IX. The Number Theory of Algebraic Curves, 520-557

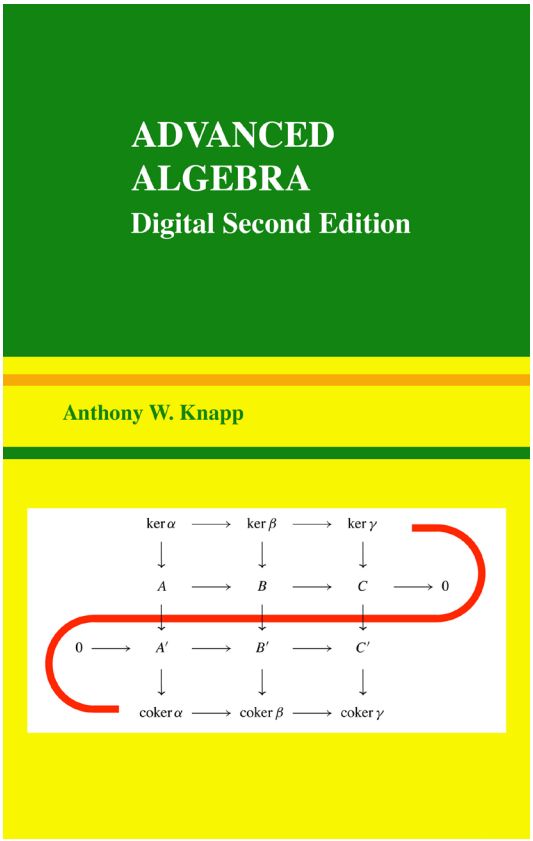
DOI: 10.3792/euclid/9781429799928-9

from

Advanced Algebra
Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928
ISBN: 978-1-4297-9992-8



Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/~aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9

Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN

Published by the Author

CHAPTER IX

The Number Theory of Algebraic Curves

Abstract. This chapter investigates algebraic curves from the point of view of their function fields, using methods analogous to those used in studying algebraic number fields.

Section 1 gives an overview, explaining how Riemann's theory of Riemann surfaces of functions ties in with the notion of an algebraic curve and explaining how such curves can be investigated through the discrete valuations of their function fields. It is shown that what needs to be studied is arbitrary function fields in one variable over a base field. It is known that every compact Riemann surface can be viewed as an algebraic curve irreducible over $\mathbb{C}$, and thus the function fields of compact Riemann surfaces are to be viewed as informative examples of the theory in the chapter.

Section 2 introduces the notion of a divisor, which is any formal finite $\mathbb{Z}$ linear combination of the discrete valuations of the function field that are trivial on the base field, and the notion of the degree of a divisor, which is the sum of its coefficients weighted suitably. Each nonzero member x of the function field gives rise to a principal divisor (x), and the main result of the section is that the degree of every principal divisor is 0. This is an analog for function fields of the Artin product formula for number fields.

Section 3 contains the definition of the genus of the function field under study. The main object of study is the vector space $L(A)$ for a divisor A; this consists of 0 and all nonzero members x of the function field such that $(x) + A$ is a divisor ≥ 0. Roughly speaking, it may be viewed as the space of functions on the zero locus of the curve whose poles are limited to finitely many points and to a certain order depending on the point. The genus is defined in terms of $\dim L(A) - \deg A$ when A is a divisor that is a large multiple of the pole part of any fixed principal divisor. The main result of the section is Riemann's inequality, which says that $\dim L(A) \geq \deg A + 1 - g$ for all divisors A, where $g \geq 0$ is the genus, and that g is the smallest integer that works in this inequality for all divisors A.

Sections 4–5 concern the Riemann–Roch Theorem, which gives an interpretation of the difference of the two sides of Riemann's inequality as $\dim L(B)$ for a suitable divisor B that can be defined in terms of A. Section 4 gives the statement and proof of the theorem, and Section 5 gives a number of simple applications.

1. Historical Origins and Overview

As was mentioned in Chapter VIII, modern algebraic geometry grew out of early attempts to solve simultaneous polynomial equations in several variables and out of the theory of Riemann surfaces. Chapter VIII discussed the impact of the first of these sources, and the present chapter discusses the impact of the second.

The theory of Riemann surfaces was begun by Riemann and continued by Liouville, Abel, Jacobi, Weierstrass, and others. This section discusses briefly the point of view in these studies, which began as an effort to solve a problem in real analysis, moved into complex analysis, and finally arrived at investigations of affine plane curves over $\mathbb{C}$, but from a point of view quite different from the one in Chapter VIII. The end result is a study of the curve through the functions on its zero locus, and the approach has something in common with the approach to algebraic number theory in Chapter VI. It is not necessary to understand the background in maximum generality, and we shall be content with suitable examples.

Riemann was interested in saying something useful about seemingly intractable integrals like the one arising from the arc length of an ellipse; let us take

$$y = y(x) = \int^x \frac{dt}{\sqrt{(t-a)(t-b)(t-c)}},$$

where a, b, c are distinct constants, as a specific example. The lower limit of integration is unimportant, since it affects the value of the integral only by an additive constant. We sketch an analysis of the integral,[1] proceeding formally for the moment. Although y as a function of x seems intractable, any sort of inverse function has nice properties. The formula for y gives us

$$dy = \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}},$$

and an inverse function $x = x(y)$ thus has derivative

$$\frac{dx}{dy} = \sqrt{(x-a)(x-b)(x-c)}.$$

Consequently we should expect that

$$\left(\frac{dx}{dy}\right)^2 = (x-a)(x-b)(x-c).$$

Of course, the singularities at a, b, c are problematic, and the square root might have a negative argument, depending on the location of x.

Riemann's starting point for a rigorous investigation was to let x be complex, rather than real, and to let the integral be taken over paths in $\mathbb{C}$. The result is then not an ordinary function $y(x)$, since the square root in the integrand is not a well-defined function for t in $\mathbb{C} - \{a, b, c\}$. We can make a choice for which the square root is well defined, however, as long as we restrict attention to a small neighborhood of a particular t. Thus we can visualize small overlapping disks each centered at a point along an arbitrary path of integration with t in $\mathbb{C} - \{a, b, c\}$ with the property that the integrand is well defined on each such

[1] For more details one can consult the author's book *Elliptic Curves*, pp. 165–183.

disk. The interpretation of the square root may be assumed to match on the intersection of any two disks. When a path goes around one or more of the singularities and we return to the same t, we view the new disk as the same as the old one if the values of the square root match, but as different if the values do not match. The union of the disks with this convention becomes a new domain of interest, and the function $F(t) = \sqrt{(t-a)(t-b)(t-c)}$ on $\mathbb{C} - \{a, b, c\}$ becomes a well-defined function $F(\zeta)$ on this new domain. This new domain is a relatively simple example of a **Riemann surface**, i.e., a connected 1-dimensional complex manifold.

In more modern language the new domain is a twofold covering of the three-times punctured plane $\mathbb{C} - \{a, b, c\}$, obtained as follows. We fix a base point z_0 in $\mathbb{C} - \{a, b, c\}$ and define a winding number for each of the points a, b, c as usual. The subset of the fundamental group of $\mathbb{C} - \{a, b, c\}$ for which the sum of the three winding numbers is even is a subgroup and corresponds, via standard covering-space theory, to a certain twofold covering space $\mathcal{R}$ of $\mathbb{C} - \{a, b, c\}$, the covering map being called e. This covering space is a new domain on which the integrand is well defined. On each fiber of the covering, e is two-to-one. Let ζ_0 be one of the two preimages of z_0. Let us adjoin points a^*, b^*, c^*, ∞^* to the covering space $\mathcal{R}$ and extend e by the definitions $e(a^*) = a, e(b^*) = b, e(c^*) = c$, $e(\infty^*) = \infty$. One can show that the complex structure extends from $\mathcal{R}$ to the enlarged space $\mathcal{R}^*$ in such a way that the extended e is a holomorphic function from $\mathcal{R}^*$ onto $\mathbb{C} \cup \{\infty\}$. The enlarged space $\mathcal{R}^*$ becomes a *compact* Riemann surface, and the extended e is a branched covering of the Riemann sphere $\mathbb{C} \cup \{\infty\}$. Topologically $\mathcal{R}^*$ turns out to be a torus, as we shall see in a moment.

Riemann in his own investigations went on to study the function theory of compact Riemann surfaces. The interest is in deciding whether there is a globally defined meromorphic function with poles/zeros only at chosen points and with poles/zeros at most/least of some specified order. If there is such a function, one wants to know the dimension of the space of such functions. The basic tool for addressing this question is the Riemann–Roch Theorem. In the context of Riemann surfaces, the Riemann–Roch Theorem has both an analysis aspect and an algebraic aspect. The analysis aspect may be viewed as using the theory of elliptic differential operators to prove existence of enough nonconstant meromorphic functions for the Riemann surface to acquire an algebraic structure. For the purposes of this book, we can just accept this circumstance and not try to extend it in any way; however, we will sketch in a moment how the algebraic structure can be obtained concretely for our example. The algebraic aspect may be viewed as mining this algebraic structure to deduce as many dimensionality relations as possible among the function spaces of interest. This is the theory that we shall want to extend; we return to our method for carrying out this project after producing the algebraic structure for our example by elementary means.

To introduce the algebraic structure in our example, we use our knowledge of $\mathcal{R}^*$ to make sense out of the expression

$$w(C) = \int_C F(\zeta)^{-1}\, d\zeta$$

for any piecewise smooth curve C on $\mathcal{R}^*$ that starts from the base point ζ_0. If C is given by $C(t)$ for t in an interval I, then this integral is to be equal to $w(C) = \int_{t\in I} F(C(t))(e\circ C)'(t)\, dt$. Let Γ_a, Γ_b, Γ_c be small loops in $\mathbb{C} - \{a, b, c\}$ respectively about a, b, c based at z_0, each having winding number 1, and define $\Gamma_1 = \Gamma_a\Gamma_b$ and $\Gamma_2 = \Gamma_b\Gamma_c$. Lift Γ_1 and Γ_2 to curves $\widetilde{\Gamma}_1$ and $\widetilde{\Gamma}_2$ in $\mathcal{R}^*$ based at ζ_0, and define

$$\omega_1 = \int_{\widetilde{\Gamma}_1} F(\zeta)^{-1}\, d\zeta \qquad \text{and} \qquad \omega_2 = \int_{\widetilde{\Gamma}_2} F(\zeta)^{-1}\, d\zeta.$$

It turns out that $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice in $\mathbb{C}$ and that there is a well-defined function $w : \mathcal{R}^* \to \mathbb{C}/\Lambda$ such that whenever ζ is in $\mathcal{R}^*$ and C is a piecewise smooth curve from ζ_0 to ζ, then $w(\zeta) \equiv w(C) \bmod \Lambda$. The function $w(\zeta)$ is one-one onto and is biholomorphic. In particular, $\mathcal{R}^*$ is exhibited as homeomorphic to a torus.

Let $w^{-1} : \mathbb{C}/\Lambda \to \mathcal{R}^*$ be the inverse function of w, and let $\mu : \mathbb{C} \to \mathbb{C}/\Lambda$ be the quotient map. Then the composition $P = e\circ w^{-1}\circ\mu$ carries $\mathbb{C}$ to $\mathbb{C}\cup\{\infty\}$ and can be seen to satisfy $P'^2 = (P-a)(P-b)(P-c)$. In other words, P has been constructed rigorously as an inverse function to the original integral. Except for small details, P is the Weierstrass $\wp$ function for the lattice Λ in $\mathbb{C}$. It is almost true that $z \mapsto (P(z), P'(z))$ is a parametrization of the zero locus of the affine plane curve $y^2 - (x-a)(x-b)(x-c)$ defined over $\mathbb{C}$. The sense in which this parametrization fails is that $P(z)$ takes on the value ∞ at certain points. What happens more precisely is that $z \mapsto [P(z), P'(z), 1]$ is a parametrization of the zero locus of the projective plane curve $Y^2W - (X - aW)(X - bW)(X - cW)$.

Our initial focus in this chapter is in mining this kind of algebraic-curve structure over $\mathbb{C}$ to deduce as many dimensionality relations as possible among interesting finite-dimensional subspaces of scalar-valued functions on the zero locus of the curve. For instance in the example above, one can ask for the dimension of the space of meromorphic functions on $\mathcal{R}^*$ with at worst simple poles at two specified points and with no other poles. The main theorem of this chapter, the Riemann–Roch Theorem, gives quantitative information about the dimension of this space and of similar spaces. The goal for this introduction is to frame this question as an algebra question about the algebraic structure and to see that some basic tools introduced in Chapter VI in the context of algebraic number theory are the appropriate tools to use here.

The primary object of study is the "function field" of the curve in question. Let us construct this function field for our example. The ideal

$$I = \big(Y^2 - (X-a)(X-b)(X-c)\big)$$

in $\mathbb{C}[X, Y]$ is prime, and the restrictions of all polynomial functions to its zero locus $V(I)$ may be identified with the integral domain $R = \mathbb{C}[X, Y]/I$ by the Nullstellensatz. It takes a little argument, which we omit, to justify saying that the meromorphic functions on the zero locus may be viewed as the field of fractions $\mathbb{F}$ of $\mathbb{C}[X, Y]/I$; suffice it to say for the moment that we insist that the behavior at all points of the locus, including any points on the line at infinity in the projective plane, be limited to poles and zeros, and that is why nonrational functions of (X, Y) do not appear. At any rate, $\mathbb{F}$ is what is taken as the function field of the curve. To have obtained a field by this construction, we could have started with any affine plane curve $f(X, Y)$ over $\mathbb{C}$ as in Chapter VIII, except that the principal ideal $(f(X, Y))$ in $\mathbb{C}[X, Y]$ has to be assumed to be prime to yield an integral domain as quotient. That is, $f(X, Y)$ has to be an irreducible polynomial; we say that the affine plane curve $f(X, Y)$ has to be assumed to be **irreducible** over $\mathbb{C}$.

The study of members of the function field $\mathbb{F}$ from the point of view of their poles and zeros is analogous to the problem of studying factorizations in the number-theoretic setting. This point was already made in Section VIII.7 of *Basic Algebra*, where the case of the affine plane curve above in which $(a, b, c) = (0, +1, -1)$ was studied in detail. For this one choice of (a, b, c), the integral domain $R = \mathbb{C}[X, Y]/I$ was observed to be the integral closure of $\mathbb{C}[X]$ in a finite separable extension of $\mathbb{C}(X)$, and it is a Dedekind domain by Theorem 8.54 of *Basic Algebra*; in fact, the same argument works for any choice of (a, b, c) as long as a, b, c are distinct complex numbers.

Unique factorization of elements into prime elements fails in this R, but we saw that a geometrically meaningful factorization instead is the factorization of nonzero ideals into prime ideals. This latter factorization is unique because R is a Dedekind domain. Meanwhile, since nonzero prime ideals are maximal in R, the Nullstellensatz shows[2] that the nonzero prime ideals in R correspond exactly to the points of the zero locus $V(I)$. Consequently the unique factorization of nonzero ideals in R has the geometric interpretation of associating orders of zeros and poles to members of R. This all seems very tidy, but there are at least three awkward matters that we need to take into account:

[2]Let $\varphi : \mathbb{C}[X, Y] \to R$ be the quotient homomorphism. If M is a maximal ideal in R, then $\varphi^{-1}(M)$ is a maximal ideal in $\mathbb{C}[X, Y]$ and hence is the set of all polynomials vanishing at some (x_0, y_0). To show that (x_0, y_0) is in $V(I)$, assume the contrary. Then there exists $g \in I$ with $g(x_0, y_0) \neq 0$. This g is not in the maximal ideal $\varphi^{-1}(M)$, and thus there exist $f \in \varphi^{-1}(M)$ and $h \in \mathbb{C}[X, Y]$ with $f + gh = 1$. Applying φ, we obtain $\varphi(f) = 1$, in contradiction to the fact that $\varphi(f)$ lies in the proper ideal M of R.

(i) we have not included information about zeros and poles at the points at infinity when the curve is viewed projectively, and that information surely plays some role,
(ii) the analysis of the function field $\mathbb{F}$ seems to rely on a subfield $\mathbb{C}(X)$ for which there is surely no canonical description,
(iii) the ring R no longer need be integrally closed if a, b, c are not assumed distinct, if for example $(a, b, c) = (0, 0, 1)$.

Point (ii) turns out to be an advantage, allowing us to work with the given curve from multiple perspectives. The "key observation" at the end of this section will make clear how we can take advantage of (ii).

