and $(\omega) \cap U \geq D \cap U$ if and only if $(f) \cap U + (\omega_0) \cap U \geq D \cap U$, which holds if and only if $f \in \Gamma(U, \mathcal{O}_X(K - D))$. Thus

$$\Omega_{X/k}(D) \cong \Omega_X(K - D) \cong \Omega_{X/k} \otimes \mathcal{O}_X(-D).$$

Let $\Omega(D) = \Gamma(X, \Omega_{X/k}(D))$.

We define a product $\langle \omega, \ \rangle$ of differentials $\omega \in \Omega_{k(X)/k}$ and répartitions $r \in R$ by the following formula:

$$\langle \omega, r \rangle = \sum_{p \in X} \mathrm{Res}_p(r_p \omega).$$

This formula is well-defined since $r_p\omega \in (\Omega_{X/k})_p$ for all but finitely many $p \in X$. The product has the following properties:

a) $\langle \omega, r \rangle = 0$ if $r \in k(X)$.

b) $\langle \omega, r \rangle = 0$ if $r \in R(D)$ and $\omega \in \Omega(D)$.

c) If $f \in k(X)$, then $\langle f\omega, r \rangle = \langle \omega, fr \rangle$.

Property a) follows from the residue formula (Proposition 18.7) and property b) follows since then $r_p\omega \in (\Omega_{X/k})_p$ for all $p \in X$.

For every $\omega \in \Omega_{k(X)/k}$, let $\theta(\omega)$ be the linear form on R defined by

$$\theta(\omega)(r) = \langle \omega, r \rangle.$$

If $\omega \in \Omega(D)$, then $\theta(\omega) \in J(D)$ by properties a) and b) since $J(D)$ is the dual of $R/(R(D) + k(X))$.

Lemma 18.8. *Suppose that $\omega \in \Omega_{k(X)/k}$ is such that $\theta(\omega) \in J(D)$. Then $\omega \in \Omega(D)$.*

Proof. Suppose that $\omega \notin \Omega(D)$. Then there is a point $p \in X$ such that $\nu_p(\omega) < \nu_p(D)$. Set $n = \nu_p(\omega) + 1$, and let r be the répartition defined by

$$r_q = \begin{cases} 0 & \text{if } q \neq p, \\ \frac{1}{t^n} & \text{where } t \text{ is a regular parameter at } p \text{ if } q = p. \end{cases}$$

We have $\nu_p(r_p\omega) = -1$ so that $\mathrm{Res}_p(r_p\omega) \neq 0$ and $\langle \omega, r \rangle \neq 0$. But $n \leq \nu_p(D)$ so $r \in R(D)$ ($\nu_q(0) = \infty$). This is a contradiction since $\theta(\omega)$ is assumed to vanish on $R(D)$. □

Theorem 18.9 (Serre duality)**.** *For every divisor D, the map θ is a k-vector space isomorphism from $\Omega(D)$ to $J(D)$.*

Proof. Suppose that $\omega \in \Omega(D)$ is such that $\theta(\omega) = 0$ in $J(D)$. Then $\theta(\omega) \in J(\Delta)$ for all divisors Δ so $\omega \in \Omega(\Delta)$ for all divisors Δ by Lemma 18.8 so that $\omega = 0$. Hence θ is injective.

By property c), θ is a $k(X)$-linear map from $\Omega_{k(X)/k}$ to J. As $\Omega_{k(X)/k}$ has dimension 1 and J has dimension ≤ 1 as $k(X)$-vector spaces by Proposition 18.5, θ maps $\Omega_{k(X)/k}$ onto J. Thus if $\alpha \in J(D)$, there exists $\omega \in \Omega_{k(X)/k}$ such that $\theta(\omega) = \alpha$ and Lemma 18.8 then shows that $\omega \in \Omega(D)$. □

Corollary 18.10. *Suppose that D is a divisor on X. Then*

$$h^1(X, \mathcal{O}_X(D)) = h^0(X, \mathcal{O}_X(K_X - D))$$

where K_X is a canonical divisor of X.

Exercise 18.11. Prove the residue formula of Proposition 18.7 for $X = \mathbb{P}^1$.

Exercise 18.12. Strengthen the conclusions of Proposition 18.5 to show that $\dim_{k(X)} J = 1$.

18.3. The Riemann-Roch theorem

Theorem 18.13 (Riemann-Roch theorem)**.** *Let D be a divisor on a nonsingular projective curve X of genus g. Then*

$$h^0(X, \mathcal{O}_X(D)) = h^0(X, \mathcal{O}_X(K_X - D)) + \deg D + 1 - g.$$

Proof. The theorem follows from Theorem 18.2 and Serre duality (Corollary 18.10). □

Corollary 18.14. *Suppose that X is a nonsingular projective curve of genus g. Then the degree of the canonical divisor is* $\deg K_X = 2g - 2$.

Proof. Take $D = K_X$ in the Riemann-Roch theorem. □

Corollary 18.15. *Suppose that D is a divisor on a nonsingular projective curve X of genus g such that* $\deg D > 2g - 2$. *Then*

$$h^0(X, \mathcal{O}_X(D)) = \deg D + 1 - g.$$

Proof. Since $\deg(K_X - D) < 0$, we have that $h^0(X, \mathcal{O}_X(K_X - D)) = 0$ by Lemma 18.1. □

Corollary 18.16. *Suppose that D is a divisor on a nonsingular projective curve X of genus g such that* $\deg(D) > 0$. *Then*

$$h^0(X, \mathcal{O}_X(nD)) = n \deg(D) + 1 - g$$

for $n > \frac{2g-2}{\deg(D)}$.

Theorem 18.17. *Suppose that X is a nonsingular projective curve. Then $X \cong \mathbb{P}^1$ if and only if $g(X) = 0$.*

Proof. Theorem 17.14 implies that $g(\mathbb{P}^1) = h^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}) = 0$. Suppose $g(X) = 0$ and $p \in X$ is a point. Then $h^0(X, \mathcal{O}_X(p)) = 2$ by the Riemann-Roch theorem (Theorem 18.13), Corollary 18.14, and Lemma 18.1. Now the complete linear system $|p|$ consists of effective divisors of degree equal to $1 = \deg p$ by Corollary 13.19 and so $X \cong \mathbb{P}^1$ by Corollary 13.20. □

A nonsingular projective curve X is called an elliptic curve if $g(X) = 1$.

Corollary 18.18. *A nonsingular projective curve X is an elliptic curve if and only if $K_X \sim 0$.*

Proof. If $g(X) = 1$, then $\deg K_X = 0$ by Corollary 18.14. Since

$$h^0(X, \mathcal{O}_X(K_X)) = 1,$$

we have $K_X \sim 0$ by Lemma 18.1.

If $K_X \sim 0$, then $g = 1$ by Corollary 18.14 □

Theorem 18.19. *Suppose that X is an elliptic curve and $p_0 \in X$ is a point. Then the map $X \to \mathrm{Cl}^0(X)$ defined by $p \mapsto [p - p_0]$ is a bijection.*

Proof. Suppose that D is a divisor of degree 0 on X. Then

$$h^0(X, \mathcal{O}_X(K_X - D - p_0)) = 0$$

since $\deg(K_X - D - p_0) = -1$. By the Riemann-Roch theorem, we then have that

$$h^0(X, \mathcal{O}_X(D + p_0)) = 1.$$

Thus there is a unique effective divisor linearly equivalent to $D + p_0$ which must be a single point p, since $\deg(D + p_0) = 1$. In particular, there exists a unique point $p \in X$ such that $p - p_0 \sim D$ from which the theorem follows. □

If D is a divisor on a nonsingular projective curve X and

$$h^1(X, \mathcal{O}_X(D)) = 0,$$

then the Riemann-Roch theorem gives the dimension of $h^0(X, \mathcal{O}_X(D))$ but only gives a lower bound if $h^1(X, \mathcal{O}_X(D)) \neq 0$. The following theorem gives an upper bound for $h^0(X, \mathcal{O}_X(D))$ when D is effective and $h^1(X, \mathcal{O}_X(D)) \neq 0$. The bound is sharp, and in fact the curves X and divisors D for which the upper bound is achieved are extremely special and are completely characterized (this is part of Clifford's original theorem). A proof of this characterization is given in [**73**, Theorem IV.5.4].

Theorem 18.20 (Clifford's theorem)**.** *Suppose that D is a divisor on a nonsingular projective curve X such that*

$$h^0(X, \mathcal{O}_X(D)) > 0 \quad \textit{and} \quad h^1(X, \mathcal{O}_X(D)) > 0.$$

Then

$$h^0(X, \mathcal{O}_X(D)) \leq \frac{1}{2}\deg(D) + 1.$$

Proof. Let $g = g(x)$. After possibly replacing D with a divisor linearly equivalent to D and K_X with a divisor linearly equivalent to K_X, we may assume that $D \geq 0$ and $D' = K_X - D \geq 0$. Further, we may assume that $h^0(X, \mathcal{O}_X(D-p)) \neq h^0(X, \mathcal{O}_X(D))$ for all $p \in X$ since otherwise we can replace D with $D - p$ and get a stronger inequality. We can then choose

$$g \in \Gamma(X, \mathcal{O}_X(D)) = \{f \in k(X) \mid (f) + D \geq 0\}$$

such that $g \notin \Gamma(X, \mathcal{O}_X(D-p))$ for all $p \in \mathrm{Supp}(D')$.

