Divisor Theory

Harold M. Edwards

Divisor Theory

Springer Science+Business Media, LLC

Harold M. Edwards
Courant Institute of Mathematical Sciences
New York University
New York, New York 10012
U.S.A.

Library of Congress Cataloging-in-Publication Data
Edwards, Harold M.
Divisor theory / Harold M. Edwards.
p. cm.

ISBN 978-0-8176-4976-0 ISBN 978-0-8176-4977-7 (eBook)
DOI 10.1007/978-0-8176-4977-7
QA242.E33 1990
512'.72—dc20 89-28692

Printed on acid-free paper.

Originally published by Birkhäuser Boston, in 1990
Softcover reprint of the hardcover 1st edition 1990

Camera-ready text provided by the author using $\TeX$.
Printed and bound by Edwards Brothers, Inc., Ann Arbor, Michigan.

9 8 7 6 5 4 3 2

Preface

Man sollte weniger danach streben, die Grenzen der mathematischen Wissenschaften zu erweitern, als vielmehr danach, den bereits vorhandenen Stoff aus umfassenderen Gesichtspunkten zu betrachten — E. Study

Today most mathematicians who know about Kronecker's theory of divisors know about it from having read Hermann Weyl's lectures on algebraic number theory [**We**], and regard it, as Weyl did, as an alternative to Dedekind's theory of ideals. Weyl's axiomatization of what he calls "Kronecker's" theory is built—as Dedekind's theory was built—around unique factorization. However, in presenting the theory in this way, Weyl overlooks one of Kronecker's most valuable ideas, namely, the idea that the objective of the theory is to define greatest common divisors, *not* to achieve factorization into primes.

The reason Kronecker gave greatest common divisors the primary role is simple: they are independent of the ambient field while factorization into primes is not. The very notion of primality depends on the field under consideration—a prime in one field may factor in a larger field—so if the theory is founded on factorization into primes, extension of the field entails a completely new theory. Greatest common divisors, on the other hand, can be defined in a manner that does not change at all when the field is extended (see §1.16). Only *after* he has laid the foundation of the theory of divisors does Kronecker consider factorization of divisors into divisors prime in some specified field.

This book gives a full development of a general theory of divisors (Part 1), together with applications to algebraic number theory (Part 2) and the theory of algebraic curves (Part 3). There is a preliminary section (Part 0) on a theorem of polynomial algebra that is a natural foundation of the theory, and an Appendix on differentials, which makes possible the statement

and proof of the Riemann-Roch theorem for curves.

The book began more than ten years ago with an effort to understand Kronecker's theory as it is presented in his treatise *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (§14 et seq.). (For an early version of the result of these efforts, see the Appendix of [**E1**].) In the intervening years, as my understanding of the theory has increased, I have made many simplifications and extensions of it.

The basic idea is simple: For polynomials with rational coefficients, the content of a product is the product of the contents. (The "content" of a polynomial is the greatest common divisor of its coefficients.) The same *should* be true of polynomials with *algebraic* coefficients. However, the notion of "content" has no obvious meaning for a polynomial with algebraic coefficients. The theory of divisors defines the "content" of a polynomial with algebraic coefficients in such a way that the content of a product is the product of the contents.

In fact, this one requirement determines what the content *must* be in any particular case; the only problems are to show that a consistent theory results and to describe in a simple way what that theory is. As the idea is stated above, and as it will be sketched in this preface, it applies to polynomials whose coefficients are *algebraic numbers* (roots of polynomials in one indeterminate with coefficients in the ring of integers $\mathbf{Z}$) but it applies just as well when the integers are replaced by any natural ring (see §1.2).