Point (iii) is quite significant. The trouble with the curve $Y^2 - X^2(X-1)$ is that the curve has a singularity at $(0, 0)$ in the sense of Section VII.5. The maximal ideals of the ring $\mathbb{C}[X, Y]\big/\big(Y^2 - X^2(X-1)\big)$ correspond to points on the zero locus of the curve; but the ring is not a Dedekind domain, and we have few tools for working with it. To handle matters properly, we have to form the function field directly as $\mathbb{F} = \mathbb{C}(X)[Y]\big/\big(Y^2 - X^2(X-1)\big)$ and define R to be the integral closure of $\mathbb{C}[X]$ in $\mathbb{F}$. This ring R is bigger than $\mathbb{C}[X, Y]\big/\big(Y^2 - X^2(X-1)\big)$ and is a Dedekind domain. Unfortunately its nonzero prime ideals no longer correspond exactly to points of the zero locus. Example 1 below will illustrate. What happens is that $\mathbb{F}$ readily provides information about the behavior of nonsingular points of the zero locus but not about singular points. Problems 5–11 at the end of the chapter address this matter for nonsingular points for affine plane curves more generally. The tool for making the connection for curves in higher dimension is Zariski's Theorem (Theorem 7.23), and we shall carry out the details in Chapter X when we treat the *geometry* of curves, as opposed to the number theory.

Point (i) is relevant and is easily handled. When we form the function field of the curve and take R to be the integral closure of $\mathbb{C}[X]$ in it, we can associate $\mathbb{C}[X]$ with the polynomials of $\mathbb{C}$ and think of them as embedded in the field $\mathbb{C}(X)$ of rational functions. The rational functions are all meaningful on the Riemann sphere $\mathbb{C} \cup \{\infty\}$, and we study behavior of rational functions near ∞ by writing them in terms of X^{-1} and regarding X^{-1} as a new variable that is near 0. In studying our curve, the points in the projective plane that we miss by considering just the affine curve are the ones that lie over ∞ in the Riemann sphere. We study them by considering the integral closure R' of $\mathbb{C}[X^{-1}]$ in $\mathbb{F}$. If the curve is nonsingular at all points lying over ∞, then these points correspond to the prime ideals of R' whose intersection with $\mathbb{C}[X^{-1}]$ is the prime ideal $X^{-1}\mathbb{C}[X^{-1}]$ of $\mathbb{C}[X^{-1}]$.

EXAMPLES.

(1) Affine plane curve $f(X, Y) = Y^2 - X^2(X-1)$. This polynomial is irreducible over $\mathbb{C}$ but is singular at $(0, 0)$ in the sense that $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial X}$ both

vanish there. Let $\mathbb{F} = \mathbb{C}(X)[Y]/(f(X, Y))$, and let x and y be the images of X and Y in $\mathbb{F}$. These elements lie in the ring $S = \mathbb{C}[X, Y]/(f(X, Y))$, whose maximal ideals correspond to points on the zero locus by the Nullstellensatz. All members of S are of the form $a(x) + yb(x)$, where a and b are arbitrary polynomials in one variable. Any proper ideal in S containing x has to be of the form $(x, yc_1(x), \ldots, yc_n(x))$ for some polynomials $c_1, \ldots, c_n$. A little argument using the fact that $\mathbb{C}[x]$ is a principal ideal domain shows that the ideal is of the form $(x, yc(x))$. Using products of x and polynomials, we see that we can discard all terms of $c(x)$ but the constant term. Hence the ideal is either (x) itself or is (x, y). The ideal (x) is not prime, since $y \cdot y$ is in it and y is not in it. The ideal (x, y) is maximal and hence prime. Since $(x, y)^2 = (x^2, xy, y^2) = (x^2, xy)$ is properly contained in (x), (x) is not the product of prime ideals in S. Thus S is not a suitable ring for investigating poles and zeros of members of the field $\mathbb{F}$. By contrast, a little computation shows that the integral closure R of $\mathbb{C}[x]$ in $\mathbb{F}$ is generated as a $\mathbb{C}$ algebra by x and $x^{-1}y$. This is a Dedekind domain, and the decomposition of the ideal (x) in R as a product of prime ideals can be checked to be $(x) = (x, x^{-1}y + i)(x, x^{-1}y - i)$. A factor on the right does not consist of all functions vanishing at some $(0, y_0)$ lying on the zero locus. The only point $(0, y_0)$ on the zero locus is $(0, 0)$, and the two prime factors of (x) say something about derivatives at that point. This example will be considered further in Problems 21–22 at the end of the chapter.

(2) Affine plane curve $f(X, Y) = Y^2 - X^4 + 1$. This polynomial is irreducible over $\mathbb{C}$ and is nonsingular at every point of its zero locus in $\mathbb{C}^2$. Again we form the function field $\mathbb{F}$, the members x and y of it, and the ring $\mathbb{C}[X, Y]/(f(X, Y))$. Using the fact that $X^4 - 1$ is square free, we can check that this ring is the full integral closure R of $\mathbb{C}[x]$ in $\mathbb{F}$. The ring R is a Dedekind domain, and its elements are all expressions $a(x)$ and $yb(x)$, where $a(x)$ and $b(x)$ are polynomials. Moreover, we have $(y + x^2)(y - x^2) = y^2 - x^4 = (x^4 - 1) - x^4 = -1$. Consequently the elements $y \pm x^2$ are nonconstant units in R, and they cannot have zeros or poles on the zero locus of $f(X, Y)$ in $\mathbb{C}^2$. Thus knowledge of the orders of zeros and poles at every point of the zero locus of $f(X, Y)$ in $\mathbb{C}^2$ does not determine a member of R up to a constant factor. Instead, we have to take into account the behavior at any points at infinity on the zero locus in the projective plane $\mathbb{P}^2_{\mathbb{C}}$. To see what this set is, we convert $f(X, Y)$ into a homogeneous polynomial of degree 4, specifically into $F(X, Y, W) = Y^2W^2 - X^4 + W^4$, and then we look for points $[x, y, w]$ with $F(x, y, w) = 0$ and $w = 0$. These have $x = 0$ and thus come down to $[0, y, 0]$. In other words, there is only one point at infinity on the zero locus of the curve. It is singular because all three partial derivatives of F are 0 there. The fact that it is singular means that we should not expect the prime ideals lying over $x^{-1}\mathbb{C}[x^{-1}]$ in the integral closure R' of $\mathbb{C}[x^{-1}]$ in $\mathbb{F}$ to correspond to the points at infinity on the curve. We return to this example shortly.

All these matters begin to sound quite complicated to sort out, but magically there is a simple way of handling them: for an affine plane curve irreducible over $\mathbb{C}$, we work with the field $\mathbb{F}$ of rational functions for the curve, ignoring the geometry of the curve, and we consider all discrete valuations on this field that are 0 on $\mathbb{C}^\times$. Discrete valuations were discussed at length in Section VI.2. They depend only on $\mathbb{F}$, not on the choice of a subring for which $\mathbb{F}$ is the field of fractions. As will be seen in Chapter X, the full set of discrete valuations of $\mathbb{F}$ gives information about all potential nonsingular points for any affine curve with function field $\mathbb{F}$, not necessarily planar; there will even be such a curve whose extension to be defined projectively is everywhere nonsingular, and then the points on the zero locus of the curve in projective space will be in one-one correspondence with the discrete valuations of $\mathbb{F}$.

Let us review what Chapter VI tells us about discrete valuations in our setting. Let $f(X, Y)$ be an irreducible polynomial in $\mathbb{C}[X, Y]$, let $\mathbb{F}$ be the field $\mathbb{C}(X)[Y]/(f(X, Y))$, let x and y be the images of X and Y in $\mathbb{F}$, and let R be the integral closure of $\mathbb{C}[x]$ in $\mathbb{F}$. This is a Dedekind domain by Theorem 8.54 of *Basic Algebra*. Corollary 6.10 classifies the discrete valuations of $\mathbb{F}$ that are 0 on $\mathbb{C}^\times$. It shows that all but finitely many correspond to prime ideals in R. There are only finitely many others. Corollary 6.10 tells us that these other discrete valuations can be described in terms of the integral closure R' of $\mathbb{C}[x^{-1}]$ in $\mathbb{F}$; this is another Dedekind domain whose field of fractions is $\mathbb{F}$. The exceptional discrete valuations of $\mathbb{F}$ arise from those prime ideals of R' that occur in the decomposition of the ideal $x^{-1}R'$ into prime ideals of R'. Geometrically we may view these additional discrete valuations as associated in some way with points at infinity in a projective space, but we can proceed with algebraic manipulations of these discrete valuations without invoking the geometric interpretation or using projective space.

EXAMPLE 2, CONTINUED. We continue with the affine plane curve $Y^2 - X^4 + 1$, the prime ideal $I = (Y^2 - X^4 + 1)$, and the ring R given as the integral closure of $\mathbb{C}[X]$ in the field $\mathbb{F} = \mathbb{C}(X)[Y]/I$. Corollary 6.10 divides the discrete valuations of $\mathbb{F}$ that are 0 on $\mathbb{C}^\times$ into two kinds. The ones of the first kind are built from the nonzero prime ideals of R. Since $y \pm x^2$ are units in R, all of these valuations take the value 0 on $y \pm x^2$. The discrete valuations of the second kind are those appearing in the decomposition of the ideal $x^{-1}R'$ in the integral closure R' of $\mathbb{C}[x^{-1}]$ in $\mathbb{F}$. The element $x^{-2}y$ is in R' because it is a root of the polynomial $Y^2 - (1 - x^{-4})$ in $\mathbb{C}[x^{-1}][Y]$. Hence R' contains x^{-1} and $x^{-2}y$. On the other hand, the most general element of $\mathbb{F}$ is of the form $a(x^{-1})x^{-2}y + b(x^{-1})$, where a and b are rational expressions in one variable, and this is a root of the polynomial

$$Y^2 - 2b(x^{-1})Y + \big(b(x^{-1})^2 - a(x^{-1})^2(1 - x^{-4})\big).$$

For this element to be in R', the coefficients must be in $\mathbb{C}[x^{-1}]$. This means that $b(X)$ is a polynomial and that $a(X)^2(1 - X^4)$ is a polynomial. Since $1 - X^4$ has no repeated roots, the latter condition forces $a(X)$ to be a polynomial. Thus x^{-1} and $x^{-2}y$ generate R' as a $\mathbb{C}$ algebra. Define ideals in R' by

$$P_1 = (x^{-1}, x^{-2}y + 1) \qquad \text{and} \qquad P_2 = (x^{-1}, x^{-2}y - 1).$$

Then it is straightforward to check the decompositions

$$(x^{-1}) = P_1 P_2, \qquad (x^{-2}y + 1) = P_1^4, \qquad \text{and} \qquad (x^{-2}y - 1) = P_2^4.$$

Since $[\mathbb{F} : \mathbb{C}(x^{-1})] = 2$ and since x^{-1} is prime in $\mathbb{C}[x^{-1}]$, the ideal (x^{-1}) in R' is the product of at most two prime ideals, and it follows that P_1 and P_2 are prime ideals in R'. They are distinct because the difference of the respective second generators is a nonzero scalar. In view of Corollary 6.10, there are exactly two discrete valuations of $\mathbb{F}$ that are 0 on $\mathbb{C}^\times$ other than the ones coming from prime ideals of R, and these are the ones coming from the prime ideals P_1 and P_2 of R'. Let us call them v_1 and v_2. The above decompositions of principal ideals give $v_1(y + x^2) = v_1(x^{-1})^{-2} + v_1(x^{-2}y + 1) = (-2) + (+4) = +2$, whereas $v_1(y - x^2) = (-2) + (0) = -2$. Thus v_1 takes the distinct values 0, $+2$, and -2 on 1, $y + x^2$, and $y - x^2$. Similarly v_2 takes the values 0, -2, and $+2$ on these elements.

We shall work with those discrete valuations of the field of rational functions for the curve under study that are 0 on the base field. These are canonical, independent of our choice of some Dedekind domain whose field of fractions is the given field. However, making a choice of Dedekind domain is convenient for making calculations. Then we can consider the discrete valuations as of two kinds, and which discrete valuations are of which kind will depend on our choice of Dedekind domain.

Context for the study in this chapter. Having concluded that the object to investigate is the field of rational functions of our curve and that the tools include the discrete valuations, we can now consider the context in which we should work. Let $\Bbbk$ be any field, not necessarily algebraically closed. We want to work with the "function field" of a suitable kind of curve defined over $\Bbbk$. If I is an ideal in $\Bbbk[X_1, \ldots, X_n]$, then the ring $R = \Bbbk[X_1, \ldots, X_n]/I$ is an integral domain if and only if the ideal I is prime, and in this case the field of fractions $\mathbb{F}$ of R can be taken to be the associated function field. Thus we restrict attention to the case that I is prime. To bring in the notion that the curve is to be 1-dimensional, we recall from Theorem 7.22 that the integral domain R has Krull dimension 1 in the sense of Section VII.4 if and only if the field of fractions $\mathbb{F}$ has transcendence degree 1 over $\Bbbk$. In this case, $\mathbb{F}$ is finitely generated as a field over $\Bbbk$, with a finite set of generators consisting of the elements $x_j = X_j + I$ for $1 \le j \le n$. That is, $\mathbb{F}$ is a function field in one variable over $\Bbbk$.

Conversely if $\mathbb{F}$ is a function field in one variable over $\Bbbk$, then $\mathbb{F}$ is a finite algebraic extension of a simple transcendental extension $\Bbbk(x_1)$. Let us write it as $\mathbb{F} = \Bbbk(x_1)[x_2, \ldots, x_n]$ for some n. Form the polynomial ring $\Bbbk[X_1, \ldots, X_n]$ and the ring homomorphism of this ring into $\mathbb{F}$ that fixes $\Bbbk$ and sends X_j into x_j. The image of this homomorphism is an integral domain R whose field of fractions is $\mathbb{F}$, and the kernel is a prime ideal I such that $R \cong \Bbbk[X_1, \ldots, X_n]/I$. Theorem 7.22 tells us that R has Krull dimension 1.

We are led to the following definition. For any field $\Bbbk$ and any integer $n \geq 1$, an ideal I in $\Bbbk[X_1, \ldots, X_n]$ is called an **affine curve irreducible**[3] **over** $\Bbbk$ if I is prime and the integral domain $R = \Bbbk[X_1, \ldots, X_n]/I$ has Krull dimension 1. An affine plane curve $(f(X, Y))$ in the sense of Chapter VIII will be an object of this kind if $f(X, Y)$ is an irreducible polynomial.[4]

The geometry of the zero loci of the curves we study will not play a role in the mathematics of this chapter; only the field of fractions $\mathbb{F}$ and the base field $\Bbbk$ will. We postpone to Chapter X any discussion of the geometry.[5] For any function field $\mathbb{F}$ in one variable over an arbitrary field $\Bbbk$, we shall study in detail those discrete valuations of $\mathbb{F}$ that are 0 on $\Bbbk$. We refer to such discrete valuations as the **discrete valuations of** $\mathbb{F}$ **defined over** $\Bbbk$. It will be helpful as motivation to remember for the special case in which $\Bbbk$ is algebraically closed

- that the members of $\mathbb{F}$ may be viewed as all rational functions on the zero locus of an affine curve irreducible over $\Bbbk$,
- that the order-of-a-zero function at any nonsingular point of this zero locus gives an example of a discrete valuation of $\mathbb{F}$ defined over $\Bbbk$, and
- that all discrete valuations of $\mathbb{F}$ defined over $\Bbbk$ arise in this way if the zero locus is nonsingular at every point and we take into account points at infinity in projective space.

However, the formal development will not make use of these interpretations.

---

[3]Beware of assuming too much irreducibility about such a curve. Just because I is prime does not mean that I remains prime when we extend the scalars and work with an algebraic closure $\Bbbk_{\text{alg}}$ of $\Bbbk$. For example, $X^2 + Y^2$ is an affine curve irreducible over $\mathbb{R}$, but it factors as $(X + iY)(X - iY)$ over $\mathbb{C}$ and is therefore not irreducible over $\mathbb{C}$.

[4]This change of context for the word "curve" from the definition in Chapter VIII is appropriate because of a change of emphasis: we shall now be studying an associated function field rather than the defining ideal. The word "curve" will undergo a genuine change in meaning in Chapter X: because of the Nullstellensatz, classical algebraic geometry in the form to be discussed in much of Chapter X places emphasis on zero loci defined by prime ideals of polynomials over an algebraically closed field, and it will be convenient to define the curve to be the zero locus rather than the defining ideal.

[5]In Chapter X we shall introduce two distinct notions of sameness for the zero loci under the assumption that the field is algebraically closed, namely "isomorphism" and "birational equivalence." The first is a refinement of the second. Birational equivalence will turn out to mean that the function fields are isomorphic. An important theorem says that each birational equivalence class of irreducible curves contains one and only one isomorphism class of curves that are everywhere nonsingular in the sense of Section VII.5.