Consider the k-linear map

$$\phi : \Gamma(X, \mathcal{O}_X(D'))/\Gamma(X, \mathcal{O}_X) \to \Gamma(X, \mathcal{O}_X(K_X))/\Gamma(X, \mathcal{O}_X(D))$$

defined by $\phi(\overline{f}) = \overline{fg}$, where bar denotes residue. The map ϕ is well-defined, since for $f \in \Gamma(X, \mathcal{O}_X(D'))$, $(fg) \geq -D - D' = -K_X$ and since

$$k = \Gamma(X, \mathcal{O}_X) = \{f \in k(X) \mid (f) \geq 0\}$$

by Theorem 3.35 and Lemma 13.3, so we have that $(gf) + D \geq 0$ if $f \in \Gamma(X, \mathcal{O}_X)$.

Suppose $\phi(\overline{f}) = 0$ for some $f \in \Gamma(X, \mathcal{O}_X(D'))$. Then $(f) + D' \geq 0$ so if $p \notin \mathrm{Supp}(D')$, then $\nu_p(f) \geq 0$. Suppose $p \in \mathrm{Supp}(D')$. Then $\nu_p(g) = -\nu_p(D)$ by our choice of g. Since $(gf) + D \geq 0$, we have $\nu_p(fg) \geq -\nu_p(D)$ and so

$$\nu_p(f) \geq -\nu_p(D) - \nu_p(g) = 0.$$

Thus $\nu_p(f) \geq 0$ for all $p \in X$ and so $f \in \Gamma(X, \mathcal{O}_X)$ and we have that ϕ is injective. Thus

$$h^0(X, \mathcal{O}_X(D')) - 1 \leq g - h^0(X, \mathcal{O}_X(D)). \tag{18.8}$$

By the Riemann-Roch theorem,

$$\begin{aligned} h^0(X, \mathcal{O}_X(D')) &= \deg(D') + 1 - g + h^0(X, \mathcal{O}_X(K_X - D')) \\ &= g - 1 - \deg(D) + h^0(X, \mathcal{O}_X(D)) \end{aligned} \tag{18.9}$$

since

$$2g - 2 = \deg K_X = \deg D + \deg D'.$$

Combining equations (18.8) and (18.9), we obtain the conclusions of the theorem. □

Theorem 18.21. *Let D be a divisor on a nonsingular projective curve X of genus g. Then:*

1) *If $\deg D \geq 2g$, then $|D|$ is base point free.*
2) *If $\deg D \geq 2g+1$, then D is very ample, so that the regular map*

$$\phi_{|D|} : X \to \mathbb{P}^{h^0(X,\mathcal{O}_X(D))}$$

is a closed embedding.

Proof. Conclusion 1) of this theorem follows from Corollary 18.15, which tells us that

$$h^0(X, \mathcal{O}_X(D-p)) = h^0(X, \mathcal{O}_X(D)) - 1$$

for all $p \in X$, and 1) of Corollary 13.34. Conclusion 2) follows from Corollary 18.15, which shows that

$$h^0(X, \mathcal{O}_X(D-p-q)) = h^0(X, \mathcal{O}_X(D)) - 2$$

for all $p, q \in X$, and 3) of Corollary 13.34. □

Theorem 18.22. *Suppose that X is a nonsingular projective curve. Then K_X is ample if $g(X) > 1$, $K_X \sim 0$ if X is an elliptic curve ($g(X) = 1$), and $-K_X$ is ample if $X \cong \mathbb{P}^1$ ($g(X) = 0$).*

Proof. This follows from Corollary 18.14, Theorem 18.21, Theorem 18.17, and Corollary 18.18. □

Theorem 18.22 generalizes to the theory of Kodaira dimension for higher-dimensional varieties. This is especially worked out in the classification of surfaces [**18**]. Some papers on the theory in higher dimensions are [**91**], [**112**], [**113**], [**114**], and [**20**].

18.4. The Riemann-Roch problem on varieties

From Theorems 18.21, 17.18, and 17.35 we obtain the following theorem.

Theorem 18.23. *Suppose that D is a divisor on a nonsingular projective curve X such that $\deg D > 0$. Then*

$$R[D] = \bigoplus_{n \geq 0} \Gamma(X, \mathcal{O}_X(nD))$$

is a finitely generated k-algebra.

Thus Corollary 18.16 is not so surprising, since $h^0(X, \mathcal{O}_X(nD))$ is the Hilbert function of $R[D]$. However, it may be that $R[D]$ is not generated in degree 1, so just knowing that $R[D]$ is a finitely generated k-algebra is not enough to conclude that its Hilbert function is eventually a polynomial. We do have that the Hilbert function of a finitely generated graded k-algebra is

eventually a quasi-polynomial, which has an expression $P(n) = a_d(n)n^d + a_{d-1}(n)n^{d-1} + \cdots + a_0(n)$ where the coefficients $a_i(n)$ are periodic functions.

The Riemann-Roch problem is to compute the function

$$P_D(n) = h^0(X, \mathcal{O}_X(nD))$$

for large n where D is a divisor on a nonsingular projective variety X.

It will follow from Theorem 19.1 that $\chi(\mathcal{O}_X(nD))$ is a polynomial in n. Thus if D is ample, we have that $P_D(n)$ is a polynomial for $n \gg 0$, as $P_D(n) = \chi(\mathcal{O}_X(nD))$ for $n \gg 0$ by Theorem 17.18.

If D is a divisor of degree 0 on a nonsingular projective curve X, then $h^0(X, \mathcal{O}_X(nD)) > 0$ if and only if $nD \sim 0$ by Lemma 18.1. We thus have the following complete solution to the Riemann-Roch problem on a curve.

Theorem 18.24. *Suppose that X is a nonsingular projective curve and D is a divisor on X. Then for $n \gg 0$,*

$$h^0(X, \mathcal{O}_X(nD)) = \begin{cases} n \deg D + 1 - g(X) & \text{if } \deg D > 0, \\ \text{a periodic function in } n & \text{if } \deg D = 0, \\ 0 & \text{if } \deg D < 0. \end{cases}$$

There are examples of effective divisors D on a nonsingular projective surface S such that $R[D] = \bigoplus_{n \geq 0} \Gamma(X, \mathcal{O}_X(nD))$ is not a finitely generated k-algebra. This was shown by Zariski in [**159**]; we will construct Zariski's example in Theorem 20.14. It may thus be expected that (the sometimes not finitely generated k-algebra) $R = \bigoplus_{n \geq 0} \Gamma(S, \mathcal{O}_S(nD))$ will not always have a good Hilbert function, that is, that $h^0(S, \mathcal{O}_S(nD))$ will not be polynomial-like. However, Zariski showed in [**159**] that this function is almost a polynomial on a surface.

Theorem 18.25 (Zariski)**.** *Let D be an effective divisor on a nonsingular projective surface S over an algebraically closed field k. Then there exists a quadratic polynomial $P(n)$ and a bounded function $\lambda(n)$ such that*

$$h^0(S, \mathcal{O}_S(nD)) = P(n) + \lambda(n).$$

for $n \geq 0$.

In this same paper, Zariski asked if $\lambda(n)$ is always eventually a periodic function of n (a periodic function in n for $n \gg 0$). This question is answered in [**44**].

Theorem 18.26. *Let D be an effective divisor on a nonsingular projective surface S. Let $\lambda(n)$ be the function of Theorem* 18.25*. Then:*

1. *If k has characteristic* 0 *or is the algebraic closure of a finite field, then $\lambda(n)$ is eventually a periodic function.*
2. *There are examples where $\lambda(n)$ is not eventually periodic if k is of positive characteristic and is not the algebraic closure of a finite field.*

Proof. Cutkosky and Srinivas [**44**, Theorems 2 and 3 and Example 3]. □

While the function $h^0(X, \mathcal{O}_X(nD))$ is almost a polynomial function when X is a surface, the behavior of the function $h^0(X, \mathcal{O}_X(nD))$ in higher dimensions can be much more complicated.

Example 18.27. Over any algebraically closed field k, there exists a nonsingular projective 3-fold X and an effective divisor D on X such that

$$\lim_{n\to\infty} \frac{h^0(X, \mathcal{O}_X(nD))}{n^3}$$

is an irrational number. In particular, $h^0(X, \mathcal{O}_X(nD))$ is not eventually a polynomial-like function.

Proof. Cutkosky and Srinivas [**44**, Example 4]. □

The volume of an invertible sheaf $\mathcal{L}$ on a d-dimensional projective variety X is defined as

$$\mathrm{Vol}(\mathcal{L}) = \lim_{n\to\infty} \sup \frac{h^0(X, \mathcal{L}^n)}{n^d/d!}.$$

The volume always exists as a limit over an algebraically closed field k (by Lazarsfeld [**98**] and Lazarsfeld and Mustaţă [**99**]) and over an arbitrary field (by Cutkosky [**42**]) but can be an irrational number (by Example 18.27).

Exercise 18.28. Find an example of a divisor D on a nonsingular projective curve such that $|D|$ is not base point free but $|n_0 D|$ is base point free for some positive multiple n_0.