Let f and g be polynomials (in any number of indeterminates) whose coefficients are algebraic numbers. There is a polynomial h, whose coefficients are algebraic numbers, such that fh has coefficients in $\mathbf{Z}$. (If the coefficients of f are contained in an algebraic number field K, the norm $N_K f$ of f relative to the field extension $K \supset \mathbf{Q}$ has coefficients in $\mathbf{Q}$, and one can take h to be $(N_K f)/f$ times a common denominator of the coefficients of $N_K f$—see §1.17.) The content of f divides the content of g if and only if the content of fh divides

the content of gh (because the contents of fh and gh are the contents of f and g, respectively, times the content of h). But, since fh has coefficients in $\mathbf{Z}$, its content is a positive integer, namely, the greatest common divisor d of the coefficients of fh. Therefore, the statement that the content of fh divides the content of gh has the natural meaning that each coefficient of gh is divisible by d (i.e., the coefficient divided by d is an algebraic integer). Thus, one can *test* whether the content of f divides the content of g by finding an h, determining d, and testing whether the coefficients of gh/d are algebraic integers; the content of f divides the content of g if and only if the answer is yes for all coefficients of gh/d. (See §1.12, Corollary (12).)

The content of a polynomial is, by definition, a *divisor*. As the theory is developed below, the word "content" is not used; the content of f is called "the divisor represented by f." Divisors are represented by polynomials, divisibility of one divisor by another can be tested by the method just described, and two divisors are regarded as *equal* if each divides the other. The task is to show that these definitions result in a consistent theory, and to develop this theory.

The nonzero divisors form a *multiplicative group*. If one specifies an algebraic number field $K \supset \mathbf{Q}$ and restricts consideration to polynomials with coefficients in K, the multiplicative group of divisors coincides with the group of *ideals* in K in the sense of Dedekind. The Kroneckerian theory of divisors has at least three clear advantages over the Dedekindian theory of ideals: (1) It follows from the single, natural premise that the content of the product of two polynomials is the product of the contents. (2) It entails an algorithmic test for divisibility, which, in Dedekindian terms, gives a specific computation for deciding whether a given element is in the ideal generated by a finite set of other elements. (For ideological reasons that are explained in [**E2**], Dedekind made a *virtue* of the lack of such a test in his theory, whereas Kronecker was

of the opposite opinion.) (3) It is independent of the ambient field, so that, unlike the Dedekindian theory, all statements remain true without modification when the ambient field is extended. (The very *definition* of an ideal as a certain kind of subset of the field depends heavily on the ambient field.) Another advantage of the theory of divisors is its applicability to integral and nonintegral divisors alike; the theory of ideals involves both integral and nonintegral ideals, but the integral ideals are far more natural and are usually the only ones introduced in the early stages of the theory.

As was already remarked, the theorem which states that a divisor (or an ideal) can be written in one and only one way as a product of powers of distinct prime divisors (ideals) has meaning only when an ambient field is specified, because only then does the word "prime" have meaning. However, many applications of this theorem require only a decomposition into a product of powers of *relatively* prime divisors, a notion independent of the ambient field. Thus, factorization into primes can often be replaced by Theorem 1 of §1.19, which states that the divisors in any given finite set can be written as products of powers of relatively prime integral divisors.

A second fundamental theorem of divisor theory is the following: An integral divisor divides at least one algebraic integer. Therefore, given an integral divisor A, there is an integral divisor B such that AB is the divisor of an algebraic integer. Theorem 2 (§1.20) states that, given any integral divisor C, one can in fact choose B to be relatively prime to C (i.e., there is an integral divisor B relatively prime to C for which AB is the divisor of an algebraic integer). One corollary of this theorem is that every divisor is the greatest common divisor of just *two* algebraic numbers. Another corollary is a divisibility test of the type used by Kummer in his definition of "ideal prime factors" of cyclotomic integers, the notion with which he initiated divisor theory, in a special case, in 1846. (See also §2.11.)

The remaining topics treated in the general theory of Part 1 all relate to divisors in some particular ambient field. They include divisor class groups, the factorization of prime divisors in normal extension fields, rings of values of a given field at a given integral divisor, discriminants, differents, and ramification. A topic *not* covered in the general theory is the representation of an arbitrary divisor as a product of powers of divisors prime in a given field. The problem of giving, in the general case, an algorithm for factoring an integral divisor into irreducible (prime) factors (see §1.18) appears to be more difficult than the problems treated here. At any rate, it is a problem for which I do not have a solution.