What to expect from the study. When $\Bbbk$ is not necessarily algebraically closed, these interpretations break down, at least to some extent. Yet the main theorem of the chapter, the Riemann–Roch Theorem, is still geared to the geometric interpretation of discrete valuations in terms of poles and zeros. One may reasonably ask why one goes to the trouble of working in such a general context that the theory no longer has its geometric interpretation. The answer is that the investigation is to be regarded as one in number theory, not in geometry. For example, studying an affine plane curve over a field $\mathbb{F}_p$ is the same as studying solutions of congruences in two variables modulo a prime. Studying such a curve over the p-adic field $\mathbb{Q}_p$ is the same as studying solutions of such congruences modulo arbitrary powers of p. The Riemann–Roch Theorem is actually the first serious aid in making this study. The present chapter therefore does not constitute such a study; it merely prepares one for such a study. In addition, there is a side benefit to understanding the number theory that arises this way: the methods and results of this subject and of algebraic number theory have enough in common that the methods and results for each suggest methods and results for the other.

An especially tantalizing example of this phenomenon concerns zeta functions. The zeros with $0 < \operatorname{Re} s \le 1$ for the Riemann zeta function, which is the meromorphic continuation to $\mathbb{C}$ of $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}$, influence the error term in the distribution of the primes as asserted by the Prime Number Theorem. The classical Riemann hypothesis is the statement that the only such zeros occur on the line $\operatorname{Re} s = \frac{1}{2}$; it implies a high level of control of this error term. There is a corresponding zeta function for any algebraic number field, and to it corresponds a version of the Riemann hypothesis appropriate for prime ideals for the number field. Proofs or counterexamples for these versions of the Riemann hypothesis have been sought for more than a century.

Meanwhile, one can formulate a Riemann hypothesis for any function field in one variable over any finite field, and again the statement has consequences for the distribution of prime ideals. This time, however, the Riemann hypothesis is a theorem, stated and proved by A. Weil in 1940. One might hope that the methods used for Weil's theorem could shed enough light on the classical Riemann hypothesis to lead to a proof, but to date this has not happened.

Key observation to be used during the study. In the next section we shall make systematic use of the following construction for any function field $\mathbb{F}$ in one variable over the field $\Bbbk$. If x is any element of $\mathbb{F}$ transcendental over $\Bbbk$, then the only discrete valuations of $\mathbb{F}$ defined over $\Bbbk$ that take a nonzero value on x may be described as follows. Let R be the integral closure of $\Bbbk[x]$ in $\mathbb{F}$, and let R' be the integral closure of $\Bbbk[x^{-1}]$ in $\mathbb{F}$. Then R and R' are Dedekind domains by Corollary 7.14, whether or not $\mathbb{F}$ is a separable extension of $\Bbbk(x)$. Both have $\mathbb{F}$ as field of fractions. Let the ideals xR of R and $x^{-1}R'$ of R' have

prime decompositions $xR = P_1^{e_1} \cdots P_g^{e_g}$ and $x^{-1}R' = Q_1^{e'_1} \cdots Q_{g'}^{e'_{g'}}$. Then the valuations v_{P_i} for $1 \le i \le g$ and v_{Q_j} for $1 \le j \le g'$ defined by P_i and Q_j have $v_{P_i}(x) = e_i$ and $v_{Q_j}(x) = -e'_j$, and no other discrete valuation of $\mathbb{F}$ that is defined over $\Bbbk$ takes a nonzero value on x. This observation follows from Corollary 6.10 and the definition of the discrete valuation associated with a nonzero prime ideal in a Dedekind domain.

2. Divisors

Let $\Bbbk$ be a field, and let $\mathbb{F}$ be a function field in one variable over $\Bbbk$. The first step is one of normalization: there is no loss of generality in replacing $\Bbbk$ by the larger field $\Bbbk'$ of all elements $\mathbb{F}$ that are algebraic over $\Bbbk$.[6]

Proposition 9.1. Let $\mathbb{F}$ be a function field in one variable over $\Bbbk$, and let $\Bbbk'$ be the subfield of all elements in $\mathbb{F}$ algebraic over $\Bbbk$. If x is in $\mathbb{F}^\times$, then every discrete valuation of $\mathbb{F}$ defined over $\Bbbk$ vanishes on x if and only if x is in $\Bbbk'$. Consequently $\mathbb{F}$ is automatically a function field in one variable over $\Bbbk'$, and as such, its discrete valuations defined over $\Bbbk'$ coincide with its discrete valuations defined over $\Bbbk$.

PROOF. If $x \in \mathbb{F}$ is transcendental over $\Bbbk$, then the observation at the end of Section 1 produces discrete valuations of $\mathbb{F}$ defined over $\Bbbk$ that take nonzero values on x. Conversely if $x \in \mathbb{F}^\times$ is algebraic over $\Bbbk$, we argue by contradiction. We may assume that $x \ne 0$. Suppose that v is a discrete valuation of $\mathbb{F}$ defined over $\Bbbk$ such that $v(x) \ne 0$. Possibly replacing x by x^{-1}, we may assume that $v(x) > 0$. Being nonzero algebraic over $\Bbbk$, x satisfies a polynomial equation

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = 0$$

with all $a_j \in \Bbbk$ and with $a_0 \ne 0$. For each j with $a_j \ne 0$, we have $v(a_j x^j) = v(a_j) + jv(x) = jv(x) > 0$. If $a_j = 0$, then $v(a_j x^j) = \infty > 0$. Thus $v(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x) > 0$. Since $v(a_0) = 0$, property (vi) of discrete valuations in Section VI.2 shows that

$$v\big((a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x) + a_0\big) = v(a_0) = 0 \ne \infty = v(0),$$

contradiction.

The conclusions in the last sentence of the proposition now follow: Since $\mathbb{F}$ is generated over $\mathbb{F}$ by finitely many elements $x_1, \ldots, x_n$, it is generated over $\Bbbk'$ by the same elements. Moreover, any element of $\mathbb{F}$ transcendental over $\Bbbk$ is transcendental over $\Bbbk'$, since $\Bbbk'$ is algebraic over $\Bbbk$. Thus $\mathbb{F}$ is a function field in one variable over $\Bbbk'$. The first paragraph of the proof shows that every discrete valuation of $\mathbb{F}$ defined over $\Bbbk$ is defined over $\Bbbk'$, and the converse statement is immediate from the definition. □

[6]The field $\Bbbk'$ is called the **field of constants** by some authors.

In accordance with Proposition 9.1, there is no loss of generality in replacing $\Bbbk$ by $\Bbbk'$ throughout. Changing notation, *we assume henceforth* that $\mathbb{F}$ is a function field in one variable defined over $\Bbbk$ and *that every element of* $\mathbb{F}$ *not in* $\Bbbk$ *is transcendental over* $\Bbbk$. These hypotheses will not be repeated for each result.

Suppressing $\Bbbk$ in the notation, we denote by $\mathbb{V}_\mathbb{F}$ the set of all discrete valuations of $\mathbb{F}$ defined over $\Bbbk$. A **divisor** is any member of the free abelian group $D_\mathbb{F}$ on $\mathbb{V}_\mathbb{F}$. Elements of $D_\mathbb{F}$ will be written additively,[7] and thus a typical member of $D_\mathbb{F}$ is

$$A = \sum_{v \in \mathbb{V}_\mathbb{F}} n_v v$$

with only finitely many of the integers n_v nonzero. We write $\operatorname{ord}_v A$ for the integer n_v, calling it the **order** of A at v. The identity element of $D_\mathbb{F}$ is called **zero** and is denoted by 0.

Each x in $\mathbb{F}^\times$ defines a **principal divisor** (x) by the formula

$$(x) = \sum_{v \in \mathbb{V}_\mathbb{F}} v(x) v.$$

We verify that (x) is indeed a divisor by showing that $v(x)$ is nonzero for only finitely many v in $\mathbb{V}_\mathbb{F}$. For x in $\Bbbk$, $v(x) = 0$ for all v. All other x are transcendental over $\Bbbk$, and the observation at the end of Section 1 shows that exactly $g + g'$ members of $\mathbb{V}_\mathbb{F}$ are nonzero on x, where g and g' are certain positive integers depending on x.

It is sometimes convenient to decompose (x) as a particular difference of two divisors, writing $(x) = (x)_0 - (x)_\infty$ with

$$(x)_0 = \sum_{\substack{v \in \mathbb{V}_\mathbb{F}, \\ v(x) > 0}} v(x) v \qquad \text{and} \qquad (x)_\infty = \sum_{\substack{v \in \mathbb{V}_\mathbb{F}, \\ v(x) < 0}} (-v(x)) v.$$

This notation is motivated by the interpretation of (x) for the case $\Bbbk = \mathbb{C}$, which is discussed in an example below.

Because of the formula $v(xy) = v(x) + v(y)$, the set of principal divisors is a subgroup $P_\mathbb{F}$ of $D_\mathbb{F}$, and the mapping $x \mapsto (x)$ is a group homomorphism of $\mathbb{F}^\times$ onto $P_\mathbb{F}$. The quotient $C_\mathbb{F} = D_\mathbb{F} / P_\mathbb{F}$ is called the group of **divisor classes** of $\mathbb{F}$ over $\Bbbk$.

EXAMPLE. $\Bbbk = \mathbb{C}$. This is the setting of a compact Riemann surface, provided we take for granted that every compact Riemann surface can be realized as a nonsingular projective curve over $\mathbb{C}$. The field $\mathbb{F}$ is the field of global meromorphic

[7] Some authors use a multiplicative notation.

functions on the surface. A principal divisor can be viewed as a compilation of the orders of the zeros and poles of a nonzero global meromorphic function: each member of $\mathbb{V}_{\mathbb{F}}$ corresponds to a point of the surface, and the order of a principal divisor (x) with $x \in \mathbb{F}^\times$ at a point is positive if the meromorphic function x has a zero at the point, negative if x has a pole there. It is known that the sum of the orders of all the zeros of a nonzero global meromorphic function equals the sum of the orders of all the poles. In the current framework the statement is that the sum over $v(x)$ is 0 for every $x \in \mathbb{F}^\times$ when $\Bbbk = \mathbb{C}$.

Theorem 9.3 will generalize the fact about compact Riemann surfaces that $\sum_{v \in \mathbb{V}_{\mathbb{F}}} v(x) = 0$ for every $x \in \mathbb{F}^\times$ when $\Bbbk = \mathbb{C}$. When $\mathbb{C}$ is replaced by a more general field that is not necessarily algebraically closed, Proposition 6.9 already shows that the terms $v(x)$ in the corresponding sum have to be weighted by certain integers in order to yield sum 0. These integers are dimensions that are shown to be finite in the next proposition.

Proposition 9.2. Let v be any discrete valuation of $\mathbb{F}$ defined over $\Bbbk$, let R_v be the valuation ring, and let P_v be the valuation ideal. Then R_v and P_v are $\Bbbk$ vector spaces, and $\dim_{\Bbbk} R_v/P_v$ is finite.

REMARKS. The integer $f_v = \dim_{\Bbbk} R_v/P_v$ is called the **residue class degree** of the valuation v. The proof gives a method for computing f_v, and we shall make use of this method shortly in proving Theorem 9.3.

PROOF. The fact that R_v and P_v are $\Bbbk$ vector spaces is immediate from Proposition 9.1. Since v is not identically zero, there exists some $x \in \mathbb{F}$ with $v(x) \neq 0$, and x is transcendental by Proposition 9.1. Possibly replacing x by x^{-1}, we may assume that $v(x) > 0$. The observation at the end of Section 1 classifies those members of $\mathbb{V}_{\mathbb{F}}$ taking positive values on x. In that notation we decompose $(x)R$ as $P_1^{e_1} \cdots P_g^{e_g}$, and v is the valuation defined by P_j for some j. Theorem 6.5e shows that $R_v/P_v \cong R/P_j$. Since x is prime in $\Bbbk[x]$, the general theory of extensions of Dedekind domains shows that $P_j \cap \Bbbk[x] = x\Bbbk[x]$ and that $f_j = \dim_{\Bbbk[x]/(x)}(R/P_j)$ is finite. The field $\Bbbk[x]/(x)$ is isomorphic to $\Bbbk$, and thus the dimension over $\Bbbk$ of $R_v/P_v \cong R/P_j$ is f_j. □

The **degree** of a divisor A is the integer $\deg A = \sum_{v \in \mathbb{V}_{\mathbb{F}}} f_v \operatorname{ord}_v(A)$, where f_v is the residue class degree of v as defined in the remarks with Proposition 9.2. Degree is a homomorphism of $D_{\mathbb{F}}$ into $\mathbb{Z}$. We shall prove in Theorem 9.3 that principal divisors have degree 0. This result extends Proposition 6.9, which handles the special case of the function field $\Bbbk(x)$. Theorem 9.3 may be regarded as a function-field analog of the Artin product formula (Theorem 6.51) for number fields, but the proof is much easier for function fields because we can take advantage of the observation at the end of Section 1.

Theorem 9.3. The degree of every principal divisor is 0. In more detail, if (x) is a principal divisor with x not in $\Bbbk$, then $\deg(x)_0 = \deg(x)_\infty = \dim_{\Bbbk(x)} \mathbb{F}$, and hence $\deg(x) = \deg(x)_0 - \deg(x)_\infty = 0$.

PROOF. If x is in $\Bbbk^\times$, then Proposition 9.1 shows that $v(x) = 0$ for every $v \in \mathbb{V}_\mathbb{F}$, and hence $\deg(x) = 0$. Thus we may assume that x is transcendental over $\Bbbk$. Applying the observation at the end of Section 1 and using the notation from there, we know that the only v's for which $v(x) \neq 0$ are the ones relative to the prime ideals P_i of R and the prime ideals Q_j of R' such that

$$xR = P_1^{e_1} \cdots P_g^{e_g} \qquad \text{and} \qquad x^{-1}R' = Q_1^{e'_1} \cdots Q_{g'}^{e'_{g'}}. \tag{$*$}$$

Moreover, $v_{P_i}(x) = e_i$ and $v_{Q_j}(x) = -e'_j$. In addition, the proof of Proposition 9.2 showed that the respective residue class degrees are the usual indices f_i and f'_j associated to the decompositions $(*)$. Thus

$$\deg(x)_0 = \sum_{i=1}^{g} f_i e_i \qquad \text{and} \qquad \deg(x)_\infty = \sum_{j=1}^{g'} f'_j e'_j.$$

Two applications of Theorem 9.60 of *Basic Algebra* show that

$$\sum_{i=1}^{g} f_i e_i = \dim_{\Bbbk(x)} \mathbb{F} \qquad \text{and} \qquad \sum_{j=1}^{g'} f'_j e'_j = \dim_{\Bbbk(x^{-1})} \mathbb{F}.$$

Thus $\deg(x)_0 = \dim_{\Bbbk(x)} \mathbb{F}$, and $\deg(x)_\infty = \dim_{\Bbbk(x^{-1})} \mathbb{F}$. The theorem therefore follows from the fact that $\Bbbk(x) = \Bbbk(x^{-1})$. □

Let $D_{\mathbb{F},0}$ be the subgroup of all divisors of degree 0. Theorem 9.3 shows that $P_\mathbb{F} \subseteq D_{\mathbb{F},0}$. The quotient $C_{\mathbb{F},0} = D_{\mathbb{F},0}/P_\mathbb{F}$ is therefore a subgroup of $C_\mathbb{F} = D_\mathbb{F}/P_\mathbb{F}$ and is the group of all divisor classes of degree 0. This is a function-field analog of the class group for an algebraic number field; it can be shown to be finite if $\Bbbk$ is a finite field but it not if $\Bbbk$ is an arbitrary field.

3. Genus

In this section, $\mathbb{F}$ denotes a function field in one variable over a field $\Bbbk$, and we assume that every element of $\mathbb{F}$ outside $\Bbbk$ is transcendental over $\Bbbk$. We continue with the notation $\mathbb{V}_\mathbb{F}$, $D_\mathbb{F}$, f_v, $\operatorname{ord}_v A$, $\deg A$, and (x) for $x \in \mathbb{F}^\times$, all as in Section 2.

If we were studying only what happens with $\Bbbk = \mathbb{C}$, we would be interested in the vector space of all meromorphic functions whose poles are limited to a certain finite set of points and are limited to some particular order at each of those

points. The underlying compact Riemann surface is an ordinary closed orientable 2-dimensional manifold, and the dimensions of these spaces of meromorphic functions turn out to control the genus of this manifold. For general $\mathbb{k}$, we study the natural generalization of this situation.[8] The vector spaces of interest are defined in terms of divisors, and we will be led to a natural definition of genus of the curve under study.