Exercise 18.29. Give an example of a finitely generated graded k-algebra such that its Hilbert function is not eventually a polynomial.

18.5. The Hurwitz theorem

Suppose that $\phi : X \to Y$ is a dominant regular map of nonsingular projective curves. Recall that ϕ is then finite (Corollary 10.26). Suppose that $P \in X$.

The ramification index e_P of ϕ at P is defined as follows. Let $Q = \phi(P)$. Recall that the valuation ν_Q is a valuation of $k(Y)$ whose valuation ring is

$\mathcal{O}_{Y,Q}$ and ν_P is a valuation of $k(X)$ whose valuation ring is $\mathcal{O}_{X,P}$. Thus ν_P is an extension of ν_Q to $k(X)$. Let x be a regular parameter in $\mathcal{O}_{X,P}$ and y be a regular parameter in $\mathcal{O}_{Y,Q}$. Then

$$y = ux^{e_P}$$

for some unit $u \in \mathcal{O}_{X,P}$ and positive integer e_P. The number e_P is called the ramification index of ν_P over ν_Q or the ramification index of P over Q.

Since $y = 0$ is a local equation for the divisor Q on Y, we have that

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_P P,$$

and by Theorem 13.18,

$$\sum_{P \in \phi^{-1}(Q)} e_P = \deg(\phi^*(Q)) = \deg(\phi) = [k(X) : k(Y)]$$

does not depend on Q.

We will say that ϕ is ramified at P if $e_P > 1$, tamely ramified at P if the characteristic p of k does not divide e_P, and wildly ramified at P if p divides e_P. We can then consider the set of all ramification points of ϕ in X.

We will say that a dominant regular map $\phi : X \to Y$ of varieties is separable if the induced extension of fields $k(Y) \to k(X)$ is finite and separable.

Proposition 18.30. *Suppose that $\phi : X \to Y$ is a finite regular map of nonsingular curves and that ϕ is separable. Then there is an exact sequence of $\mathcal{O}_X$-modules*

$$0 \to \phi^*\Omega_{Y/k} \to \Omega_{X/k} \to \Omega_{X/Y} \to 0. \tag{18.10}$$

Proof. By formula (14.4), the sequence (18.10) is right exact, so we need only show that the map

$$\phi^*\Omega_{Y/k} \to \Omega_{X/k} \tag{18.11}$$

is injective. Since $\phi^*\Omega_{Y/k}$ and $\Omega_{X/k}$ are invertible sheaves of $\mathcal{O}_X$-modules, we need only show that the map (18.11) is nonzero. Tensoring over $\mathcal{O}_X$ with $k(X)$, we reduce by Lemma 14.8 to showing that the natural map $\Omega_{k(Y)/k} \otimes_{k(Y)} k(X) \to \Omega_{k(X)/k}$ is nonzero, which will follow if the natural map

$$\Omega_{k(Y)/k} \to \Omega_{k(X)/k} \tag{18.12}$$

is nonzero. The field $k(Y)$ is separably generated over the algebraically closed field k (by Theorem 1.14). Let $z \in k(Y)$ be a transcendental element over k such that $k(Y)$ is separable over $k(z)$. Then $k(X)$ is separable over

$k(z)$, so z is also a separable transcendence basis of $k(X)$ over k. By Theorem 21.75, $d_{K(Y)/k}(z)$ is a generator of $\Omega_{k(Y)/k}$ and $d_{k(X)/k}(z)$ is a generator of $\Omega_{k(X)/k}$. Thus (18.12) is an injection, and $\Omega_{k(Y)/k} \otimes_{k(Y)} k(X) \to \Omega_{k(X)/k}$ is nonzero. □

Suppose that $P \in X$. Let $Q = \phi(P)$. Let x be a regular parameter in $\mathcal{O}_{X,P}$ and y be a regular parameter in $\mathcal{O}_{Y,Q}$. Taking stalks at P in (18.10) gives us (by Proposition 14.15) the short exact sequence

$$0 \to \mathcal{O}_{X,P}dy \to \mathcal{O}_{X,P}dx \to (\Omega_{X/Y})_P \to 0. \tag{18.13}$$

We define

$$\frac{dy}{dx} \in \mathcal{O}_{X,P}$$

by

$$dy = \frac{dy}{dx}dx.$$

We have that $y = ux^{e_P}$ where u is a unit in $\mathcal{O}_{X,P}$. Since d is a derivation, we have that

$$dy = e_P u x^{e_P - 1}dx + x^{e_P}du.$$

Now $du = adx$ for some $a \in \mathcal{O}_{X,P}$, so $dy = (e_p u x^{e_p - 1} + ax^{e_p})dx$. We thus obtain the following proposition.

Proposition 18.31. *Let $\phi : X \to Y$ be a separable finite regular map of nonsingular curves. Then:*

1. *The support of $\Omega_{X/Y}$ is the finite set of ramification points of ϕ in X.*
2. *For each $P \in X$, $(\Omega_{X/Y})_P$ is a cyclic $\mathcal{O}_{X,P}$-module (generated by one element) of k-dimension equal to $\nu_P(\frac{dy}{dx})$.*
3. *If ϕ is tamely ramified at P, then*
$$\dim_k(\Omega_{X/Y})_P = e_P - 1.$$
4. *If ϕ is wildly ramified at P, then*
$$\dim_k(\Omega_{X/Y})_P > e_P - 1.$$

Let $\mathcal{D}_{X/Y}$ be the ideal sheaf in $\mathcal{O}_X$ which is the annihilator of $\Omega_{X/Y}$. Let R be the effective divisor such that $\mathcal{D}_{X/Y} = \mathcal{O}_X(-R)$. We then have that $\mathcal{D}_{X/Y}$ is the annihilator of $\Omega_{X/Y} \otimes \Omega_{X/k}^{-1}$. Tensoring (18.10) with the invertible sheaf $\Omega_{X/k}^{-1}$, we obtain the short exact sequence

$$0 \to \phi^*\Omega_{Y/k} \otimes \Omega_{X/k}^{-1} \to \mathcal{O}_X \to \Omega_{X/Y} \otimes \Omega_{X/k}^{-1} \to 0$$

so that

$$\phi^*\Omega_{Y/k} \otimes \Omega_{X/k}^{-1} \cong \mathcal{O}_X(-R)$$

and

$$\mathcal{O}_R = \mathcal{O}_R/\mathcal{O}_X(-R) \cong \Omega_{X/Y} \otimes \Omega_{X/k}^{-1} \cong \Omega_{X/Y}$$

since $\Omega_{X/Y}$ has finite support. Thus

$$R = \sum_{p \in X} \dim_k(\Omega_{X/Y})_P P. \tag{18.14}$$

Taking degrees of divisors in

$$\mathcal{O}_X(-R) \cong \phi^*\Omega_{Y/k} \otimes \Omega_{X/k}^{-1} \cong \mathcal{O}_X(\phi^*(K_Y) - K_X),$$

we have that

$$\begin{aligned} \deg R &= \deg K_X - \deg \phi^*(K_Y) \\ &= \deg K_X - \deg(\phi) \deg K_Y \\ &= (2g(X) - 2) - \deg(\phi)(2g(Y) - 2) \end{aligned}$$

by Theorem 13.18 and Corollary 18.14. We thus have the following theorem.

Theorem 18.32 (Hurwitz)**.** *Let $\phi : X \to Y$ be a dominant separable regular map of nonsingular projective curves. Then*

$$2g(X) - 2 = \deg(\phi)(2g(Y) - 2) + \deg(R),$$

where R is the ramification divisor (18.14)*. If ϕ has only tame ramification, then*

$$\deg(R) = \sum_{P \in X} (e_P - 1).$$

In the case that X and Y are affine, with coordinate rings $A = k[Y]$ and $B = k[X]$, the annihilator $\Gamma(X, \mathcal{D}_{X/Y}) = \Gamma(X, \mathcal{O}_X(-R))$ of $\Gamma(X, \Omega_{X/Y}) = \Omega_{B/A}$ is the different $\mathfrak{D}_{B/A}$ ([**135**, Proposition 14]). The different is defined in [**135**, Chapter III] and [**160**, Section 11 of Chapter V], using the trace of the quotient field of B over A. Proposition 18.31 is proven in [**160**, Theorem 28 of Section 11, Chapter V] and [**135**, Proposition 13]. On [**160**, page 312], a derivation of "Hilbert's formula" is given to compute $\deg(R)$ in the case of a Galois extension, even in the presence of wild ramification.

18.6. Inseparable maps of curves

Recall that a dominant regular map $\phi : X \to Y$ of varieties is separable if the induced field extension $k(Y) \to k(X)$ is finite and separable. We will say that $\phi : X \to Y$ is inseparable if $k(Y) \to k(X)$ is not separable and that $\phi : X \to Y$ is purely inseparable if $k(Y) \to k(X)$ is purely inseparable.

If $K \to L$ is a finite field extension, then there exists a (unique) intermediate field M (called the separable closure of K in L) such that L is purely inseparable over M and M is separable over K (Theorem 1.15). It

follows that any dominant finite regular map of algebraic varieties factors as a purely inseparable finite map, followed by a separable finite map.