We introduce a partial ordering on $D_{\mathbb{F}}$ by saying that two divisors A and B have $A \le B$ if $\operatorname{ord}_v A \le \operatorname{ord}_v B$ for all $v \in \mathbb{V}_{\mathbb{F}}$. The inequality $B \ge A$ is to mean the same thing as $A \le B$. If $A \le B$ and $A' \le B'$, then $A + A' \le B + B'$ because $\operatorname{ord}_v(A + A') = \operatorname{ord}_v A + \operatorname{ord}_v A' \le \operatorname{ord}_v B + \operatorname{ord}_v B' = \operatorname{ord}_v(B + B')$. If $A \le B$, then $-A \ge -B$.

For each divisor A, we shall study the $\mathbb{k}$ vector space

$$L(A) = \{0\} \cup \big\{x \in \mathbb{F}^\times \mid (x) \ge -A\big\} = \big\{x \in \mathbb{F} \mid v(x) \ge -\operatorname{ord}_v A\big\}.$$

For $x \ne 0$, we can think of $v(x)$ as telling the order of the zero of x at a point corresponding to v. In that spirit, if $A \ge 0$, then $L(A)$ consists of all functions whose poles are limited to the set of v's for which $\operatorname{ord}_v A \ne 0$, with the order of the pole bounded above by the number $\operatorname{ord}_v A$. For general A, a similar interpretation is valid, except that the members of $L(A)$ are required also to vanish at certain points at least to certain orders.

We shall suppress any name for the function that embeds $\mathbb{V}_{\mathbb{F}}$ in $D_{\mathbb{F}}$. Thus for example if v_0 is in $\mathbb{V}_{\mathbb{F}}$, then $L(v_0)$ refers to $L(A)$ for the divisor A such that $\operatorname{ord}_{v_0} A = 1$ and $\operatorname{ord}_v A = 0$ when $v \ne v_0$.

Corollary 9.4. $L(0) = \mathbb{k}$, and $L(A) = 0$ if A is a nonzero divisor with $A \le 0$.

PROOF. If $A \le 0$ is nontrivial and if $x \in \mathbb{F}^\times$ were to have $(x) \ge -A$, then we would have $\deg(x) \ge -\deg A > 0$, in contradiction to the conclusion $\deg(x) = 0$ of Theorem 9.3. Thus $L(A) = 0$. Next, we have

$$L(0) = \big\{x \in \mathbb{F}^\times \mid v(x) = 0 \text{ for all } x\big\} \cup \bigcup_{v \in \mathbb{V}_{\mathbb{F}}} L(-v).$$

The first term on the right side is $\mathbb{k}^\times$, and the second term gives 0 by what we have just proved. Hence $L(0) = \mathbb{k}$. □

If $A \le B$, then it follows from the definition that $L(A) \subseteq L(B)$. We shall be interested in how much $L(B)$ increases when B increases. This change is measured by what happens to the quotient space $L(B)/L(A)$. The key case is that $B = A + v_0$ for some $v_0 \in \mathbb{V}_{\mathbb{F}}$, and we treat that in the following lemma.

[8] In doing so, we follow the approach in the book by Villa Salvador, Chapter 3, but with different notation.

Lemma 9.5. If A is a divisor and v_0 is in $\mathbb{V}_{\mathbb{F}}$, then

$$\dim_{\Bbbk} L(A + v_0)/L(A) \le f_{v_0} = \deg v_0.$$

PROOF. Put $f = f_{v_0}$, let R_{v_0} be the valuation ring of v_0, and let P_{v_0} be the valuation ideal of v_0. Since v_0 carries $\mathbb{F}^\times$ onto $\mathbb{Z}$, we can choose an element $y \in \mathbb{F}^\times$ with $v_0(y) = \operatorname{ord}_{v_0}(A + v_0)$.

Let $f + 1$ members $x_1, \dots, x_{f+1}$ of $L(A + v_0)$ be given. We shall produce an equation of linear dependence among the cosets $x_i + L(A)$, and this will prove the lemma. Computation gives

$$v_0(x_i y) = v_0(x_i) + v_0(y) = v_0(x_i) + \operatorname{ord}_{v_0}(A + v_0) \ge 0$$

for $1 \le i \le f + 1$, since x_i is in $L(A + v_0)$. Hence $x_i y$ is in R_{v_0}. Since $\dim_{\Bbbk}(R_{v_0}/P_{v_0}) = f$, there exist members $c_1, \dots, c_{f+1}$ of $\Bbbk$ not all 0 such that $\sum_{i=1}^{f+1} c_i(x_i y + P_{v_0}) = P_{v_0}$, i.e., such that $\sum_{i=1}^{f+1} c_i x_i y$ lies in P_{v_0}. Then $\sum_{i=1}^{f+1} c_i x_i$ lies in $y^{-1} P_{v_0}$, and

$$v_0\Big(\sum_{i=1}^{f+1} c_i x_i\Big) \ge -v_0(y) + 1 = -\operatorname{ord}_{v_0}(A + v_0) + 1 = -\operatorname{ord}_{v_0} A. \qquad (*)$$

Since each x_i is in $L(A + v_0)$, so is $\sum_{i=1}^{f+1} c_i x_i$. This fact and $(*)$ together show that $\sum_{i=1}^{f+1} c_i x_i$ is in $L(A)$, i.e., that $\sum_{i=1}^{f+1} c_i x_i + L(A)$ is the 0 coset. This proves the desired linear dependence and shows that $\dim_{\Bbbk} L(A + v_0)/L(A) \le f$. □

Theorem 9.6. If A and B are divisors such that $A \le B$, then $L(B)/L(A)$ is finite-dimensional over $\Bbbk$ with

$$\dim_{\Bbbk} L(B)/L(A) \le \deg B - \deg A.$$

Moreover, $L(A)$ and $L(B)$ are separately finite-dimensional over $\Bbbk$, and consequently

$$\dim_{\Bbbk} L(B) - \deg B \le \dim_{\Bbbk} L(A) - \deg A.$$

REMARKS. We define $\ell(A) = \dim_{\Bbbk} L(A)$. This is finite by the theorem, and the resulting inequality of the theorem is that

$$\ell(B) - \deg B \le \ell(A) - \deg A.$$

PROOF. The first conclusion is immediate from Lemma 9.5 by induction on $\sum_v (\operatorname{ord}_v B - \operatorname{ord}_v A)$. Fixing a reference point v_0 in $\mathbb{V}_{\mathbb{F}}$ and taking $A =$

$\sum_{\mathrm{ord}_v B \le 0}(\mathrm{ord}_v B)v - v_0$ and applying Corollary 9.4 to A, we see that $L(A) = 0$. Therefore the first conclusion specializes to

$$\dim_{\Bbbk} L(B) - \deg B \le -\deg A.$$

Since $\dim_{\Bbbk} L(B)$ is certainly nonnegative, this inequality implies that $L(B)$ is finite-dimensional. Then we can expand the left side of the first conclusion of the theorem to obtain

$$\dim_{\Bbbk} L(B) - \dim_{\Bbbk} L(A) = \deg B - \deg A,$$

and the proof is complete. □

The theorem identifies $\ell(B) - \deg B$ as a quantity of interest when we are trying to understand a divisor B. We shall undertake a study of this quantity, beginning first with the case of a divisor B equal to a multiple of the pole part $(x)_\infty$ of a principal divisor (x). Recall that the signs are arranged to have $(x)_\infty \ge 0$.

Lemma 9.7. For each x in $\mathbb{F}$ that is not in $\Bbbk$, there exists a constant C_x such that the multiple $p(x)_\infty$ of $(x)_\infty$ satisfies

$$\ell\big(p(x)_\infty\big) - \deg\big(p(x)_\infty\big) \ge C_x$$

for every integer p.

PROOF. Applying the observation at the end of Section 1, we form the integral closure R of $\Bbbk[x]$ in $\mathbb{F}$ and the integral closure R' of $\Bbbk[x^{-1}]$ in $\mathbb{F}$. The discrete valuations v for which $v(x) < 0$ are exactly those arising from prime ideals in the prime decomposition of $x^{-1}\Bbbk[x^{-1}]$, according to Corollary 6.10. Specifically the ideal $x^{-1}\Bbbk[x^{-1}]$ in R' decomposes as a product $Q_1^{e'_1} \cdots Q_{g'}^{e'_{g'}}$, and the corresponding discrete valuations have $v_{Q_k}(x^{-1}) = e'_k$. Theorem 9.3 shows that $\deg(x)_\infty = \dim_{\Bbbk(x)} \mathbb{F}$.

Let $n = \dim_{\Bbbk(x)} \mathbb{F}$. Choose a basis $y_1, \dots, y_n$ of $\mathbb{F}$ over $\Bbbk(x)$ consisting of members of R. Each v arising from a prime ideal of R has $v(y_j) \ge 0$ for $1 \le j \le n$ by Proposition 6.7. The remaining v's all have $v(x) < 0$, and therefore there exists an integer $k \ge 0$ such that $v(y_j) \ge kv(x)$ for $1 \le j \le n$ and for all these remaining v's. For this value of the integer k, the elements $y_1, \dots, y_n$ all lie in $L(k(x)_\infty)$.

Let $m \ge 0$ be arbitrary. The v's coming from some Q_k, i.e., those with $v(x) < 0$, have $v(x^i) \ge v(x^m)$ whenever $0 \le i \le m$, and the remaining v's, i.e., those with $v(x) \ge 0$, all have $v(x^i) \ge 0$ for $0 \le i \le m$. Therefore $1, x, x^2, \dots, x^m$ all lie in $L((x^m)_\infty) = L(m(x)_\infty)$.

Multiplying, we see that $x^i y_j$ lies in $L\big((k+m)(x)_\infty\big)$ for $0 \le i \le m$ and $1 \le j \le n$. These elements $x^i y_j$ are linearly independent over $\Bbbk$, and therefore

$$\ell\big((k+m)(x)_\infty\big) \ge (m+1)n = (m+1)\deg(x)_\infty.$$

Since deg is a homomorphism from $D_{\mathbb{F}}$ into $\mathbb{Z}$,

$$\deg\big((k+m)(x)_\infty\big) = (k+m)\deg(x)_\infty.$$

Therefore each $m \ge 0$ has

$$\begin{aligned}\ell\big((k+m)(x)_\infty\big) - \deg\big((k+m)(x)_\infty\big) &\ge (m+1-k-m)\deg(x)_\infty \\ &= (1-k)\deg(x)_\infty.\end{aligned}$$

We have therefore proved that

$$\ell(q(x)_\infty) - \deg(q(x)_\infty) \ge (1-k)\deg(x)_\infty$$

for all integers q that are sufficiently positive. If p is any integer, we can find q as above with $p \le q$. Then $p(x)_\infty \le q(x)_\infty$, and Theorem 9.6 shows that

$$(1-k)\deg(x)_\infty \le \ell(q(x)_\infty) - \deg(q(x)_\infty) \le \ell(p(x)_\infty) - \deg(p(x)_\infty).$$

This proves the lemma with $C_x = (1-k)\deg(x)_\infty$. □

Lemma 9.8. If A is any divisor and x is any member of $\mathbb{F}^\times$, then $L((x)+A) \cong L(A)$ canonically. Therefore $\ell((x)+A) = \ell(A)$. In addition, $\deg((x)+A) = \deg A$.

PROOF. Define a $\Bbbk$ linear mapping $\varphi : L(A) \to \mathbb{F}$ by $\varphi(y) = x^{-1}y$. This is certainly one-one, and its image is contained in $L((x)+A)$ because any nonzero z in $L(A)$ has $(z) \ge -A$ and then also $(x^{-1}z) = -(x)+(z) \ge -(x)-A$. Similarly $\psi(y) = xy$ is one-one and carries $L((x)+A)$ into $L(A)$. By inspection, $\psi\varphi = 1$ and $\varphi\psi = 1$. Therefore $L((x)+A)$ and $L(A)$ are canonically isomorphic and have the same dimension over $\Bbbk$. For the last conclusion, $\deg((x)+A) = \deg(x) + \deg A = \deg A$ by Theorem 9.3. □

Theorem 9.9 (Riemann's inequality). For each x in $\mathbb{F}$ that is not in $\Bbbk$, let g_x be the integer such that $1 - g_x$ is the largest possible C_x with

$$\ell\big(p(x)_\infty\big) - \deg\big(p(x)_\infty\big) \ge C_x$$

for every integer p. Then

(a) the integer $g = g_x$ is independent of x,
(b) g is ≥ 0,
(c) $\ell(A) - \deg A \ge 1 - g$ for every divisor A.

REMARKS. The integer g_x in the theorem exists by Lemma 9.7. Once it has been proved to be an integer g independent of x, it is called the **genus** of the function field $\mathbb{F}$ over $\Bbbk$.

PROOF. We begin by proving (c) with g replaced by g_x. Let C_x be any integer with the property that $\ell(p(x)_\infty) - \deg(p(x)_\infty) \geq C_x$ for all p. If a divisor A is given, we can write $A = A_0 - A_\infty$, where $A_0 = \sum_{\operatorname{ord}_v A>0} (\operatorname{ord}_v A)v$ and $A_\infty = \sum_{\operatorname{ord}_v A<0} (-\operatorname{ord}_v A)v$. Then $A \leq A_0$, and Theorem 9.6 shows that $\ell(A) - \deg A \geq \ell(A_0) - \deg A_0$. Thus it is enough to prove (c) for A_0. Let p be any integer ≥ 0. Since $A_0 \geq 0$, we have $p(x)_\infty - A_0 \leq p(x)_\infty$. Hence a second application of Theorem 9.6 shows that

$$\ell\big(p(x)_\infty - A_0\big) - \deg\big(p(x)_\infty - A_0\big) \geq \ell\big(p(x)_\infty\big) - \deg\big(p(x)_\infty\big) \geq C_x.$$

Since deg is a homomorphism, this inequality implies that

$$\ell\big(p(x)_\infty - A_0\big) \geq C_x + p\deg(x)_\infty - \deg A_0.$$

Fix an integer p large enough for the right side to be positive. For this p, the vector space $L(p(x)_\infty - A_0)$ is nonzero; let y be a nonzero member of it. This y has $(y) \geq -(p(x)_\infty - A_0)$, and hence $p(x)_\infty \geq A_0 - (y)$. A third application of Theorem 9.6, in combination with Lemma 9.8, shows that

$$\begin{aligned}\ell\big(p(x)_\infty\big) - \deg\big(p(x)_\infty\big) &\leq \ell(A_0 - (y)) - \deg(A_0 - (y)) \\ &= \ell(A_0) - \deg A_0.\end{aligned}$$

The left side is $\geq C_x$, and hence $\ell(A_0) - \deg A_0 \geq C_x$. Therefore

$$\ell(A) - \deg A \geq C_x \tag{$*$}$$

for every divisor A. Since one choice of C_x is $1 - g_x$, this proves (c).

Taking $A = p(y)_\infty$, we see that the best C_y has $C_y \geq C_x$. Since the roles of x and y can be interchanged, this proves (a). Finally if we take $A = 0$ in (c) and apply Corollary 9.4, we see that $1 - 0 \geq 1 - g$. Thus $g \geq 0$. This proves (b). □

EXAMPLES OF GENUS.

(1) $\mathbb{F} = \Bbbk(x)$ for a transcendental x. In the proof of Lemma 9.7, we have $n = 1$ and can take $y_1 = 1$. Then $k = 0$, and the proof of the lemma shows that the inequality of the lemma holds with $C_x = (1 - 0)\deg(x)_\infty = 1$. Therefore $1 - g \geq C_x = 1$, and $g \leq 0$. So $g = 0$ by Theorem 9.9b.

(2) $\mathbb{F} = \mathbb{C}[x, y]/(y^2 - x^4 + 1)$. This example was discussed in Section 1, and we have $x^{-1}R' = P_1P_2$ with $P_1 = (x^{-1}, x^{-2}y + 1)$ and $P_2 = (x^{-1}, x^{-2}y - 1)$. The corresponding valuations therefore have $v_{P_1}(x) = v_{P_2}(x) = -1$. Meanwhile, the elements 1 and y form a basis of $\mathbb{F}$ over $\Bbbk(x)$. The element 1 has $v_{P_1}(1) = v_{P_2}(1) = 0$; so 1 is in $L(p(x)_\infty)$ for every $p \geq 0$. Since $x^{-2}y$ is the sum of a generator of P_1 and a generator of P_2, $x^{-2}y$ lies in R'. Write $(x^{-2}y) = I_1 \cdots I_l$, where each I_j is a prime ideal in R'. Since $x^{-2}y$ and P_1 together generate 1, P_1 is not one of the ideals I_j. Similarly P_2 is not one of the I_j's. Thus $(y) = (x^{-1})^{-2}(x^{-2}y) = (P_1P_2)^{-2}I_1 \cdots I_l$, and we obtain $v_{P_1}(y) = v_{P_2}(y) = -2$. Hence y lies in $L(2(x)_\infty)$, and we can take $k = 2$ in the proof of Lemma 9.7. For this k, we have $C_x = (1 - 2)\deg(x)_\infty = -2$. Therefore $1 - g \geq C_x = -2$, and $g \leq 3$. In fact, $g = 1$ here, as a special case of the next example. Thus a routine use of the estimate from Lemma 9.7 has its limitations.

(3) $\mathbb{F} = \Bbbk[x, y]/(y^2 - p(x))$, where $p(x)$ is a square-free polynomial of degree m and $\Bbbk$ has characteristic $\neq 2$. Then $g = \frac{1}{2}m - 1$ if m is even and $g = \frac{1}{2}(m - 1)$ if m is odd. This computation will be carried out in Problems 12–20 at the end of the chapter.

Theorem 9.9 gives the lower bound of $1 - g$ for $\ell(A) - \deg A$ for all divisors A. There is also an upper bound, with the proviso that $L(A) \neq 0$.

Proposition 9.10. If A is any divisor such that $L(A) \neq 0$, then

$$\ell(A) - \deg A \leq 1.$$

Hence any divisor A with $\deg A \leq -1$ has $\ell(A) = 0$.

PROOF. Let y be a member of $\mathbb{F}^\times$ that lies in $L(A)$. Then every $v \in \mathbb{V}_\mathbb{F}$ has $v(y) \geq -\operatorname{ord}_v A$ and hence $0 \geq -\operatorname{ord}_v A - v(y) = -\operatorname{ord}_v(A + (y))$. This inequality says that $A + (y) \geq 0$. Then Corollary 9.4 and Theorem 9.6 together give

$$1 = \ell(0) - \deg 0 \geq \ell(A + (y)) - \deg(A + (y)),$$

and the right side equals $\ell(A) - \deg A$ by Lemma 9.8. Then $1 - \deg A \leq \ell(A) - \deg A \leq 1$, and we must have $\deg A \geq 0$ whenever $\ell(A) \geq 1$. □

4. Riemann–Roch Theorem

Riemann's inequality, proved in Section 3, shows that every divisor A satisfies $\ell(A) - \deg A \geq 1 - g$, where g is the genus of the curve in question. The Riemann–Roch Theorem, to be proved in the present section, gives an interpretation for the difference between the two sides of the inequality.

In the classical setting of compact Riemann surfaces, the proof of the Riemann–Roch Theorem makes use of meromorphic differential forms, sometimes called abelian differentials by complex analysts. Meromorphic differential forms are objects that locally look like $f(z)\,dz$, where z is a local coordinate and $f(z)$ is a meromorphic function, and that fit together to be globally defined on the complex manifold. What the formula $f(z)\,dz = g(w)\,dw$ for fitting together means that in the overlap of the regions for two local coordinates z and w, $f(z)\,dz = g(w(z))\,\frac{dw}{dz}\,dz$ holds and hence $f(z) = g(w(z))\,\frac{dw}{dz}$. In the language of differential geometry, a meromorphic differential form is a meromorphic section of the cotangent bundle of the complex manifold. An important step that has to be carried out to make these differential forms useful is to prove a version of the Residue Theorem. This theorem says that the sum over all points of the manifold of the residues of the differential form is 0, the residue of $f(z)\,dz$ at the point corresponding to $z = 0$ being the coefficient of z^{-1} in the Laurent expansion[9] of $f(z)$ about 0. Once this theorem is in hand, one can begin to prove the Riemann–Roch Theorem.

In our present setting with the function field $\mathbb{F}$ in one variable over $\Bbbk$, it is not too hard to define an analog of meromorphic differential forms and to establish that they behave the way one would expect from differential calculus. In order to make use of these forms, one has to prove an analog of the Residue Theorem, and doing so requires some hard work. A. Weil discovered that this construction could be bypassed and that one could prove the theorem directly. The idea is to introduce the tool that differential forms make available and to skip the differential forms themselves.

It is worth understanding this background in a little more detail because otherwise the proof below may seem very strange indeed. To fix the ideas for this background only, suppose that the base field $\Bbbk$ is algebraically closed. Let us recall that elements of $\mathbb{V}_{\mathbb{F}}$ are meant to correspond to points of a zero locus in projective space, at least when the curve is everywhere nonsingular. We write this correspondence as $v \mapsto p(v)$. A local coordinate about $p(v)$ is denoted by a symbol like z classically, and in the setup with valuations, it is simply a member of the valuation ideal of v with $v(z) = 1$. A differential form that is given locally by classical expressions like $f(z)\,dz$ attaches to each v in $\mathbb{V}_{\mathbb{F}}$ the function $g_v \mapsto \text{Residue}_{p(v)}(g_v f\,dz)$, where g_v is any Laurent expansion about $p(v)$.

Classically this Laurent expansion is to be convergent in some deleted neighborhood of $p(v)$, and it involves only finitely many negative powers of the local coordinate. The assumption that it converges is not important because if $v(f) = n$, then the only powers of z whose coefficients in g_v affect the residue at $p(v)$ are the k^{th} powers for $k + n \le -1$. Thus the assumption on g_v is that it is

[9] One has to show that this coefficient is independent of the choice of the local coordinate.

a member of the Laurent series field $\Bbbk((z))$. To compute the residue for $g_v f\,dz$, we need to know how to interpret $f(z)$ as a Laurent series about $p(v)$. Let R_v be the valuation ring of v, and let P_v be the valuation ideal. The field R_v/P_v is a finite extension of $\Bbbk$ and must be isomorphic to $\Bbbk$ because $\Bbbk$ is algebraically closed. For each $c \in \Bbbk$, choose a member $a_c \in R_v$ such that the coset $a + P_v$ corresponds to c; we may assume that $a_0 = 0$. Denote the set of these elements a_c by $R_\Bbbk$. If $v(f) = n$, then $h = z^{-n} f$ is in R_v, and thus some unique a_0 in $R_\Bbbk$ has the property that $h - a_0$ is in P_v. Hence $z^{-1}(h - a_0)$ is in R_v, and some unique a_1 in $R_\Bbbk$ has the property that $z^{-1}(h - a_0) - a_1$ is in P_v. From this, $z^{-1}(z^{-1}(h - a_0) - a_1)$ is in R_v, and we can continue to subtract members of $R_\Bbbk$ and divide by z in this way. The result is that $h = a_0 + a_1 z + a_2 z^2 + \cdots$ in the sense that $v(h - a_0 - a_1 z - \cdots - a_k z^k) \geq k + 1$ for every k. Therefore $f = z^n h = z^n(a_0 + a_1 z + a_2 z^2 + \cdots)$. If we replace each a_k by the corresponding member c_k of $\Bbbk$, then $z^n(c_0 + c_1 z + c_2 z^2 + \cdots)$ is the member of $\Bbbk((z))$ that we associate to f.

With this identification in place, we can regard the given differential form as yielding a $\Bbbk$ linear function

$$\text{Residue} : \prod_{v \in \mathbb{V}_\mathbb{F}} \Bbbk((z)) \to \prod_{v \in \mathbb{V}_\mathbb{F}} \Bbbk.$$

We want to cut down the domain of this mapping so the sum of the residues is meaningful for every member of the image. The local expressions $f(z)\,dz$ involve only finitely many poles in a neighborhood of each point, and compactness implies that there are only finitely many such points globally. Except at these points the residue of $g_v f\,dz$ can be nonzero only if g_v has a pole at $p(v)$. Thus we can ensure that the sum of the residues is meaningful if we assume that $v(g_v) \geq 0$ except for finitely many v.

For algebraic purposes the domain is still unnecessarily large. Since each local coordinate in the algebraic realization is actually a member of $\mathbb{F}$, the only members of $\Bbbk((z))$ that we need to handle at each point are the members of $\mathbb{F}$. So let $\mathcal{A}_\mathbb{F}^* = \prod_{v \in \mathbb{V}_\mathbb{F}} \mathbb{F}$, and let $\mathcal{A}_\mathbb{F}$ be the $\Bbbk$ subspace of all members $\{g_v\}$ of the product such that $v(g_v) < 0$ only finitely often. Then the differential form gives us a $\Bbbk$ linear functional

$$\text{Sum of Residues} : \mathcal{A}_\mathbb{F} \to \Bbbk.$$

We have seen that if the differential form is given by $f(z)\,dz$ locally near $p(v)$ and if $v(g_v) \geq -v(f)$, then the residue is 0 at $p(v)$. Hence there is some divisor A, depending on the differential form, such that if $v(g_v) \geq -\operatorname{ord}_v A$ for all $v \in \mathbb{V}_\mathbb{F}$, then all residues are 0 and the sum of the residues is 0. Consequently the kernel of the sum-of-residues map associated to the differential form contains all tuples $\{g_v\}$ of $\mathcal{A}_\mathbb{F}$ such that $v(g_v) \geq -\operatorname{ord}_v A$ for this divisor A and all v.

Finally there is one more classical fact to bring into play. This is the Residue Theorem itself, saying that the sum of the residues is zero for any meromorphic differential form. If $\{g_v\}$ is actually a constant tuple with $g_v = h$ for some $h \in \mathbb{F}$, then the sum-of-residues map as defined above is giving us the classical sum of residues for the product of h and the given differential form. This sum is zero. In other words, every member of the diagonally embedded $\mathbb{F}$ in $\mathcal{A}_\mathbb{F}$ lies in the kernel of the sum-of-residues map associated to the differential form.

Weil's idea in a nutshell is that instead of developing differential forms, working with residues, and proving the consequence of the Residue Theorem, one should just start with any abstract linear functional on $\mathcal{A}_\mathbb{F}$ that satisfies the conditions that we noted above. Then the Riemann–Roch Theorem drops out fairly easily. This is the approach we shall follow. The abstract kind of linear functional on $\mathcal{A}_\mathbb{F}$ will be called a "differential" in what follows, as a reminder of the classical object that lies behind it.[10]

Without further ado, we proceed with the Riemann–Roch Theorem. In this section, $\mathbb{F}$ denotes a function field in one variable over a field $\Bbbk$, and we assume that every element of $\mathbb{F}$ outside $\Bbbk$ is transcendental over $\Bbbk$. We continue with the notation $\mathbb{V}_\mathbb{F}$, $D_\mathbb{F}$, f_v, $\operatorname{ord}_v A$, $\deg A$, and (x) for $x \in \mathbb{F}^\times$, all as in Sections 2–3, and with the notation $L(A)$ and $\ell(A)$ as in Section 3. If A is a divisor, we let

$$\delta(A) = \ell(A) - \deg A - (1 - g).$$

Riemann's inequality (Theorem 9.9) implies that $\delta(A) \geq 0$ for all A's and that $\delta(A) = 0$ for some A's. We seek an interpretation of $\delta(A)$.

Let $\mathcal{A}_\mathbb{F}^*$ be the ring of all functions from $\mathbb{V}_\mathbb{F}$ into $\mathbb{F}$, with the operations taken pointwise. It is customary to write such a function ξ as $v \mapsto \xi_v$ rather than as $v \mapsto \xi(v)$. Let $\mathcal{A}_\mathbb{F}$ be the subring[11] of all members ξ of $\mathcal{A}_\mathbb{F}^*$ such that $v(\xi_v) < 0$ for only finitely many v in $\mathbb{V}_\mathbb{F}$. We shall treat $\mathcal{A}_\mathbb{F}$ as an infinite-dimensional associative $\Bbbk$ algebra with identity.

Consider the diagonal map $\Delta : \mathbb{F} \to \mathcal{A}_\mathbb{F}$ defined by the formula $\Delta(x)_v = x$ for all $x \in \mathbb{F}$. Under this map, the member x of $\mathbb{F}$ goes to the function whose value at each v is x. The reason that $\Delta(x)$ is in $\mathcal{A}_\mathbb{F}$ and not just $\mathcal{A}_\mathbb{F}^*$ is that $v(x) < 0$ for only finitely many $v \in \mathbb{V}_\mathbb{F}$. The map Δ is a one-one $\Bbbk$ algebra homomorphism.

[10] Weil's argument dates to 1935. It appears in book form in Weil's *Basic Number Theory*, where the details are carried out when $\Bbbk$ is a finite field and where comments are made for general $\Bbbk$. Lang simplified Weil's argument and wrote it down for algebraically closed fields $\Bbbk$ in his *Introduction to Algebraic and Abelian Functions*. A version of this argument for general $\Bbbk$ appears in Villa Salvador's book. The present exposition benefits from all three of these books.

[11] For readers familiar with Section VI.10, the notation is intended to hint at "adeles" of $\mathbb{F}$. However, completions and topologies will play no role in the construction.

For each divisor A, define

$$\mathcal{L}(A) = \{\xi \in \mathcal{A}_{\mathbb{F}} \mid v(\xi_v) \geq -\operatorname{ord}_v(A)\}.$$

It is immediate from the definitions that

$$\mathcal{L}(A) \cap \Delta(\mathbb{F}) = \Delta(L(A)).$$

Let us see that

$$A \leq B \qquad \text{if and only if} \qquad \mathcal{L}(A) \subseteq \mathcal{L}(B).$$

In fact, the "only if" part of the statement is evident. Conversely suppose that $\mathcal{L}(A) \subseteq \mathcal{L}(B)$. Choose for each $v \in \mathbb{V}_{\mathbb{F}}$ an element π_v in $\mathbb{F}$ with $v(\pi_v) = 1$. The function $\xi_A : \mathbb{V}_{\mathbb{F}} \to \mathbb{F}$ defined by $(\xi_A)_v = \pi^{-\operatorname{ord}_v A}$ has $v((\xi_A)_v) = -\operatorname{ord}_v A$ and lies in $\mathcal{A}_{\mathbb{F}}$, since $\operatorname{ord}_v A$ is nonzero for only finitely many v. The definitions show that ξ_A lies in $\mathcal{L}(A)$, hence in $\mathcal{L}(B)$. Thus $-\operatorname{ord}_v(A) = v((\xi_A)_v) \geq -\operatorname{ord}_v B$, $\operatorname{ord}_v A \leq \operatorname{ord}_v B$, and $A \leq B$. This proves the "if" part of the displayed equivalence. If we apply the equivalence twice, we see that

$$A = B \qquad \text{if and only if} \qquad \mathcal{L}(A) = \mathcal{L}(B).$$

Let us take note of two operations on divisors A and the effect of these operations on the spaces $\mathcal{L}(A)$. If A and B are divisors, we define $C = \min(A, B)$ pointwise by the formula $\operatorname{ord}_v C = \min(\operatorname{ord}_v A, \operatorname{ord}_v B)$. Then C is a divisor with $C \leq A$ and $C \leq B$. Thus $\mathcal{L}(C) \subseteq \mathcal{L}(A)$ and $\mathcal{L}(C) \subseteq \mathcal{L}(B)$, and we consequently obtain

$$\mathcal{L}(\min(A, B)) \subseteq \mathcal{L}(A) \cap \mathcal{L}(B).$$

Still with A and B as divisors, we define $C = \max(A, B)$ pointwise by the formula $\operatorname{ord}_v C = \max(\operatorname{ord}_v A, \operatorname{ord}_v B)$. Then $A \subseteq C$ and $B \subseteq C$, from which we obtain $\mathcal{L}(A) \subseteq \mathcal{L}(C)$ and $\mathcal{L}(B) \subseteq \mathcal{L}(C)$. This proves the inclusion $\subseteq$ in the identity

$$\mathcal{L}(A) + \mathcal{L}(B) = \mathcal{L}(\max(A, B)).$$

To prove $\supseteq$, let ξ be in $\mathcal{L}(\max(A, B))$. We shall decompose ξ as a sum $\eta + \zeta$ in $\mathcal{L}(A) + \mathcal{L}(B)$ with one of η_v and ζ_v equal to 0 for each v. Let v be given. Since ξ is in $\mathcal{L}(\max(A, B))$, $v(\xi_v) \geq -\operatorname{ord}_v(\max(A, B)) = -\max(\operatorname{ord}_v A, \operatorname{ord}_v B)$. That is, $-v(\xi_v) \leq \max(\operatorname{ord}_v A, \operatorname{ord}_v B)$. If $-v(\xi_v) \leq \operatorname{ord}_v A$, then define $\eta_v = \xi_v$ and $\zeta_v = 0$; otherwise, we have $-v(\xi_v) \leq \operatorname{ord}_v B$, and we define $\eta_v = 0$ and $\zeta_v = \xi_v$. Then $v(\eta_v) \geq -\operatorname{ord}_v A$ for all v, and $v(\zeta_v) \geq -\operatorname{ord}_v B$ for all v. This proves $\supseteq$ in the displayed formula.