Suppose that κ is a perfect field of characteristic $p > 0$ and R is a κ-algebra. Let $Fr : R \to R$ be the Frobenius homomorphism, defined by $Fr(x) = x^p$ for $x \in R$. The map Fr is a ring homomorphism but it is not a κ-algebra homomorphism. Let R_p be the ring R with the κ-algebra structure $\cdot$ given by $a \cdot x = a^p x$ for $a \in \kappa$ and $x \in R$. Then $Fr : R \to R_p$ is a κ-algebra homomorphism. Since R_p is equal to R as a ring, R_p is a domain if and only if R is a domain, R_p is normal if and only if R is normal, and R_p is regular if and only if R is regular.

Now suppose that R is also a domain with quotient field K. We can express R as a κ-algebra by $R = \kappa[S]$ for some subset S of K. Let Ω be an algebraic closure of K. Define $\Lambda : R_p \to \Omega$ by $\Lambda(f) = f^{\frac{1}{p}}$. For $a \in \kappa$ and $x \in R_p$, we have that

$$\Lambda(a \cdot x) = \Lambda(a^p x) = a x^{\frac{1}{p}} = a\Lambda(x),$$

so Λ is a κ-algebra homomorphism, which identifies R_p with the κ-subalgebra $\Lambda(R_p) = \kappa[S^{\frac{1}{p}}]$ of Ω (we have that $\Lambda(\kappa) = \kappa$ as κ is perfect). The composition $\Lambda Fr(x) = x$ for $x \in R$, so $Fr : R \to R_p$ is identified with the natural inclusion of κ-algebras

$$\kappa[S] \to \kappa[S^{\frac{1}{p}}]. \tag{18.15}$$

In particular, the quotient field of R_p is identified with $K^{\frac{1}{p}}$ as a κ-algebra.

Now suppose that X is an affine variety over an algebraically closed field k of characteristic $p > 0$. Let $R = k[X]$. The above construction gives us a finitely generated k-algebra R_p which is a domain and a k-algebra homomorphism $Fr : R \to R_p$. Thus there is an affine variety X_p and a regular map $F : X_p \to X$ such that $F^* = Fr$ (by Proposition 2.40).

If X is a quasi-projective variety, we can apply the above construction on an affine open cover of X to obtain by Proposition 3.39 a quasi-projective variety X_p with regular map $F : X_p \to X$. (If X is embedded in $\mathbb{P}^n$, then X_p is embedded in $\mathbb{P}^n_p$ which is isomorphic to $\mathbb{P}^n$ as a variety over k.) Applying the construction (18.15) to $Fr : k(X) \to k(X)$, we see that $k(X_p) \cong k(X)^{\frac{1}{p}}$ and $F^* : k(X) \to k(X_p)$ is the natural inclusion $k(X) \subset k(X)^{\frac{1}{p}}$. The regular map $F : X_p \to X$ is called the k-linear Frobenius map. If X is normal, then X_p is also normal, since X_p has an affine cover by normal varieties.

Theorem 18.33. *Suppose that X is a variety of dimension n. Then*

$$[k(X)^{\frac{1}{p}} : k(X)] = p^n.$$

Proof. An algebraic function field over a perfect field k is separably generated over k (by Theorem 1.14). The theorem then follows from 2) of Theorem 21.76 since $\text{trdeg}_k k(X) = \dim X = n$. □

Theorem 18.34. *Suppose that $f : X \to Y$ is a finite purely inseparable regular map of nonsingular projective curves. Then f is a composition of k-linear Frobenius maps. In particular, $g(X) = g(Y)$.*

Proof. Let the degree of f be $[k(X) : k(Y)] = p^r$. Suppose that $g \in k(X)$. The minimal polynomial of g over $k(Y)$ is $z^{p^i} - h$ for some $h \in k(Y)$ and $i \in \mathbb{N}$ with $i \leq r$ since g is purely inseparable over $k(Y)$ and $[k(Y)[g] : k(Y)]$ divides p^r. Thus $k(X)^{p^r} \subset k(Y)$ so $k(X) \subset k(Y)^{\frac{1}{p^r}}$. Let F' be the composition of k-linear Frobenius maps

$$Y_{p^r} \xrightarrow{F} Y_{p^{r-1}} \to \cdots \to Y_p \xrightarrow{F} Y$$

where $Y_{p^i} = (Y_{p^{i-1}})_p$. Here F' has degree p^r by Theorem 18.33. Since $k(X) \subset k(Y)^{\frac{1}{p^r}}$ and both $k(X)$ and $k(Y)^{\frac{1}{p^r}}$ have the same degree over $k(Y)$, we have that $k(X) = k(Y)^{\frac{1}{p^r}}$. Since a nonsingular projective curve is uniquely determined by its function field (by Corollary 10.25), we have that $X \cong Y_{p^r}$, and thus $f = F'$.

Let $\underline{U} = \{U_i\}$ be an affine open cover of Y with corresponding affine open cover $\underline{V} = \{V_i\}$ of Y_{p^r}. Now each $\Gamma(U_i, \mathcal{O}_Y)$ is isomorphic to $\Gamma(V_i, \mathcal{O}_{Y_{p^r}})$ as a ring (but not as a k-algebra) and the Čech complexes $C^*(\underline{U}, \mathcal{O}_Y)$ and $C^*(\underline{V}, \mathcal{O}_{Y_{p^r}})$ are isomorphic complexes of rings. Thus the cohomology is isomorphic, so $H^1(Y_{p^r}, \mathcal{O}_{Y_{p^r}})$ is $H^1(Y, \mathcal{O}_Y)$ with the vector space operation $a \cdot v = a^{p^r} v$ for $a \in k$. Since k is perfect, we have that

$$h^1(Y, \mathcal{O}_Y) = \dim_k H^1(Y, \mathcal{O}_Y) = \dim_k H^1(Y_{p^r}, \mathcal{O}_{Y_{p^r}}) = h^1(Y_{p^r}, \mathcal{O}_{Y_{p^r}})$$

and $g(Y) = g(Y_{p^r})$. □

Exercise 18.35. Let $\mathbb{P}^n$ be projective space over an algebraically closed field k of characteristic $p > 0$. Show that $(\mathbb{P}^n)_p$ is isomorphic to $\mathbb{P}^n$ (as varieties over k).

Exercise 18.36. Suppose that $f : X \to Y$ is a finite regular map of nonsingular projective curves. Show that $g(X) \geq g(Y)$.

Exercise 18.37 (Lüroth's theorem)**.** Suppose that k is an algebraically closed field and L is a subfield of a one-dimensional rational function field $k(t)$ over k such that L contains k and is not equal to k. Show that L is a one-dimensional rational function field over k.

Exercise 18.38. Give an example of a finite purely inseparable regular map of nonsingular projective surfaces which is not a composition of Frobenius maps.

18.7. Elliptic curves

Recall that a nonsingular projective curve X is called an elliptic curve if it has genus $g(X) = 1$. An elliptic curve is characterized by $K_X \sim 0$ by Corollary 18.18. The theory of elliptic curves is particularly remarkable and extensive. We give a brief introduction here. The group of regular isomorphisms of a variety X will be denoted by $\mathrm{Aut}(X)$.

Every nonsingular cubic curve X in $\mathbb{P}^2$ is an elliptic curve. This follows since by adjunction, Theorem 14.21, $\mathcal{O}_X(K_X) \cong \mathcal{O}_{\mathbb{P}^2}(K_{\mathbb{P}^2} + X) \otimes \mathcal{O}_X$ and since $K_{\mathbb{P}^2} = -X$ by Example 14.20.

The reader should peruse the definitions and statements of Section 21.7 on the Galois theory of varieties before reading the proofs of this section.

Lemma 18.39. *Suppose that X is an elliptic curve and P, Q are two not necessarily distinct points in X. Then there exists a regular automorphism $\sigma : X \to X$ such that $\sigma^2 = \mathrm{id}$, $\sigma(P) = Q$, and for any $R \in X$, $R + \sigma(R) \sim P + Q$.*

Proof. We have that $h^0(X, \mathcal{O}_X(P+Q)) = 2$ by Corollary 18.15 and $|P+Q|$ is base point free by Theorem 18.21. We thus have a regular map $\phi = \phi_{|P+Q|} : X \to \mathbb{P}^1$. A linear hyperplane section H on $\mathbb{P}^1$ is a point and $\phi^*(H)$ is an effective divisor linearly equivalent to $P + Q$ by Lemma 13.28. Thus $\deg(\phi) = [k(X) : k(\mathbb{P}^1)] = 2$ by Theorem 13.18. The field extension $k(X)/k(\mathbb{P}^1)$ is separable by Theorem 18.34, since otherwise $g(x) = g(\mathbb{P}^1) = 0$. Thus $k(X)$ is a Galois extension of $k(\mathbb{P}^1)$, so X is Galois over $\mathbb{P}^1$ by Theorem 21.69, with $G(X/\mathbb{P}^1) \cong \mathbb{Z}_2$ by Proposition 21.67. Let $\sigma \in G(X/\mathbb{P}^1)$ be a generator. Since X is Galois over $\mathbb{P}^1$, σ interchanges the two points of a fiber. There exists $S \in \mathbb{P}^1$ such that $\phi^*(S) = P + Q$ by Lemma 13.28, so $\sigma(P) = Q$. We have that

$$\bigcup_{F \in |P+Q|} F = \bigcup_{S \in \mathbb{P}^1} \phi^*(S) = X,$$

so for any $R \in X$, $R + \sigma(R) \in |P + Q|$, and thus $R + \sigma(R) \sim P + Q$. □