Lemma 9.11. If A and B are divisors with $A \le B$, then

$$\dim_{\Bbbk} \big(\mathcal{L}(B)/\mathcal{L}(A)\big) = \deg B - \deg A.$$

PROOF. Proceeding inductively, we see that it is enough to handle the case that $B = A + v_0$, where v_0 is in $\mathbb{V}_{\mathbb{F}}$. Thus we are to show that

$$\dim_{\Bbbk} \big(\mathcal{L}(A + v_0)/\mathcal{L}(A)\big) = f_{v_0} = \deg(v_0). \tag{$*$}$$

Put $f = f_{v_0}$, let R_{v_0} be the valuation ring of v_0, and let P_{v_0} be the valuation ideal of v_0. To prove $\le$ in $(*)$, we argue as in the proof of Lemma 9.5. Since v_0 carries $\mathbb{F}^\times$ onto $\mathbb{Z}$, we can choose an element $y \in \mathbb{F}^\times$ with $v_0(y) = \operatorname{ord}_{v_0}(A + v_0)$.

Let $f + 1$ members $\xi^{(1)}, \dots, \xi^{(f+1)}$ of $\mathcal{L}(A + v_0)$ be given. We shall produce an equation of linear dependence among the cosets $\xi^{(i)} + \mathcal{L}(A)$, and this will prove $\le$ in $(*)$. Computation gives

$$v_0(\xi^{(i)}_{v_0} y) = v_0(\xi^{(i)}_{v_0}) + v_0(y) = v_0(\xi^{(i)}_{v_0}) + \operatorname{ord}_{v_0}(A + v_0) \ge 0$$

for $1 \le i \le f + 1$, with the inequality at the right holding because $\xi^{(i)}$ is in $\mathcal{L}(A + v_0)$. Hence $\xi^{(i)}_{v_0} y$ is in R_{v_0}. Since $\dim_{\Bbbk}(R_{v_0}/P_{v_0}) = f$, there exist members $c_1, \dots, c_{f+1}$ of $\Bbbk$ not all 0 such that $\sum_{i=1}^{f+1} c_i(\xi^{(i)}_{v_0} y + P_{v_0}) = P_{v_0}$, i.e., such that $\sum_{i=1}^{f+1} c_i \xi^{(i)}_{v_0} y$ lies in P_{v_0}. Then $\sum_{i=1}^{f+1} c_i \xi^{(i)}_{v_0}$ lies in $y^{-1} P_{v_0}$, and

$$v_0\Big(\sum_{i=1}^{f+1} c_i \xi^{(i)}_{v_0}\Big) \ge -v_0(y) + 1 = -\operatorname{ord}_{v_0}(A + v_0) + 1 = -\operatorname{ord}_{v_0} A. \tag{$**$}$$

Since each $\xi^{(i)}$ is in $\mathcal{L}(A + v_0)$, so is $\sum_{i=1}^{f+1} c_i \xi^{(i)}_{v_0}$. This fact and $(**)$ together show that $\sum_{i=1}^{f+1} c_i \xi^{(i)}_{v_0}$ is in $\mathcal{L}(A)$, i.e., that $\sum_{i=1}^{f+1} c_i \xi^{(i)} + \mathcal{L}(A)$ is the 0 coset. This proves the desired linear dependence and shows that $\dim_{\Bbbk} \mathcal{L}(A + v_0)/\mathcal{L}(A) \le f$.

To prove $\ge$ in $(*)$, we shall produce f members $\xi^{(j)}$ of $\mathcal{L}(A + v_0)$ that are linearly independent modulo $\mathcal{L}(A)$. We begin by choosing η in $\mathcal{L}(A)$ with $v_0(\eta_{v_0}) = -\operatorname{ord}_{v_0} A$. (For example take any member η' of $\mathcal{L}(A)$, change η'_{v_0} to a new value on which v_0 takes the value $-\operatorname{ord}_{v_0} A$, and leave η' unchanged at all other v.) Let $x_1, \dots, x_f$ be a set of representatives in R_{v_0} of the f members of a $\Bbbk$ basis of the quotient R_{v_0}/P_{v_0}, and let π_{v_0} be a member of $\mathbb{F}$ with $v_0(\pi_{v_0}) = 1$. Define $\xi^{(j)}$ for $1 \le j \le f$ by

$$\xi^{(j)}_v = \begin{cases} \eta_v & \text{for } v \ne v_0, \\ \eta_{v_0} x_j \pi_{v_0}^{-1} & \text{for } v = v_0. \end{cases}$$

For each j, we have

$$\begin{aligned} v_0(\eta_{v_0} x_j \pi^{-1}) &= v_0(\eta_{v_0}) + v(x_j) - v_0(\pi_{v_0}) \\ &= -\operatorname{ord}_{v_0} A + v(x_j) - 1 \ge -\operatorname{ord}_{v_0} A - 1, \end{aligned}$$

and thus $\xi^{(j)}$ is in $\mathcal{L}(A + v_0)$. To prove the linear independence modulo $\mathcal{L}(A)$, suppose that $c_1, \dots, c_f$ are members of $\Bbbk$ such that $\sum_{j=1}^f c_j \xi^{(j)}$ is in $\mathcal{L}(A)$. In this case we have an inequality $v_0\big(\sum_{j=1}^f c_j \xi^{(j)}\big) \geq -\operatorname{ord}_{v_0} A$, which expands out as

$$v_0\Big(\sum_{j=1}^f c_j \eta_{v_0} x_j \pi_{v_0}^{-1}\Big) \geq v_0(\eta_{v_0}).$$

Since $v_0(\pi_{v_0}^{-1}) = -1$, subtraction of $v_0(\eta_{v_0})$ from both sides yields $v_0\big(\sum_{j=1}^f c_j x_j\big) \geq 1$. Therefore $\sum_{j=1}^f c_j x_j$ lies in P_{v_0}. By the assumed linear independence over $\Bbbk$ of the x_j's modulo P_{v_0}, all the c_j's are 0. Therefore the elements $\xi^{(j)}$ are linearly independent modulo $\mathcal{L}(A)$, and the proof of $\geq$ in $(*)$ is complete. □

Lemma 9.12. If A and B are divisors with $A \leq B$, then there is an exact sequence in the category of $\Bbbk$ vector spaces given by

$$\begin{aligned} 0 \longrightarrow L(B)/L(A) &\xrightarrow{\psi} \mathcal{L}(B)/\mathcal{L}(A) \\ &\xrightarrow{\varphi} (\mathcal{L}(B) + \Delta(\mathbb{F}))\big/(\mathcal{L}(A) + \Delta(\mathbb{F})) \longrightarrow 0. \end{aligned}$$

Consequently

$$\begin{aligned} \dim_{\Bbbk}(\mathcal{L}(B) + \Delta(\mathbb{F}))\big/(\mathcal{L}(A) + \Delta(\mathbb{F})) &= (\ell(A) - \deg A) - (\ell(B) - \deg B) \\ &= \delta(A) - \delta(B). \end{aligned}$$

PROOF. The map ψ is induced by the map $\Delta : L(B) \to \mathcal{L}(B)$ followed by passage to the quotient. It descends to $L(B)/L(A)$ because $\Delta(L(A)) \subseteq \mathcal{L}(A)$, and it is one-one because $\Delta(L(B)) \cap \mathcal{L}(A) \subseteq L(A)$. The map φ is induced by the map $x \mapsto x + \Delta(\mathbb{F})$ followed by passage to the quotient. It descends to $\mathcal{L}(B)/\mathcal{L}(A)$ because $\mathcal{L}(A)$ maps into $\mathcal{L}(A) + \Delta(\mathbb{F})$, and it is onto because $x \mapsto x + \Delta(\mathbb{F})$ carries $\mathcal{L}(B)$ onto $\mathcal{L}(B) + \Delta(\mathbb{F})$. The composition $\varphi\psi$ is 0 because $L(B)$ maps under Δ into $\Delta(\mathbb{F})$, which lies in the 0 coset.

To prove the exactness, let $\xi + \mathcal{L}(A)$ be in $\ker\varphi$. This condition means that ξ is in $\mathcal{L}(B)$ and has $\xi + \Delta(\mathbb{F})$ in $\mathcal{L}(A) + \Delta(\mathbb{F})$. Thus there exists η in $\mathcal{L}(A)$ with $\xi - \eta$ in $\Delta(\mathbb{F})$. Since ξ and η are in $\mathcal{L}(B)$, $\xi - \eta$ is in $\mathcal{L}(B) \cap \Delta(\mathbb{F}) \subseteq \Delta(L(B))$. Hence $\xi + \mathcal{L}(A) = (\xi - \eta) + \mathcal{L}(A)$ lies in $\Delta(L(B)) + \mathcal{L}(A) = \operatorname{image}\psi$, and exactness is proved.

From the exactness we obtain

$$\dim_{\Bbbk} \mathcal{L}(B)/\mathcal{L}(A) = \dim_{\mathbb{K}} L(B)/L(A) + \dim_{\Bbbk}(\mathcal{L}(B) + \Delta(\mathbb{F}))\big/(\mathcal{L}(A) + \Delta(\mathbb{F})).$$

The left side equals $\deg B - \deg A$ by Lemma 9.11, and the first term on the right side equals $\ell(B) - \ell(A)$ by the finite dimensionality of $L(B)$ and $L(A)$, which was proved as part of Theorem 9.6. The result follows. □

Theorem 9.13. There exists a divisor C such that $\mathcal{A}_{\mathbb{F}} = \mathcal{L}(C) + \Delta(\mathbb{F})$. For each divisor A,

$$\delta(A) = \dim_{\Bbbk} \big(\mathcal{A}_{\mathbb{F}} \big/ (\mathcal{L}(A) + \Delta(\mathbb{F}))\big).$$

PROOF. Riemann's inequality produces a divisor C, specifically any sufficiently large positive power of a divisor $(x)_\infty$, such that $\delta(C) = 0$. If we can show that $\mathcal{A}_{\mathbb{F}} = \mathcal{L}(C) + \Delta(\mathbb{F})$, then the dimensional equality in Lemma 9.12 with $B = C$ will complete the proof of the present theorem.

Suppose that there exists a member ξ of $\mathcal{A}_{\mathbb{F}}$ that is not in $\mathcal{L}(C) + \Delta(\mathbb{F})$. For each $v \in \mathbb{V}_{\mathbb{F}}$, let $a_v = \min(v(\xi_v), -\operatorname{ord}_v C)$, and define $C' = -\sum_{v \in \mathbb{V}_{\mathbb{F}}} a_v v$. Since ξ is in $\mathcal{A}_{\mathbb{F}}$, only finitely many integers $v(\xi_v)$ are negative. This fact and the fact that C is a divisor together imply that only finitely many a_v are negative. Since C is a divisor, only finitely many integers $-\operatorname{ord}_v C$ can be positive, and thus only finitely many a_v can be positive. Therefore C' is a divisor.

The definition of C' is arranged in such a way that $C \le C'$. Also, every v has $v(\xi_v) \ge a_v = -\operatorname{ord}_v C'$, and hence ξ lies in $\mathcal{L}(C')$. Consequently

$$\dim_{\Bbbk}(\mathcal{L}(C') + \Delta(\mathbb{F})) \big/ (\mathcal{L}(C) + \Delta(\mathbb{F})) \ge 1.$$

By Lemma 9.12, $\delta(C) - \delta(C') \ge 1$. Since C was assumed to have $\delta(C) = 0$, we obtain $-\delta(C') \ge 1$, in contradiction to the fact that $\delta(A) \ge 0$ for every divisor A. We conclude that every ξ in $\mathcal{A}_{\mathbb{F}}$ lies in $\mathcal{L}(C) + \Delta(\mathbb{F})$. □

Theorem 9.13 gives a first interpretation of the difference $\delta(A)$ between the two sides of Riemann's inequality (Theorem 9.9). We shall now apply Theorem 9.13 and reinterpret $\delta(A)$ as the dimension $\ell(B)$ of a suitable divisor B obtained from A, and then we will have obtained the Riemann–Roch Theorem.

A **differential** of $\mathbb{F}$ is a $\Bbbk$ linear functional ω on $\mathcal{A}_{\mathbb{F}}$ with the property that ω vanishes on $\mathcal{L}(A)$ for some divisor A and ω vanishes also on $\Delta(\mathbb{F})$. The set of all differentials of $\mathbb{F}$ will be denoted by $\operatorname{Diff}(\mathbb{F})$. Let us observe that $\operatorname{Diff}(\mathbb{F})$ is a vector subspace of $\Bbbk$ linear functionals on $\mathcal{A}_{\mathbb{F}}$. Scalar multiplication by $\Bbbk$ is not an issue. To see that $\operatorname{Diff}(\mathbb{F})$ is closed under pointwise addition, let ω and ω' be differentials vanishing on $\mathcal{L}(A)$ and $\mathcal{L}(B)$, respectively. We have seen that $\mathcal{L}(\min(A, B)) \subseteq \mathcal{L}(A) \cap \mathcal{L}(B)$. Thus $\omega + \omega'$ vanishes on $\mathcal{L}(\min(A, B))$. Since $\omega + \omega'$ vanishes also on $\Delta(\mathbb{F})$, $\omega + \omega'$ is a differential.

The $\Bbbk$ vector space of differentials vanishing on $\mathcal{L}(A) + \Delta(K)$ may be identified with the vector space of $\Bbbk$ linear functionals on the quotient $\mathcal{A}_{\mathbb{F}}/(\mathcal{L}(A) + \Delta(\mathbb{F}))$, and the latter space is finite-dimensional of dimension $\delta(A)$ by Theorem 9.13. Since a finite-dimensional vector space and its dual have the same dimension, the $\Bbbk$ vector space of differentials vanishing on $\mathcal{L}(A) + \Delta(K)$ has $\Bbbk$ dimension $\delta(A)$.

In addition, $\operatorname{Diff}(\mathbb{F})$ carries a scalar multiplication by $\mathbb{F}$ that makes it into an $\mathbb{F}$ vector space. What is required to verify this statement is a definition, and then

the verification of the properties of an $\mathbb{F}$ vector space is routine. If y is in $\mathbb{F}$ and ω is a differential, we define $y\omega$ on $\mathcal{A}_\mathbb{F}$ by $(y\omega)(\xi) = \omega(\Delta(y)\xi)$. The linear functional $y\omega$ vanishes on $\Delta(\mathbb{F})$ because Δ is a homomorphism. It is enough to check for $y \neq 0$ that

$$\text{if } \omega \text{ vanishes on } \mathcal{L}(A), \text{ then } y\omega \text{ vanishes on } \mathcal{L}(A + (y)),$$

where (y) is the principal divisor corresponding to y. To prove this vanishing, let ξ be in $\mathcal{L}(A + (y))$. Then $v(\xi_v) \geq -\operatorname{ord}_v(A + (y)) = -\operatorname{ord}_v A - \operatorname{ord}_v(y) = -\operatorname{ord}_v A - v(y)$, which implies that $v(\xi_v y) \geq -\operatorname{ord}_v A$, which implies that $\xi\Delta(y)$ lies in $\mathcal{L}(A)$, which implies that $\omega(\xi\Delta(y)) = 0$, which implies that $(y\omega)(\xi) = 0$. This proves the asserted vanishing, and it follows that $\operatorname{Diff}(\mathbb{F})$ carries a well-defined scalar multiplication by $\mathbb{F}$.

Each set $\mathcal{L}(A)$, where A is a divisor, will be called a **parallelotope** of $\mathcal{A}_\mathbb{F}$. These sets are large subsets of $\mathcal{A}_\mathbb{F}$, since $\dim_\Bbbk \mathcal{A}_\mathbb{F}/(\mathcal{L}(A) + \Delta(\mathbb{F}))$ is finite and $\dim_\Bbbk \mathcal{A}_\mathbb{F}/\Delta(\mathbb{F})$ is infinite. We are going to associate a particular parallelotope to each nonzero differential. Since we have seen that distinct parallelotopes correspond to distinct divisors, we shall obtain a way of associating a divisor to each nonzero differential.

Corollary 9.14. If ω is a nonzero differential and $\mathcal{L}(A)$ is a parallelotope in its kernel, then

$$\ell(A) \leq \delta(0) \qquad \text{and} \qquad \deg A \leq \delta(0) + g - 1.$$

Consequently there exists a unique maximum parallelotope on which ω vanishes.

REMARKS. In view of the remarks before the corollary, we therefore obtain a function $\omega \mapsto \operatorname{Div}(\omega)$ from the set $\operatorname{Diff}(\mathbb{F}) - \{0\}$ of nonzero differentials into the set $D_\mathbb{F}$ of divisors.

PROOF. If we know that $\ell(A) \leq \delta(0)$, then addition to this inequality of Riemann's inequality $\deg A - \ell(A) \leq g - 1$ as given in Theorem 9.9 shows that

$$\deg A \leq \delta(0) + g - 1$$

and proves the second inequality. The inequality $\ell(A) \leq \delta(0)$ is trivial if $L(A) = 0$.

Therefore we may assume in the two inequalities that $L(A) \neq 0$. Let y be any nonzero member of $L(A)$. Since the kernel of ω contains $\mathcal{L}(A)$, the kernel of $y\omega$ contains $\mathcal{L}(A + (y))$, by a computation made above. Meanwhile, the element y, being in $L(A)$, has $(y) \geq -A$ and hence $0 \leq A + (y)$. Therefore $\mathcal{L}(0) \subseteq \mathcal{L}(A + (y))$, and the kernel of $y\omega$ contains $\mathcal{L}(0)$. Since the kernel of $y\omega$ contains $\Delta(\mathbb{F})$, $y\omega$ is well defined on the quotient space $\mathcal{A}_\mathbb{F}/(\mathcal{L}(0) + \Delta(\mathbb{F}))$.

Now suppose that $y_1, \ldots, y_n$ is a $\Bbbk$ basis of $L(A)$. Let us use the fact that $\omega \neq 0$ to prove that $y_1\omega, \ldots, y_n\omega$ are linearly independent when viewed on $\mathcal{A}_{\mathbb{F}}/(\mathcal{L}(0) + \Delta(\mathbb{F}))$: If $c_1, \ldots, c_n$ are members of $\Bbbk$ not all 0, then $z = \sum_{j=1}^n c_j y_j$ is a nonzero member of $L(A)$, and we have just seen that $z\omega$ is well defined on $\mathcal{A}_{\mathbb{F}}/(\mathcal{L}(0) + \Delta(\mathbb{F}))$. Then we have $\sum_{j=1}^n c_j(y_j\omega) = \big(\sum_{j=1}^n c_j y_j\big)\omega = z\omega$, and this cannot act as 0 on $\mathcal{A}_{\mathbb{F}}/(\mathcal{L}(0) + \Delta(\mathbb{F}))$ without being identically 0 on $\mathcal{A}_{\mathbb{F}}$. Since any ξ_0 such that $\omega(\xi_0) \neq 0$ has the property that $z\omega(\Delta(z)^{-1}\xi_0) \neq 0$, the linear functionals $y_1\omega, \ldots, y_n\omega$ on $\mathcal{A}_{\mathbb{F}}/(\mathcal{L}(0) + \Delta(\mathbb{F}))$ are linearly independent.

We know that $\delta(0) = \dim_{\Bbbk} \mathcal{A}_{\mathbb{F}}/(\mathcal{L}(0) + \Delta(\mathbb{F}))$ by Theorem 9.13, and hence

$$n = \ell(A) \leq \delta(0).$$

This completes the proof of the two inequalities.

We turn to the existence and uniqueness of the maximum parallelotope on which ω vanishes. We continue to assume that $\omega \neq 0$. Now suppose that A is a divisor such that ω vanishes on $\mathcal{L}(A)$. Suppose that B is a divisor for which $B \leq A$ fails and for which $\omega(\mathcal{L}(B)) = 0$. We know that the divisor $\max(A, B)$ has the property that $\mathcal{L}(\max(A, B)) = \mathcal{L}(A) + \mathcal{L}(B)$. Since ω vanishes on $\mathcal{L}(A)$ and $\mathcal{L}(B)$, it follows that it vanishes on $\mathcal{L}(\max(A, B))$. Since $B \leq A$ fails, there exists some $v_0 \in \mathbb{V}_{\mathbb{F}}$ with $\operatorname{ord}_{v_0} B > \operatorname{ord}_{v_0} A$, and this v_0 has $\operatorname{ord}_{v_0} \max(A, B) > \operatorname{ord}_{v_0} A$. Thus $\deg \max(A, B) > \deg A$.

The second inequality proved above shows that the degree is bounded on all divisors whose parallelotopes are in $\ker \omega$. In finitely many steps we consequently arrive at a divisor C with $\mathcal{L}(C) \subseteq \ker \omega$ such that any divisor B with $\mathcal{L}(B) \subseteq \ker \omega$ has $B \leq C$. Then C is the unique maximum divisor on whose parallelotope ω vanishes. The parallelotope determines the divisor, and the proof of the corollary is complete. □

Recall from Section 2 that the additive subgroup $P_{\mathbb{F}}$ of principal divisors within the group $D_{\mathbb{F}}$ of all divisors breaks $D_{\mathbb{F}}$ into equivalence classes known as **divisor classes**. The group $C_{\mathbb{F}} = D_{\mathbb{F}}/P_{\mathbb{F}}$ is the group of all divisor classes. The operation of a principal divisor (y), for $y \in \mathbb{F}^\times$, on a divisor A is $A \mapsto A + (y)$. On the other hand, we have seen that if a nonzero differential ω vanishes on $\mathcal{L}(A)$, then $y\omega$ vanishes on $\mathcal{L}(A + (y))$. In the notation of the remarks with Corollary 9.14, we therefore have

$$\operatorname{Div}(y\omega) = \operatorname{Div}(\omega) + (y).$$

A single orbit of nonzero differentials under the scalar-multiplication action on $\operatorname{Diff}(\mathbb{F})$ by $\mathbb{F}^\times$ thus yields a single divisor class within $D_{\mathbb{F}}$. We shall show that $\operatorname{Diff}(\mathbb{F})$ is 1-dimensional as an $\mathbb{F}$ vector space. Then the nonzero differentials form a single orbit under $\mathbb{F}^\times$, and the divisors that arise as $\operatorname{Div}(\omega)$ for some nonzero differential ω form a single divisor class.

Lemma 9.15. As a vector space over $\mathbb{F}$, the space Diff($\mathbb{F}$) of differentials is 1-dimensional.

PROOF. First we prove that Diff($\mathbb{F}$) is nonzero. Referring to Theorem 9.13, we know that $\delta(A) = \dim_{\Bbbk}\big(\mathcal{A}_{\mathbb{F}}\big/(\mathcal{L}(A) + \Delta(\mathbb{F}))\big)$. If $\delta(A) > 0$, then there exist nonzero linear functionals on $\mathcal{A}_{\mathbb{F}}\big/(\mathcal{L}(A) + \Delta(\mathbb{F}))$, and the lift of such a nonzero linear functional to $\mathcal{A}_{\mathbb{F}}$ is a nonzero differential. Thus it is enough to produce a divisor A with $\delta(A) > 0$. Fix v_0 in $\mathbb{V}_{\mathbb{F}}$, and let $A = -2v_0$. Proposition 9.10 shows that $\ell(A) = 0$. Therefore

$$\delta(A) = \ell(A) - \deg A - (1 - g) = 2 + g - 1 = g + 1 > 0,$$

and this A has $\delta(A) > 0$.

Now we shall prove that the $\mathbb{F}$ dimension of Diff($\mathbb{F}$) is at most 1. Arguing by contradiction, suppose that ω and ω' are differentials that are linearly independent over $\mathbb{F}$. If ω vanishes on $\mathcal{L}(A)$ and ω' vanishes on $\mathcal{L}(A')$, then $\omega + \omega'$ vanishes on $\mathcal{L}(A) \cap \mathcal{L}(A') \supseteq \mathcal{L}(C)$, where $C = \min(A, A')$. Let B be an arbitrary divisor. Suppose for the moment that $L(B) \neq 0$. If $y \neq 0$ is in $L(B)$, then $(y) \geq -B$, and $C + (y) \geq C - B$. So $\mathcal{L}(C + (y)) \supseteq \mathcal{L}(C - B)$. We have seen that the vanishing of ω on $\mathcal{L}(C)$ implies the vanishing of $y\omega$ on $\mathcal{L}(C + (y))$. Therefore $y\omega$ vanishes on $\mathcal{L}(C - B)$. Similarly $y\omega'$ vanishes on $\mathcal{L}(C - B)$.

Still with $L(B) \neq 0$, let $n = \ell(B)$, and let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be bases of $L(B)$ over $\Bbbk$. Then $x_1\omega, \ldots, x_n\omega, y_1\omega', \ldots, y_n\omega'$ are linearly independent over $\Bbbk$ because a relation

$$\sum_{i=1}^{n} a_i x_i \omega + \sum_{j=1}^{n} b_j y_j \omega' = 0$$

would mean that the members $x = \sum_{i=1}^{n} a_i x_i$ and $y = \sum_{j=1}^{n} b_j y_j$ of $\mathbb{F}$ have $x\omega + y\omega' = 0$. Since ω and ω' are assumed to be linearly independent over $\mathbb{F}$, $x = y = 0$. But then $a_i = 0$ for all i and $b_j = 0$ for all j. Consequently we can generate $2n$ linearly independent differentials that all vanish on $\mathcal{L}(C - B)$. These differentials may be regarded as linear functionals on the $\Bbbk$ vector space $\mathcal{A}_{\mathbb{F}}/(\mathcal{L}(C - B) + \Delta(\mathbb{F}))$, whose $\Bbbk$ dimension is $\delta(C - B)$ by Theorem 9.13.

Consequently

$$\delta(C - B) \geq 2\ell(B),$$

and this inequality is true also if $L(B) = 0$, by Riemann's inequality. Substituting from the formula for $\delta(\,\cdot\,)$, we obtain

$$\begin{aligned} \ell(C - B) - \deg(C - B) - 1 + g &\geq 2\ell(B) \\ &= 2\big(\deg B + 1 - g) + \delta(B)\big) \\ &\geq 2 \deg B + 2 - 2g \end{aligned}$$

because Riemann's inequality shows that $\delta(B) \geq 0$. Replacing $\deg(C - B)$ by $\deg C - \deg B$ gives

$$\deg B \leq \ell(C - B) - \deg C - 3 + 3g. \qquad (*)$$

Proposition 9.10 shows that $\ell(C - B) \leq 1 + \deg(C - B)$ if $\ell(C - B) \neq 0$. In this case the two inequalities together give

$$2 \deg B \leq -2 + 3g;$$

hence $\ell(C - B) = 0$ if $\deg B$ is positive and sufficiently large. Choosing then a divisor B with $\deg B$ positive and sufficiently large, we have $\ell(C - B) = 0$, and $(*)$ gives

$$\deg B \leq -\deg C - 3 + 3g.$$

Since the right side is fixed and the left side can be made arbitrarily large, we have arrived at a contradiction. □

As a result of Lemma 9.15, the divisors of the form $\mathrm{Div}(\omega)$ for some nonzero differential ω constitute a single class in the group $C_{\mathbb{F}} = D_{\mathbb{F}}/P_{\mathbb{F}}$ of divisor classes. This class is called the **canonical class** of $\mathbb{F}$, and any divisor in the class is called a **canonical divisor**.

Theorem 9.16 (Riemann–Roch Theorem). Let $\mathbb{F}$ be a function field in one variable over a field $\Bbbk$, and suppose that every member of $\mathbb{F}$ not in $\Bbbk$ is transcendental over $\Bbbk$. If A is any divisor of $\mathbb{F}$ and C is any canonical divisor, then

$$\ell(A) = \deg A + (1 - g) + \ell(C - A),$$

where g is the genus of $\mathbb{F}$.

PROOF. Lemma 9.15 shows that there exists a nonzero differential ω_0. Let $C_0 = \mathrm{Div}(\omega_0)$. Lemma 9.15 shows that $C = C_0 + (y_0)$ for some $y_0 \in \mathbb{F}^\times$. Then $\omega = y_0\omega_0$ has

$$\mathrm{Div}(\omega) = \mathrm{Div}(y_0\omega_0) = \mathrm{Div}(\omega_0) + (y_0) = C_0 + (y_0) = C.$$

Let B be a divisor to be specified, and consider $C - B$. Any nonzero differential ω' vanishing on $\mathcal{L}(C - B)$ is of the form $\omega' = z\omega$ for some $z \in \mathbb{F}^\times$ by Lemma 9.15, and $\mathrm{Div}(\omega') = \mathrm{Div}(z\omega) = C + (z)$. Therefore $\mathcal{L}(C + (z)) \supseteq \mathcal{L}(C - B)$, $C + (z) \geq C - B$, and $(z) \geq -B$. This inequality means that z is in $L(B)$. Conversely if y is any nonzero element in $L(B)$, then $(y) \geq -B$ and $C + (y) \geq C - B$. So $\mathcal{L}(C + (y)) \supseteq \mathcal{L}(C - B)$. We know that $y\omega$ vanishes on $\mathcal{L}(C + (y))$, and hence $y\omega$ vanishes on $\mathcal{L}(C - B)$.

Consequently the differentials vanishing on $\mathcal{L}(C - B)$ are exactly the differentials $y\omega$ with y in $L(B)$. Such differentials vanish on $\Delta(\mathbb{F})$ by definition, and the space of them is $\Bbbk$ isomorphic to the space of $\Bbbk$ linear functionals on $\mathcal{A}_{\mathbb{F}}\big/\big(\mathcal{L}(C - B) + \Delta(\mathbb{F})\big)$. By Theorem 9.13 the latter space has $\Bbbk$ dimension $\delta(C - B)$, and hence the space of differentials in question has $\Bbbk$ dimension $\delta(C - B)$. In short,

$$\delta(C - B) = \ell(B).$$

Since B is arbitrary, we can specialize it to $B = C - A$. Then we obtain

$$\ell(C - A) = \delta(A) = \ell(A) - \deg A - (1 - g),$$

and the theorem follows. □

5. Applications of the Riemann–Roch Theorem

We begin with some immediate applications of the Riemann–Roch Theorem, and then we obtain some applications that require arguments that are a bit more subtle. Another application appears in the problems at the end of Chapter X.

Corollary 9.17. If C is any canonical divisor, then $\ell(C) = g$.

PROOF. Put $A = 0$ in Theorem 9.16, and use the fact given in Corollary 9.4 that $\ell(0) = 1$. □

Corollary 9.18. If C is any canonical divisor, then $\deg C = 2g - 2$.

PROOF. Put $A = C$ in Theorem 9.16, and apply Corollary 9.17 and Corollary 9.4. □

Corollary 9.19. Any divisor A with $\deg A > 2g - 2$ has $\delta(A) = 0$, i.e., $\ell(A) = \deg A + (1 - g)$.

PROOF. If $\deg A > 2g - 2$, then it follows from Corollary 9.18 that $\deg(C - A) < 0$. By Proposition 9.10, $\ell(C - A) = 0$. Then the corollary is immediate from Theorem 9.16. □

Corollary 9.20. If A is a divisor with $\deg A = 2g - 2$, then either A is a canonical divisor and $\ell(A) = g$, or A is not a canonical divisor and $\ell(A) = g - 1$.

PROOF. If A is a canonical divisor, then $\ell(A) = g$ by Corollary 9.17. Otherwise, the divisor $C - A$, which has degree 0 by Corollary 9.18, is not a principal divisor. Any nonzero y in $L(C - A)$ then would have $(y) \geq -(C - A)$ and $0 = \deg(y) \geq -\deg(C - A) = 0$; hence $v(y) = -\operatorname{ord}_v(C - A)$ for all v, and $(y) = C - A$, contradiction. Consequently $L(C - A) = 0$ and $\ell(C - A) = 0$. Theorem 9.16 now gives $\ell(A) = \deg A + (1 - g) = (2g - 2) + (1 - g) = g - 1$. □

EXAMPLES OF CANONICAL DIVISORS.

(1) Genus $g = 0$. In Corollary 9.20 with $g = 0$, the alternative $\ell(A) = g - 1 = -1$ is impossible, and therefore every divisor with degree -2 is a canonical divisor.

(2) Genus $g = 1$. In Corollary 9.20 with $g = 1$, take $A = 0$. Then $\ell(A) = 1 = g$ by Corollary 9.4. So Corollary 9.20 says that the divisor 0 is a canonical divisor.

Corollary 9.21. If v_0 is in $\mathbb{V}_{\mathbb{F}}$ and $n > \max(2g - 1, 0)$, then there exists a nonscalar x in $\mathbb{F}^\times$ with $(x)_\infty \le nv_0$.