Corollary 18.40. *The group $\mathrm{Aut}(X)$ of regular automorphisms of an elliptic curve X is transitive on X.*

Lemma 18.41. *Suppose that $\phi_1 : X \to \mathbb{P}^1$ and $\phi_2 : X \to \mathbb{P}^1$ are two regular maps of degree 2 from an elliptic curve X to $\mathbb{P}^1$. Then there exist automorphisms $\sigma \in \mathrm{Aut}|(X)$ and $\tau \in \mathrm{Aut}(\mathbb{P}^1)$ such that $\phi_2\sigma = \tau\phi_1$.*

Proof. Let $P_1 \in X$ be a ramification point of ϕ_1 and $P_2 \in X$ be a ramification point of ϕ_2 (which exist by Theorem 18.32). By Corollary 18.40 there is $\sigma \in \mathrm{Aut}(X)$ such that $\sigma(P_1) = P_2$. Since P_1 is a ramification point of the

degree 2 map ϕ_1 and $h^0(X, \mathcal{O}_X(2P_1)) = 2$, we have that $\phi_1 = \phi_{|2P_1|}$, and since P_2 is a ramification point of the degree 2 map ϕ_2, $\phi_2 = \phi_{|2P_2|}$. Since σ takes P_1 to P_2, ϕ_1 and $\phi_2\sigma$ are induced by base point free linear systems which are contained in $|2P_1|$. But $|2P_1|$ is the only such linear system. Thus ϕ_1 and $\phi_2\sigma$ are induced by the same linear system, so they differ only by an automorphism of $\mathbb{P}^1$. □

Proposition 18.42. *Suppose that X is an elliptic curve over an algebraically closed field k of characteristic $\neq 2$ and let $P_0 \in X$ be a point. Then there is a closed embedding $\phi : X \to \mathbb{P}^2$ such that the image is the curve with the homogeneous equation*

$$x_2x_1^2 - x_0(x_0 - x_2)(x_0 - \lambda x_2) = 0 \tag{18.16}$$

for some $\lambda \in k \setminus \{0, 1\}$ and $\phi(P_0) = (0 : 1 : 0)$.

The affine equation of the image $\phi(X)\setminus\{(0 : 1 : 0)\}$ of $X \setminus P_0$ in $\mathbb{P}^2_{x_2} \cong \mathbb{A}^2$ is

$$y^2 = x(x - 1)(x - \lambda), \tag{18.17}$$

where $x = \frac{x_0}{x_2}$, $y = \frac{x_1}{x_2}$. We think of P_0 as being the "point at infinity" on X under this embedding, since $\phi(P_0) = (0 : 1 : 0) = \phi(X) \cap Z(x_2)$.

Proof. We have that $h^0(X, \mathcal{O}_X(nP_0)) = n$ for $n > 0$ by the Riemann-Roch theorem. The linear system $|3P_0|$ gives a closed embedding $\phi = \phi_{|3P_0|}$ of X into $\mathbb{P}^2$ by Theorem 18.21. Within the function field $k(X)$, we have inclusions

$$k = \Gamma(X, \mathcal{O}_X) = \Gamma(X, \mathcal{O}_X(P_0)) \subset \Gamma(X, \mathcal{O}_X(2P_0)) \subset \cdots .$$

Choose $x \in k(X)$ so that $1, x$ are a basis of $\Gamma(X, \mathcal{O}_X(2P_0))$ and choose $y \in k(X)$ so that $1, x, y$ are a basis of $\Gamma(X, \mathcal{O}_X(3P_0))$. Since $h^0(X, \mathcal{O}_X(6P_0)) = 6$, there is a linear relation between the seven functions $1, x, y, x^2, xy, x^3, y^2 \in \Gamma(X, \mathcal{O}_X(6P_0))$. Further, x^3 and y^2 must both have nonzero coefficients in this relation, since otherwise the relation will have a pole of finite order at P_0, as x has a pole of order 2 at P_0 and y has a pole of order 3 at P_0. (1 has no pole at P_0 and xy has a pole of order 5 at P_0.) Replacing x and y by suitable scalar multiples, we may assume that we have a relation

$$y^2 + b_1xy + b_2y = f(x)$$

where $f(x)$ is a degree 3 monic polynomial in x and $b_1, b_2 \in k$. Completing the square in y by replacing y with

$$y' = y + \frac{1}{2}(b_1x + b_2),$$

we obtain the relation

$$y^2 = g(x) \tag{18.18}$$

where $g(x) = x^3 + a_1x^2 + a_2x + a_3$ for some $a_1, a_2, a_3 \in k$ (this is where we need characteristic $\neq 2$).

We represent the closed embedding $\phi : X \to \mathbb{P}^2$ by $\phi = (x : y : 1) = (\frac{x_0}{x_2} : \frac{x_1}{x_2} : 1)$. The relation (18.18) becomes

$$x_1^2x_2 = x_0^3 + a_1x_0^2x_2 + a_2x_0x_2^2 + a_3x_2^3. \tag{18.19}$$

Thus $\phi(X) \subset Z(F)$ where

$$F = x_1^2x_2 - x_0^3 - a_1x_0^2x_2^2 - a_2x_0x_2 - a_3x_2^3.$$

The image of ϕ is a closed irreducible curve $\phi(X)$, which has codimension 1 in $\mathbb{P}^2$. Since F is irreducible in the coordinate ring $k[x_0, x_1, x_2]$ of $\mathbb{P}^2$, $(F) = I(\phi(X))$.

The regular functions on the affine open subset $\mathbb{P}^2_{x_2} \cong \mathbb{A}^2$ of $\mathbb{P}^2$ are $k[\mathbb{P}^2_{x_2}] = k[\overline{x}, \overline{y}]$ where $\overline{x} = \frac{x_0}{x_2}, \overline{y} = \frac{x_1}{x_2}$. The ideal of $\phi(X) \cap \mathbb{P}^2_{x_2}$ is generated by $f = \overline{y}^2 - g(\overline{x})$.

Since $\phi(X)$ is nonsingular, $g(\overline{x})$ can have no multiple roots (by the Jacobian criterion of Proposition 10.14). Thus we can make a change of variables $x' = \alpha x + \beta$ for some $\alpha \neq 0, \beta \in k$, and replace y with a scalar multiple of y to obtain an expression (18.18) with $g(x) = x(x-1)(x-\lambda)$ for some $\lambda \in k$ with $\lambda \neq 0$ or 1. Finally, we see that the set of points at infinity on $\phi(X)$ is the algebraic set $Z(x_2) \cap \phi(X) = Z(x_2, x_0^3) = \{(0 : 1 : 0)\}$. Since x has a pole of order 2 at P_0 and y has a pole of order 3 at P_0,

$$\phi(P_0) = \left(\frac{x}{y}(P_0) : 1 : \frac{1}{y}(P_0)\right) = (0 : 1 : 0). \qquad \square$$

We can regard $\mathbb{P}^1$ as $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$, with $k[\mathbb{A}^1] = k[z]$ and $k(\mathbb{P}^1) = k(z)$. The group of automorphisms of $\mathbb{P}^1$ consists of the linear automorphisms (Exercise 13.47), so they can be represented as fractional linear transformations

$$\frac{az + b}{cz + d}$$

with $a, b, c, d \in k$ and $ad - bc \neq 0$. The corresponding transformation in homogeneous coordinates is

$$(ax_0 + bx_1 : cx_0 + dx_1).$$

Let G be the subgroup of $\mathrm{Aut}(\mathbb{P}^1)$ consisting of the automorphisms which permute $\{0, 1, \infty\}$. Then $G \cong S_3$ with

$$G = \left\{ z, \frac{1}{z}, 1-z, \frac{1}{1-z}, \frac{z}{z-1}, \frac{z-1}{z} \right\}. \tag{18.20}$$

We have that the group G is generated by $\frac{1}{z}$ and $1 - z$.

Suppose that X is an elliptic curve with char $k \neq 2$ and $P_0 \in X$. Consider the linear system $|2P_0|$ which gives a regular map $\Psi = \phi_{|2P_0|} : X \to \mathbb{P}^1$ which is Galois of degree 2 (as we saw in the proof of Lemma 18.39). By Hurwitz's theorem (Ψ is tamely ramified since char $k \neq 2$), Ψ is ramified over four points: $a, b, c, d \in \mathbb{P}^1$ with $\Psi(P_0) = d$. There exists a unique linear automorphism τ of $\mathbb{P}^1$ which takes d to ∞, a to 0, and b to 1. Let λ be the image of c. Then $\tau\Psi$ is ramified over $0, 1, \lambda, \infty$.

Define the j invariant of X as

$$j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

We have (we need only check the generators $\frac{1}{z}$ and $1 - z$ of G in (18.20)) that

$$j(\sigma(\lambda)) = j(\lambda) \quad \text{for } \sigma \in G. \tag{18.21}$$

Write $\mathbb{P}^2 = \mathbb{A}^2 \cup H$ where $H = Z(x_2)$ is "the hyperplane at infinity". The closed embedding $\phi = \phi_{|3P_0|}$ of Proposition 18.42 gives an expression of X as (isomorphic) to the union of the affine curve

$$C = Z(y^2 - x(x-1)(x-\lambda)) \subset \mathbb{A}^2$$

and the point "at infinity" $P_0 = (0 : 1 : 0)$. The degree 2 map $\Psi = \phi_{|2P_0|}$ is the linear projection to $\mathbb{P}^1$ which takes $(a, b) \in C$ to $a \in \mathbb{A}^1$ and P_0 to ∞.

Theorem 18.43. *Suppose that k is an algebraically closed field of characteristic not equal to 2. For $\lambda_1, \lambda_2 \in k \setminus \{0, 1\}$, if X_1 is an elliptic curve which gives λ_1 in the above construction of λ and X_2 is an elliptic curve which gives λ_2, then X_1 is isomorphic to X_2 if and only if $j(\lambda_1) = j(\lambda_2)$. Further, every element of k is the j invariant of some elliptic curve X.*

Proof. We will first show that $j(\lambda)$ is uniquely determined by an elliptic curve X. Suppose $P_1, P_2 \in X$ and $\Psi_1 : X \to \mathbb{P}^1$ is induced by $|2P_1|$ so that the ramification points of Ψ_1 in $\mathbb{P}^1$ are $0, 1, \lambda_1, \infty$ with $\Psi_1(P_1) = \infty$ and $\Psi_2 : X \to \mathbb{P}^1$ is induced by $|2P_2|$ so that the ramification points of Ψ_2 in $\mathbb{P}^1$ are $0, 1, \lambda_2, \infty$ with $\Psi_2(P_2) = \infty$. By Lemma 18.41 and its proof, there exist automorphisms $\sigma \in \mathrm{Aut}(X)$ and $\tau \in \mathrm{Aut}(\mathbb{P}^1)$ such that $\Psi_2\sigma = \tau\Psi_1$ with $\sigma(P_1) = P_2$ so that $\tau(\infty) = \infty$ and τ sends the other ramification

points $\{0, 1, \lambda_1\}$ to $\{0, 1, \lambda_2\}$ in some order. Let $\gamma(z)$ be the fractional linear transformation of $\mathbb{P}^1$ defined by

$$\gamma(z) = \frac{z - \tau(0)}{\tau(1) - \tau(0)}.$$

Then $\gamma\tau(0) = 0$, $\gamma\tau(1) = 1$, and $\gamma\tau(\infty) = \infty$, so $\gamma\tau$ is the identity map. Thus

$$\lambda_1 = \gamma\tau(\lambda_1) = \frac{\tau(\lambda_1) - \tau(0)}{\tau(1) - \tau(0)}.$$

Since the sets $\{\tau(0), \tau(1), \tau(\lambda_1)\}$ and $\{0, 1, \lambda_2\}$ are equal, we have that

$$\lambda_2 \in \left\{ \lambda_1, \frac{1}{\lambda_1}, 1 - \lambda_1, \frac{1}{1 - \lambda_1}, \frac{\lambda_1}{\lambda_1 - 1}, \frac{\lambda_1 - 1}{\lambda_1} \right\},$$

and so $j(\lambda_1) = j(\lambda_2)$ by (18.21).

Now suppose that X_1 and X_2 are two elliptic curves, giving λ_1 and λ_2, respectively, and such that $j(\lambda_1) = j(\lambda_2)$. The regular map $j : \mathbb{A}^1 \setminus \{0, 1\} \to \mathbb{A}^1$ extends to a regular map $j = (j : 1) : \mathbb{P}^1 \to \mathbb{P}^1$ with $j^{-1}(\infty) = \{0, 1, \infty\}$, which induces

$$j^* : k(\mathbb{P}^1) = k(j) \to k(\mathbb{P}^1) = k(\lambda)$$

defined by

$$j \mapsto 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

For $j_0 \in \mathbb{A}^1$,

$$2^8(\lambda^2 - \lambda + 1)^3 - j_0\lambda^2(\lambda - 1)^2 = 0$$

is an equation of degree 6 in λ, so counting multiplicities, it has six roots. Thus

$$6 = \deg(j^*(j_0)) = [k(\lambda) : k(j)]$$

by Theorem 13.18. By (18.21), substituting λ for z, G acts on $k(\lambda)$ by k-automorphisms which leave $k(j)$ invariant. Since $[k(\lambda) : k(j)] = 6$ and $|G| = 6$, we have that $k(\lambda)$ is Galois over $k(j)$ with Galois group G. Thus $j : \mathbb{P}^1 \to \mathbb{P}^1$ is Galois with Galois group G (Theorem 21.69), and so

$$j(\lambda_1) = j(\lambda_2)$$

if and only if there exists $\tau \in G$ such that $\tau(\lambda_1) = \lambda_2$.

By Proposition 18.42, X_1 and X_2 can be embedded in $\mathbb{P}^2$ with respective affine equations

$$y^2 = x(x - 1)(x - \lambda_1) \tag{18.22}$$

and

$$y^2 = x(x - 1)(x - \lambda_2). \tag{18.23}$$

Since $j(\lambda_1) = j(\lambda_2)$, there exists $\tau \in G$ such that $\tau(\lambda_1) = \lambda_2$, and thus τ permutes $0, 1, \infty$. Let $\Psi_1 : X_1 \to \mathbb{P}^1$ be the 2-1 cover induced by projection onto the x-axis in (18.22). Then $\tau\Psi_1 : X_1 \to \mathbb{P}^1$ is a degree 2 map which is ramified over $0, 1, \lambda_2, \infty$ in $\mathbb{P}^1$. Let $Q = (\tau\Psi_1)^{-1}(\infty)$. Then $x \in H^0(X_1, \mathcal{O}_{X_1}(2Q))$ where $\tau\Psi_1 = (x : 1)$. Proceeding as in the proof of Proposition 18.42, we find $y \in H^0(X_1, \mathcal{O}_{X_1}(3Q))$, giving the relation $y^2 = g(x)$ of (18.18) and such that $\phi_{|3Q|} = (x : y : 1)$ is a closed embedding of X_1 into $\mathbb{P}^2$. The points in $X_1 \subset \mathbb{P}^2$ where $\tau\Psi_1 : X_1 \to \mathbb{P}^1$ is ramified are Q and the points in $X_1 \cap \mathbb{A}^2$ where $y = 0$. Since $\tau\Psi_1$ is ramified over 0, 1, λ_2, and ∞ and g is monic of degree 3, we see that $g(x) = x(x-1)(x-\lambda_2)$. Thus X_1 is isomorphic to the cubic curve with affine equation (18.23), so X_1 is isomorphic to X_2.

Now given $j_0 \in k$, we can solve the equation

$$2^8(\lambda^2 - \lambda + 1)^3 - j_0\lambda^2(\lambda - 1)^2 = 0$$

to find a solution $\lambda_0 \in k$, which cannot be 0 or 1. The elliptic curve with affine equation

$$y^2 = x(x-1)(x-\lambda_0)$$

defines a nonsingular cubic curve of degree 3 in $\mathbb{P}^2$ which is an elliptic curve that has j_0 as its j invariant. □

Let X be an elliptic curve with a fixed point $P_0 \in X$. By Theorem 18.19, the map $P \mapsto [P - P_0]$ is a bijection from X to $\mathrm{Cl}^0(X)$. This induces a group structure on X with P_0 as the zero element and with addition $\oplus$ defined by $P \oplus Q = R$ if and only if $P + Q \sim R + P_0$ as divisors on X.

Proposition 18.44. *Suppose that X is an elliptic curve with the group structure given as above by the choice of a point $P_0 \in X$. Then the addition map $X \times X \to X$ and the inverse map $X \to X$ are regular maps.*

Proof. We will denote the addition of P and Q in X by $P \oplus Q$ and the inverse of P by $\ominus P$.

By Lemma 18.39, taking $P = Q = P_0$, there is an automorphism σ of X such that for any $R \in X$, $R + \sigma(R) \sim 2P_0$. Thus $\ominus R = \sigma(R)$, and so the inverse map $\ominus$ is a regular map.

Let $P \in X$. By Lemma 18.39, there is an automorphism τ of X such that $R + \tau(R) \sim P + P_0$ for all $R \in X$. Thus $P \ominus R = \tau(R)$, and since $\ominus$ is a regular map, we have that translation $R \mapsto R \oplus P$ is a regular map for fixed $P \in X$.

Embed X into $\mathbb{P}^2$ by $\phi_{|3P_0|}$. Let $F = 0$ be the homogeneous cubic equation of X in $\mathbb{P}^2$. If L is a linear form on $\mathbb{P}^2$, then L intersects X in three points with multiplicity, considering the restriction of F to L as a degree

3 form on $L \cong \mathbb{P}^1$. (This is a special case of Bézout's theorem, which we will prove later in Theorem 19.20.) Thus we have a map $\lambda : X \times X \to X$ obtained by letting the image of (P, Q) be the third point of intersection of the line through P and Q with X (if $P = Q$, the line through P is required to be tangent to X at p).

We will establish that this map is in fact regular everywhere. It will follow that addition, $(P, Q) \mapsto P \oplus Q$, is a regular map, since $P + Q + \lambda(P, Q) \sim 3P_0$ and $P + Q \sim (P \oplus Q) + P_0$, so $(P \oplus Q) \oplus \lambda(P, Q) = P_0$ and thus $P \oplus Q = \ominus\lambda(P, Q)$.