PROOF. Let $A = nv_0$, and let f_{v_0} be the residue class degree of v_0. Then $\deg A = nf_{v_0} \ge n > \max(2g - 1, 0)$, and Corollary 9.19 gives

$$\begin{aligned}\ell(A) &= \deg A + (1 - g) = nf_{v_0} + (1 - g)\\ &> \max(2g - 1, 0) + (1 - g) = \max(g, 1 - g) \ge 1.\end{aligned}$$

Hence $\ell(A) \ge 2$, and $L(A)$ contains a nonscalar element x. This x has

$$-n = -\operatorname{ord}_{v_0} A \le \operatorname{ord}_{v_0}(x) = \operatorname{ord}_{v_0}(x)_0 - \operatorname{ord}_{v_0}(x)_\infty = -\operatorname{ord}_{v_0}(x)_\infty,$$

and thus $(x)_\infty \le nv_0$. □

Doubly periodic meromorphic functions on $\mathbb{C}$ in the subject of complex analysis may be viewed as meromorphic functions on some torus,[12] which is a compact Riemann surface of genus 1. The Weierstrass $\wp$ function for the torus in question has a double pole at one point, two zeros, and no other poles or zeros. It is therefore a function x with $(x)_\infty = 2v_0$ if v_0 is the discrete valuation corresponding to the location of the pole. Hence this x provides an example with equality holding in Corollary 9.21 when $g = 1$. A theorem of Liouville in this terminology says that there is no meromorphic function on the torus having just one simple pole and no other poles. The final corollaries abstract this result to our setting, but they need an additional hypothesis to ensure that $f_{v_0} = 1$. Certainly f_{v_0} will equal 1 if $\Bbbk$ is algebraically closed. We consider $g = 1$ and $g > 1$ separately. These corollaries will be generalized in Problems 23–25 at the end of the chapter.

Corollary 9.22. If $\Bbbk$ is algebraically closed, if v_0 is in $\mathbb{V}_{\mathbb{F}}$, and if $g = 1$, then every x in $\mathbb{F}$ with $(x)_\infty \le v_0$ is a scalar multiple of the identity.

PROOF. Put $A = v_0$. We seek $x \in \mathbb{F}$ with $v_0(x) \ge -1 = -\operatorname{ord}_{v_0} A$ and with $v(x) \ge 0 = -\operatorname{ord}_v A$ for all other v. Thus we seek x in $L(A)$. This A has $\deg A = 1 = g = 2g - 1$. By Corollary 9.19, $\ell(A) = \deg A + (1 - g) = 1 + (1 - 1) = 1$. Since $L(A)$ already contains the multiples of the identity, it contains nothing else. □

[12]The particular torus is $\mathbb{C}/\Lambda$, where Λ is the lattice of periods.

Corollary 9.23. If $\Bbbk$ is algebraically closed, if v_0 is in $\mathbb{V}_{\mathbb{F}}$, and if $g > 1$, then every x in $\mathbb{F}$ with $(x)_\infty \le v_0$ is a scalar multiple of the identity.

PROOF. We argue by contradiction. Suppose that x is a nonscalar element in $L(v_0)$. Take $r = 2g - 1$, and let $c_1, \dots, c_r$ be distinct members of $\Bbbk$. For each j with $1 \le j \le r$, $x - c_j$ is in $L(v_0)$. Since $\deg(x - c_j) = 0$, there exists a unique $v_j \in \mathbb{V}_{\mathbb{F}}$ with $v_j(x - c_j) = 1$. The divisor of the element $(x - c_j)^{-1}$ is then $v_0 - v_j$. It follows that every $\Bbbk$ linear combination of the elements $(x - c_j)^{-1}$ lies in $L(A)$ for $A = v_1 + \cdots + v_r$. On the other hand, these elements are linearly independent because $v_j\big(\sum_{i=1}^r a_i(x - c_j)^{-1}\big) < 0$ if and only if $a_j \ne 0$. Thus $\ell(A) \ge 2g - 1$ and $\deg A = 2g - 1$. Since $\deg A > 2g - 2$, Corollary 9.19 is applicable and gives $\ell(A) = \deg A + 1 - g$. Thus $2g - 1 \le \ell(A) = \deg A + 1 - g = 2g - 1 + 1 - g = g$, and we obtain the contradiction $g \le 1$. □

6. Problems

1. Let $\mathbb{F}$ be a function field in one variable over the field $\Bbbk$, and let $\Bbbk'$ be the subfield of all members of $\mathbb{F}$ that are algebraic over $\Bbbk$.
   (a) Suppose that $t_1, \dots, t_n$ are members of $\Bbbk'$ that are linearly independent over $\Bbbk$, and suppose that $x \in \mathbb{F}$ is transcendental over $\Bbbk$. Prove that $t_1, \dots, t_n$ are linearly independent over $\Bbbk(x)$.
   (b) Deduce from (a) that $[\Bbbk' : \Bbbk] \le [\Bbbk'(x) : \Bbbk(x)]$.
   (c) Deduce that $[\Bbbk' : \Bbbk] < \infty$.

Problems 2–4 concern perfect fields, which were defined in Section VII.3. The field $\Bbbk$ is perfect if either it has characteristic 0 or else it has characteristic p and the field map $x \mapsto x^p$ of $\Bbbk$ into itself is onto.

2. Prove that an algebraic extension of a perfect field is perfect.

3. When $\Bbbk$ is perfect, refine an argument in Section 1 by making use of Theorems 7.18, 7.20, 7.22, and the Theorem of the Primitive Element, and show that any function field in one variable is the function field of some affine plane curve irreducible over $\Bbbk$.

4. Let $\Bbbk$ be a perfect field. An affine plane curve $f(X, Y)$ irreducible over $\Bbbk$ is nonsingular at a point (a, b) of its zero locus if at least one of $\frac{\partial f}{\partial X}(a, b)$ and $\frac{\partial f}{\partial Y}(a, b)$ is nonzero. Using Bezout's Theorem and taking a cue from the proof of Theorem 7.20, prove that the curve can be singular at only finitely many points of its zero locus.

Problems 5–11 seek to attach a discrete valuation of the function field of an irreducible affine plane curve to each point of the zero locus at which the curve is nonsingular. Let $\Bbbk$ be a base field, let $f(X, Y)$ be an irreducible polynomial in $\Bbbk[X, Y]$, let $R =$

$\Bbbk[X, Y]/(f(X, Y))$, let x and y be the images of X and Y in R, and let $\mathbb{F}$ be the field of fractions of R. Suppose that $(a, b) \in \Bbbk^2$ has the property that $f(a, b) = 0$. The condition of nonsingularity of f at (a, b) is that one of $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ be nonvanishing at (a, b), and it will be assumed that $\frac{\partial f}{\partial X}(a, b) \neq 0$. Observe from Lemma 7.16 that if S is any integral domain, if s is in S, and if $c(X)$ is in $S[X]$, then $c(X)-c(s) = (X-s)d(X)$ for some $d(X)$ in $S[X]$.

5. Let $f_1(X)$ be the member of $\Bbbk[X]$ defined as above to make $f(X, b) = (X - a)f_1(X)$. Using the fact that $\frac{\partial f}{\partial X}(a, b) \neq 0$, prove that $f_1(a) \neq 0$ and therefore also that $f_1(x) \neq 0$.

6. Let $g(X, Y)$ be a member of $\Bbbk[X, Y]$ with $g(x, y) \neq 0$. Prove that if $g(a, b) = 0$, then there exist $g_1(X)$ in $\Bbbk[X]$ and $h_1(X, Y)$ in $\Bbbk[X, Y]$ with

$$g(X, Y)f_1(X) - f(X, Y)g_1(X) = (Y - b)h_1(X, Y),$$

and deduce that $g(x, y) = (y - b)h_1(x, y)/f_1(x)$.

7. Show that there is a discrete valuation v_1 of $\mathbb{F}$ over $\Bbbk$ with $v_1(y - b) > 0$.

8. If $h(a, b) = 0$ in Problem 6, then the process can be repeated to give

$$g(x, y) = (y - b)^2 h_2(x, y)/f_1(x)^2.$$

It can be repeated again if $h_2(a, b) = 0$, and so on. By applying the valuation v_1 of the previous problem to $g(a, y)$, show that there is an upper bound to the integers $k \geq 0$ such that a nonzero member $g(x, y)$ in R can be written in the form $g(x, y) = (y - b)^k h_k(x, y)/f_1(x)^k$ for some $h_k(x, y)$ in R.

9. (a) Deduce that each nonzero $g(x, y)$ in R is of the form

$$g(x, y) = (y - b)^n h(x, y)/f_1(x)^n$$

with $n \geq 0$, $h(x, y)$ in R, and $h(a, b) \neq 0$, and that the integer n and the member $h(x, y)$ of R are uniquely determined by $g(x, y)$.

(b) Conclude that every nonzero member $g(x, y)$ of the field of fractions $\mathbb{F}$ is of the form $(y - b)^n h_1(x, y)/h_2(x, y)$ with n in $\mathbb{Z}$, $h_1(x, y)$ and $h_2(x, y)$ nonzero in R, $h_1(a, b) \neq 0$, and $h_2(a, b) \neq 0$.

(c) Prove in (b) that $g(x, y)$ uniquely determines n.

10. Write each nonzero $g(x, y)$ in $\mathbb{F}$ as in (b) of the previous problem, and put $v(g) = n$. Also, define $v(0) = \infty$. Show that the resulting function v is a well-defined valuation of $\mathbb{F}$ having R in its valuation ring, taking the value 0 on all members of R that are nonvanishing at (a, b), and having all members of R vanishing at (a, b) in its valuation ideal.

11. Prove that there is only one valuation of $\mathbb{F}$ over $\Bbbk$ taking the value 0 on all members of R that are nonvanishing at (a, b) and having all members of R vanishing at (a, b) in its valuation ideal.

Problems 12–20 compute the genus of certain function fields in one variable. Let $\Bbbk$ be a field of characteristic $\neq 2$, let $f(X)$ be a square-free nonconstant polynomial in $\Bbbk[X]$, let $\mathbb{F} = \Bbbk(X)[Y]/(Y^2 - f(X))$, and let x and y be the images of X and Y in $\mathbb{F}$. In these problems, p denotes a positive integer.

12. Verify that
    (a) the element x is transcendental over $\Bbbk$, y is algebraic over $\Bbbk(x)$ with $y^2 = f(x)$, and $\mathbb{F}$ is a function field in one variable over $\Bbbk$,
    (b) every member of $\mathbb{F}$ is uniquely of the form $a(x) + yb(x)$ with $a(x)$ and $b(x)$ in $\Bbbk(x)$,
    (c) every member of $\mathbb{F}$ not in $\Bbbk$ is transcendental over $\Bbbk$,
    (d) $\mathbb{F}/\Bbbk(x)$ is a Galois extension of degree 2, and the nontrivial element σ of $\mathrm{Gal}(\mathbb{F}/\Bbbk(x))$ satisfies $\sigma(a(x) + yb(x)) = a(x) - yb(x)$ for $a(x)$ and $b(x)$ in $\Bbbk(x)$.

13. Prove that the integral closure of $\Bbbk[x]$ in $\mathbb{F}$ is the ring R of all elements $a(x) + yb(x)$ such that $a(x)$ and $b(x)$ are in $\Bbbk(x)$.

14. (a) Deduce from the previous problem that R is the set of all members z of $\mathbb{F}$ such that $v(z) \geq 0$ for all v in $D_{\mathbb{F}}$ that satisfy $v(x) \geq 0$.
    (b) Deduce from (a) that $L(p(x)_\infty) \subseteq R$.

15. Let v be any member of $D_{\mathbb{F}}$ with $v(x) < 0$.
    (a) Prove that every nonzero $c(x)$ in $\Bbbk[x]$ has $v(c(x)) = (\deg c)v(x)$.
    (b) Prove that $v(y) = \frac{1}{2}(\deg f)v(x)$.
    (c) Prove that if $a(x)$ and $b(x)$ are in $\Bbbk[x]$ with $\deg b + \frac{1}{2}\deg f \leq p$ and $\deg a \leq p$, then $v(a(x) + yb(x)) \geq pv(x)$.

16. Prove that if $a(x)$ and $b(x)$ are in $\Bbbk[x]$ with $\deg b + \frac{1}{2}\deg f \leq p$ and $\deg a \leq p$, then $a(x) + yb(x)$ lies in $L(p(x)_\infty)$.

17. (a) Prove that if v is in $D_{\mathbb{F}}$ and if σ is in $\mathrm{Gal}(\mathbb{F}/\Bbbk(x))$, then the function v^σ defined by $v^\sigma(z) = v(\sigma(z))$ for $z \in \mathbb{F}$ is in $D_{\mathbb{F}}$.
    (b) Why is $v(x) < 0$ if and only if $v^\sigma(x) < 0$?
    (c) Deduce that if z is in $L(p(x)_\infty)$, then so is $\sigma(z)$.

18. (a) Using the previous problem, show that if $a(x)$ and $b(x)$ are in $\Bbbk[x]$ with $a(x) + yb(x)$ in $L(p(x)_\infty)$ and if v is a member of $D_{\mathbb{F}}$ with $v(x) < 0$, then $v(a(x)) \geq pv(x)$ and $v(a(x)^2 - f(x)b(x)^2) \geq 2pv(x)$. Conclude that $\deg a \leq p$ and $\deg(a^2 - fb^2) \leq 2p$.
    (b) Deduce that $L(p(x)_\infty)$ consists of all members $a(x) + yb(x)$ of R such that $\deg a \leq p$ and $\deg b + \frac{1}{2}\deg f \leq p$.

19. Calculate that $\ell(p(x)_\infty) = 2p + 2 - \left[\frac{1}{2}(1 + \deg f)\right]$ if $p \geq \left[\frac{1}{2}(1 + \deg f)\right]$. Here $[\,\cdot\,]$ denotes the greatest integer function.

20. (a) Why is $\deg(x)_\infty = 2$?
    (b) Using Corollary 9.19 with $A = p(x)_\infty$ for a suitable p, prove that the genus of $\mathbb{F}$ is $g = \left[\frac{1}{2}(1 + \deg f)\right] - 1$.

Problems 21–22 compute the genus of certain further function fields in one variable. The notation is as in Problems 12–20 except that $f(X)$ is allowed to have repeated factors. Suppose that $f(X) = g(X)^2 h(X)$, where $h(X)$ is a square-free nonconstant polynomial and $g(X)$ is in $\Bbbk[X]$. Let $\mathbb{F} = \Bbbk(X)[Y]/(Y^2 - f(X))$.

21. With $\mathbb{F}' = \Bbbk(X)[Z]/(Z^2 - h(X))$, exhibit a field isomorphism $\mathbb{F} \to \mathbb{F}'$ fixing $\Bbbk$.

22. Suppose that $f(X)$ has degree 3.
    (a) Prove that $\mathbb{F}$ has genus 1 if $f(X)$ has no repeated root in $\Bbbk$ and that $\mathbb{F}$ has genus 0 otherwise.
    (b) Prove that the affine plane curve $Y^2 - f(X)$ over $\Bbbk$ has a singularity in $\Bbbk_{\text{alg}}^2$ if and only if $f(X)$ has a repeated root in $\Bbbk_{\text{alg}}^2$. Here $\Bbbk_{\text{alg}}$ denotes an algebraic closure of $\Bbbk$.

Problems 23–25 introduce Weierstrass points. Let $\Bbbk$ be an algebraically closed field, and let $\mathbb{F}$ be a function field in one variable over $\Bbbk$ of genus g. Fix a discrete valuation v in $D_{\mathbb{F}}$.

23. Why is it true that $\ell(0v) = 1$, $\ell(1v) = 1$ if $g \geq 1$, $\ell((2g-1)v) = g$, $\ell(2gv) = g + 1$, and $\ell(nv) \leq \ell((n+1)v) \leq \ell(nv) + 1$ for all integers $n \geq 0$?

24. Deduce from the previous problem that there exist exactly g integers $0 < n_1 < n_2 < \cdots < n_g < 2g$ such that there is no x in $\mathbb{F}$ with $(x)_\infty = n_i v$. (Educational note: The integers n_i are called the **Weierstrass gaps** of v, and $(n_1, \ldots, n_g)$ is the **gap sequence** for v. Classically when $\mathbb{F}$ is viewed as the function field of an everywhere nonsingular projective curve, then the points of the zero locus in projective space are in one-one correspondence with the members of $D_{\mathbb{F}}$; with this understanding, the point corresponding to v is called a **Weierstrass point** if the gap sequence for v is anything but $(1, 2, \ldots, g)$. Accordingly let us call v a **Weierstrass valuation** in this case.)

25. Prove that
    (a) v is a Weierstrass valuation if and only if $\ell(gv) > 1$.
    (b) 1 is a Weierstrass gap if $g > 0$.
    (c) v is not a Weierstrass valuation if $g = 0$ or $g = 1$.
    (d) if r and s are positive integers with sum $< 2g$ that are not Weierstrass gaps at v, then $r + s$ is not a Weierstrass gap at v.
    (e) if 2 is not a Weierstrass gap at v, then the gap sequence is $(1, 3, 5, \ldots, 2g-1)$.