Given $P, Q \in X$, there exists a linear form H of $\mathbb{P}^2$ such that all three intersection points of the line through P and Q with X lie in $\mathbb{P}^2_H$. Thus we are reduced to showing that if $f = 0$ is the equation of $C = X \cap \mathbb{P}^2_H$ in $\mathbb{P}^2_H \cong \mathbb{A}^2$ and if P, Q are points of C such that the line through P and Q in C has three intersections with C in $\mathbb{A}^2$ (counting multiplicity), then the rational map λ is regular near (P, Q).

We now consider $P = (\alpha, \beta)$ and $Q = (\gamma, \delta)$ as variable points in $\mathbb{A}^2$. The line through P and Q in $\mathbb{A}^2$ can be parameterized as

$$x = \alpha + t(\gamma - \alpha), \qquad y = \beta + t(\delta - \beta).$$

The intersection points of this line with C are obtained from the solutions in t to

$$g(t) = f(\alpha + t(\gamma - \alpha), \beta + t(\delta - \beta)) = 0.$$

Write $g(t) = at^3 + bt^2 + ct + d$ with a, b, c, d in the polynomial ring $k[\alpha, \beta, \gamma, \delta]$. We now constrain $P = (\alpha, \beta)$ and $Q = (\gamma, \delta)$ to lie on C. Thus we consider the residues $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ of a, b, c, d in

$$R = k[\alpha, \beta, \gamma, \delta]/(f(\alpha, \beta), f(\gamma, \delta))$$

(which is a domain by Proposition 5.7). Let $\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta}$ be the residues of $\alpha, \beta, \gamma, \delta$ in R, so that $R = k[\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta}]$. Let $\overline{g}(t) = \overline{a}t^3 + \overline{b}t^2 + \overline{c}t + \overline{d}$ be the residue of $g(t)$ in $R[t]$. We have that $\overline{g}(0) = f(\overline{\alpha}, \overline{\beta}) = 0$ and $\overline{g}(1) = f(\overline{\gamma}, \overline{\delta}) = 0$. Thus $\overline{d} = 0$ and $\overline{a} + \overline{b} + \overline{c} = 0$, and we have a factorization

$$\overline{g}(t) = t(t - 1)(\overline{a}t + (\overline{a} + \overline{b})).$$

We see that if $a \neq 0$, then λ is the regular map defined by

$$\lambda\left((u_1, v_1) \times (u_2, v_2)\right) = \left(u_1 - \frac{a+b}{a}(u_1, v_1, u_2, v_2)(u_2 - u_1), v_1 - \frac{a+b}{a}(u_1, v_1, u_2, v_2)(v_2 - v_1)\right).$$

□

In the language of [**146**], (α, β) and (γ, δ) in the above proof are "independent generic points".

Lemma 18.45 (Rigidity lemma)**.** *Let X be a projective variety, Y and Z be quasi-projective varieties, and $f : X \times Y \to Z$ be a regular map such that for some $Q \in Y$, $f(X \times \{Q\}) = P$ is a single point of Z. Then there is a regular map $g : Y \to Z$ such that if $\pi_2 : X \times Y \to Y$ is the projection, we have that $f = g \circ \pi_2$.*

Proof. Let $R \in X$ be a point and define $g : Y \to Z$ by $g(y) = f(R, y)$. Since two regular maps on a variety are equal if they agree on a nontrivial open set, we need only show that f and $g \circ \pi_2$ agree on some open subset of $X \times Y$. Let U be an affine open neighborhood of P in Z, $F = Z \setminus U$, and $G = \pi_2(f^{-1}(F))$. The set G is closed in Y since $f^{-1}(F)$ is closed in $X \times Y$ and X is projective, and hence π_2 is a closed map (Corollary 5.13). We have that $Q \notin G$ since $f(X \times \{Q\}) = P \notin F$. Thus $V = Y \setminus G$ is a nonempty open neighborhood of Q in Y. For each $y \in V$, the projective variety $X \times \{y\}$ is mapped by f into the affine variety U and hence to a single point of U (by Corollary 5.16). Thus for any $x \in X$ and $y \in V$, we have that

$$f(x, y) = f(R, y) = g \circ \pi_2(x, y),$$

proving the lemma. □

Corollary 18.46. *Let X be an elliptic curve with group structure defined by a point $P_0 \in X$ and let Y be an elliptic curve with group structure defined by $Q_0 \in Y$. Suppose that $\Phi : X \to Y$ is a regular map such that $\Phi(P_0) = Q_0$. Then Φ is a group homomorphism.*

Proof. Consider the regular map $\Psi : X \times X \to Y$ defined by

$$\Psi(x, y) = \Phi(x \oplus y) \ominus \Phi(x) \ominus \Phi(y).$$

Then $\Psi(X \times \{P_0\}) = \Psi(\{P_0\} \times X) = Q_0$, so $\Psi(x, y) = Q_0$ for all $x, y \in X$ by Lemma 18.45. □

18.8. Complex curves

A nonsingular projective curve X over $k = \mathbb{C}$ has the structure of a Riemann surface, and $g = g(X)$ is the topological genus of X (X is topologically a sphere with g handles). This is discussed, for instance, in [**115**] and [**62**]. Now such X has the Euclidean topology. We proved that when G is an Abelian group, then $\Gamma(U, G) \cong G^r$ where r is the number of connected components of U (by Proposition 11.14). This is the same as the first singular cohomology $H^0_{\text{Sing}}(U, G)$. Now the Čech complex computes singular cohomology of X, since X can be triangulated ([**49**, Section 9 of Chapter X]

or [**62**]) and computes sheaf cohomology, so we obtain that the sheaf cohomology $H^i(X, \mathbb{Z}_{\text{an}})$ is isomorphic to $H^i_{\text{Sing}}(X, \mathbb{Z})$. We write $\mathbb{Z}_{\text{an}}$ to indicate that we are in the Euclidean topology. Now we regard X as a compact two-dimensional oriented real manifold, and then we have (for instance by [**103**]) that

$$H^i_{\text{Sing}}(X, \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if } i = 0, \\ \mathbb{Z}^{2g} & \text{if } i = 1, \\ \mathbb{Z} & \text{if } i = 2, \\ 0 & \text{if } i > 2. \end{cases}$$

Let $\mathcal{O}_X^{\text{an}}$ be the sheaf of analytic functions on X and $(\mathcal{O}_X^{\text{an}})^*$ be the sheaf of nonvanishing analytic functions. Then we have a short exact sequence of sheaves

$$0 \to \mathbb{Z} \to \mathcal{O}_X^{\text{an}} \xrightarrow{e} (\mathcal{O}_X^{\text{an}})^* \to 0,$$

where e denotes the exponential map $f \mapsto e^f$.

It follows from GAGA [**133**] that if Y is a complex projective variety and $\mathcal{F}$ is a coherent sheaf on Y, then the cohomology of the extension $\mathcal{F}^{\text{an}}$ of $\mathcal{F}$ to an analytic sheaf is the same as the cohomology of $\mathcal{F}$. Thus $H^i(X, \mathcal{O}_X^{\text{an}}) \cong H^i(X, \mathcal{O}_X)$ for all i. Taking sheaf cohomology, we get the long exact sequence

$$\begin{aligned} 0 \to \mathbb{Z} \to \mathbb{C} \xrightarrow{e} \mathbb{C}^* \to H^1(X, \mathbb{Z}) \to H^1(X, \mathcal{O}_X) \\ \to H^1(X, (\mathcal{O}_X^{\text{an}})^*) \xrightarrow{c} H^2(X, \mathbb{Z}) \to H^2(X, \mathcal{O}_X). \end{aligned}$$

Now X has genus g and dimension 1, so that $H^2(X, \mathcal{O}_X) = 0$. Further, $e : \mathbb{C} \to \mathbb{C}^*$ is onto. Thus from our above exact sequence, we deduce that we have an exact sequence of groups

$$0 \to \mathbb{C}^g/\mathbb{Z}^{2g} \to H^1(X, (\mathcal{O}_X^{\text{an}})^*) \xrightarrow{c} \mathbb{Z} \to 0,$$

since

$$H^1(X, \mathcal{O}_X)/H^1(X, \mathbb{Z}) \cong \mathbb{C}^g/\mathbb{Z}^{2g}.$$

From the argument of Theorem 17.16, we have that

$$H^1(X, (\mathcal{O}_X^{\text{an}})^*) \cong \text{Pic}^{\text{an}}(X),$$

the group of invertible analytic sheaves on X, modulo isomorphism. Now again by GAGA, we know that all global analytic sheaves on X are isomorphic to algebraic sheaves, and this isomorphism takes global analytic homomorphisms to algebraic homomorphisms. Thus the natural map

$$\text{Pic}(X) \to \text{Pic}^{\text{an}}(X)$$

is an isomorphism. In conclusion, we have obtained the following theorem:

Theorem 18.47. *Suppose that X is a nonsingular projective curve of genus g over the complex numbers. Then there is a short exact sequence of groups*

$$0 \to G \to \mathrm{Pic}(X) \xrightarrow{c} \mathbb{Z} \to 0,$$

where G is a group $\mathbb{C}^g/\mathbb{Z}^{2g}$.

The subset $H^1(X,\mathbb{Z}) \cong \mathbb{Z}^{2g}$ of $H^1(X,\mathcal{O}_X) \cong \mathbb{C}^g$ is in fact a lattice, if we regard $\mathbb{C}^g$ as a $2g$-dimensional real vector space. Thus in the Euclidean topology, $G \cong (S^1)^{2g}$ where S is the circle $\mathbb{R}/\mathbb{Z}$ and G is a "torus". This group G naturally has the structure of an analytic manifold (of complex dimension g), and it is even an algebraic variety (of dimension g). The group structure on G is algebraic. The map c is just the degree map, and the exact sequence of the theorem is just the exact sequence

$$0 \to \mathrm{Cl}^0(X) \to \mathrm{Cl}(X) \xrightarrow{\deg} \mathbb{Z} \to 0$$

of (13.11).

Using our natural isomorphism of $\mathrm{Pic}(X)$ with $\mathrm{Cl}(X)$, the map c (for Chern) is actually the degree of a divisor which we studied on a curve earlier. We can thus identify the algebraic group G with the group $\mathrm{Cl}^0(X)$ of linear equivalence classes of divisors of degree 0 on X. This group G is called the Jacobian of X (in honor of Jacobi). Fixing a point $P_0 \in X$, we obtain a map $X \to J$ defined by mapping a point P to the class of $P - P_0$. This map is a regular map and is a closed embedding if $g > 0$.

18.9. Abelian varieties and Jacobians of curves

In this section we discuss the algebraic construction of the Jacobian. We need to introduce a couple of new concepts first.

An Abelian variety A (in honor of Abel) is a projective variety with a group structure such that the multiplication $m : A \times A \to A$ is a regular map and the inverse map $i : A \to A$ is a regular map. There is an extensive literature on these remarkable varieties. A few references are [**146**], [**96**], [**119**], and [**110**]. The elliptic curves are the one-dimensional Abelian varieties. An Abelian variety is commutative and nonsingular (as is shown in any of these references). A g-dimensional Abelian variety over the complex numbers is isomorphic by an analytic isomorphism to a complex torus $\mathbb{C}^g/\Lambda$, where Λ is a lattice in $\mathbb{C}^g$.

Suppose that X is a variety and r is a positive integer. The symmetric group S_r acts on the product X^r by permuting factors. There exists a variety $X^{(r)}$ whose function field is $k(X^r)^{S_r}$ which is a quotient X^r/S_r [**119**, II, Section 7 and III Section 11]. In the case when X is a nonsingular projective

curve, $X^{(r)}$ is nonsingular [**111**, Proposition 3.2]. The points of $X^{(r)}$ can be considered as effective divisors $p_1 + p_2 + \cdots + p_r$ of degree r on X.

We have the following theorem.

Theorem 18.48. *Suppose that X is a nonsingular projective curve of genus g. Then there exists an Abelian variety J of dimension g and a regular map $\phi : X \to J$ such that:*

1. *ϕ is a closed embedding.*
2. *ϕ induces a birational regular map $X^{(g)} \to J$ by*

$$p_1 + \cdots + p_g \mapsto \sum_{i=1}^{g} \phi(p_i).$$

3. *ϕ induces a group isomorphism $\mathrm{Cl}^0(X) \to J$ by $[D] \mapsto \sum n_i \phi(p_i)$ if $D = \sum n_i p_i$.*

The variety J of Theorem 18.48 is called the Jacobian of X.

An Abelian variety A of positive dimension $n > 0$ over the complex numbers has lots of points of infinite order (under the group law of A). This follows from the fact that there is an analytic isomorphism of A with the quotient of $\mathbb{C}^g$ by a lattice of $\mathbb{C}^g$. However, if A is an Abelian variety over the algebraic closure of a finite field, then every element of A has finite order. We see this as follows. Suppose that k is the algebraic closure of a finite field and A is an Abelian variety over k. Then A is a subvariety of a projective space $\mathbb{P}^n_k$. Suppose that $x \in A$. Then there exists a finite field k' such that the embedding of A into $\mathbb{P}^n$ is defined over k, x is a rational point over k', and the addition on A is defined over k'. There are only finitely many points of $\mathbb{P}^n$ which are rational over k' so there are only finitely many points of A which are rational over k'. All multiples of x are rational over k' since the multiplication is defined over k' and x is rational over k'. Thus x has finite order in the group A.

Let A be an Abelian variety over an algebraically closed field k. Let $A(k)$ be the group of points of A, so that $A(k)$ is a $\mathbb{Z}$-module. The rank of $A(k)$ is $\mathrm{rank}(A(k)) = \dim_{\mathbb{Q}} A(k) \otimes \mathbb{Q}$. We have seen that if A is an Abelian variety over the algebraic closure k of a finite field, then $\mathrm{rank}(A(k)) = 0$. However, we have the following theorem ensuring us that there are lots of points of infinite order on an Abelian variety of positive dimension over any other algebraically closed field.

Theorem 18.49. *Suppose that A is a positive-dimensional Abelian variety defined over an algebraically closed field k which is not the algebraic closure of a finite field. Then the rank of $A(k)$ is equal to the cardinality of k.*

Proof. [**56**, Theorem 10.1]. □

We also have the following proposition describing the points of finite order in an Abelian variety.

Proposition 18.50. *Let A be an Abelian variety of dimension g over an algebraically closed field k. For $n \in \mathbb{Z}_{\geq 0}$, let*

$$A_n(k) = \{x \in A \mid nx = 0\}.$$

Suppose that the characteristic p of k does not divide n. Then $A_n(k) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof. [**119**, Proposition, page 64]. □

In the case when $k = \mathbb{C}$, so that there is an analytic isomorphism $A \cong \mathbb{C}^g/\Lambda$ where Λ is a lattice in $\mathbb{C}^g$, the proposition follows since $A_n(\mathbb{C}) \cong (\frac{1}{n}\Lambda)/\Lambda$.

The history of Abelian varieties and Jacobian varieties is outlined at the end of Milne's article [**111**]. Milne proves many interesting facts about the Jacobian in [**111**], including giving in [**111**, Section 7] a proof in modern language of Weil's proof in [**146**] of Theorem 18.48, the original proof using the language of *Foundations of Algebraic Geometry* [**145**]. Milne refers to Section 2 of Artin [**12**] for a proof in modern language of Weil's theorem that a "birational group" is isomorphic to an algebraic group [**146**].

Throughout these exercises C will denote a nonsingular projective curve of genus g.

Exercise 18.51. Show that $|K_C|$ is base point free if $g \geq 1$.

Exercise 18.52. Show that mK_C is very ample if $g \geq 3$ and $m \geq 2$.

Exercise 18.53. If $g = 2$, show that mK_C is very ample for $m \geq 3$ and $\phi_{|2K_C|} : C \to \mathbb{P}^2$ is a degree 2 regular map onto a quadric curve in $\mathbb{P}^2$ (which is isomorphic to $\mathbb{P}^1$).

Exercise 18.54. Suppose that C is defined over an algebraically closed field k of characteristic 0. Suppose that $0 \neq f \in k(C)$ and that the regular map $\phi = (f : 1) : C \to \mathbb{P}^1$ has degree n. Show that

$$g = \frac{1}{2}\left(\sum_{p \in C}(e_p - 1)\right) - n + 1.$$

Exercise 18.55. A curve C is called a hyperelliptic curve if there exists a degree 2 regular map $\phi : C \to \mathbb{P}^1$. Suppose that k is an algebraically closed field of characteristic 0 and $a_1, \ldots, a_l \in k$ are distinct. Let γ be the affine

curve $\gamma = Z(y^2 - f(x)) \subset \mathbb{A}^2$ where $f(x) = \prod_{i=1}^{l}(x - a_i)$. Let C be the resolution of singularities of the Zariski closure of γ in $\mathbb{P}^2$, and let $\pi : C \to \mathbb{P}^1$ be the regular map which when restricted to γ is the projection of γ onto the x-axis. Show that π is a degree 2 map. Compute the ramification of π and show that C has genus $g = l - 1$.

Exercise 18.56. Suppose that C is a plane curve of degree 4.

a) Show that the effective canonical divisors on C are the divisors $i^*(L)$ where $i : C \to \mathbb{P}^2$ is inclusion and L is a line on $\mathbb{P}^2$.

b) Show that the genus of C is 3.

c) If D is any effective divisor of degree 2 on C, show that $h^0(C, \mathcal{O}_C(D)) = 1$.

d) Conclude that C is not hyperelliptic.

Exercise 18.57. Suppose that C is not a hyperelliptic curve. Show that K_C is very ample.

Exercise 18.58. Suppose that C is a hyperelliptic curve with degree 2 regular map $\phi : C \to \mathbb{P}^1$ and $p \in C$ is a ramification point. Show that

$$h^0(C, \mathcal{O}_C(mp)) = \begin{cases} i+1 & \text{if } m = 2i,\ 1 \le i \le g, \\ i+1 & \text{if } m = 2i+1,\ 1 \le i \le g, \\ m+1-g & \text{if } m \ge 2g. \end{cases}$$

Exercise 18.59. Suppose that $g \ge 2$ and $\phi : C \to C$ is a dominant regular map. Show that ϕ is an isomorphism.