However, in the special case of Part 2—the case of algebraic number fields—it is quite simple to write any given divisor as a product of powers of prime divisors (§2.1). Much of Part 2 is devoted to proving the validity of the following method for factoring the divisor of a prime integer p in an algebraic number field. Let $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ be algebraic integers and let $K = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_\nu)$ be the field they generate over $\mathbf{Q}$. Let $X, u_1, u_2, \ldots, u_\nu$ be indeterminates, let $F(X, u_1, u_2, \ldots, u_\nu)$ be the norm of $X - u_1\alpha_1 - u_2\alpha_2 - \cdots - u_\nu\alpha_\nu$ relative to $K \supset \mathbf{Q}$ (F is a polynomial with coefficients in $\mathbf{Z}$), and let $F \equiv f_1^{e_1} f_2^{e_2} \cdots f_m^{e_m} \bmod p$ be the factorization of $F \bmod p$ into powers of distinct irreducible polynomials with coefficients in the field $\mathbf{Z} \bmod p$. *Normally* the divisor P_i represented by the polynomial $p + f_i(\alpha_1 u_1 + \cdots + \alpha_\nu u_\nu, u_1, u_2, \ldots, u_\nu)$ is prime in K, $P_i \neq P_j$ for $i \neq j$, and $P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m}$ is the divisor of p. For a given set of α's, this is true for all but a finite number of primes p (§2.4). If the α's have the property that every algebraic integer in K can be expressed as a polynomial in the α's with coefficients in $\mathbf{Z}$—and for given K such a set of α's can always be found—it is true for *all* primes p.

This method of factoring the divisor of p was first proposed by Kronecker [**Kr1**, §25], who proposed it in a much more general case than the case of algebraic number fields. The va-

lidity of the method in the number field case was proved by Hensel, but, although Hensel stated [**He**, p. 76] that he had a proof which he would soon publish, I do not know of a proof of Kronecker's more general case. (If one could be given, it would be a large step toward the solution of the problem of factoring divisors in the general case.)

Two other topics treated in Part 2 are Dedekind's discriminant theorem (§2.8) and the factorization of primes in subfields of cyclotomic fields (§2.11).

Application of the theory of divisors to algebraic curves in Part 3 calls for a slight extension of the notion of "divisor." The field of functions K on an algebraic curve over the rationals is an algebraic extension of the natural ring $\mathbf{Q}[x]$ and as such has a divisor theory. This divisor theory depends, however, on the choice of a parameter x on the curve. A *global* divisor in such a field K is the assignment to each parameter x of a divisor A_x in the divisor theory for this parameter in such a way that the divisors A_x "agree on overlaps" in a natural way (§3.4). In Part 3, unless otherwise stated, "divisor" means "global divisor."

Divisor theory provides the following answer to the perennial question "What is a point?" in the theory of algebraic curves. Let K be the field of rational functions on the algebraic curve defined by the equation $F(x, y) = 0$, where F is an irreducible polynomial in two indeterminates with coefficients in $\mathbf{Z}$. Let a and b be algebraic numbers in K such that $F(a, b) = 0$. There is associated to such a pair of algebraic numbers a divisor in K, namely, the numerator of the divisor represented by $(x - a)U + (y - b)V$ (where $x - a$ and $y - b$ are elements of K, and U and V are indeterminates). If (a, b) is a *nonsingular* point of $F = 0$, that is, if the partial derivatives of F at (a, b) are not both zero, the divisor in K obtained in this way is called a *place* (see §3.13). Places can also be characterized as divisors in K which are prime in K and in all extensions of K obtained by adjoining constants to K (§3.22). Yet another

characterization of places is as divisors for which the ring of values coincides with the field of constants of K.

Places capture algebraically the notion of a point on a curve. For example, the origin $(0,0)$ does not give rise to a place on the folium of Descartes $x^3+y^3-xy=0$, but, rather, gives rise to a *product of two* places, namely, the zero and the pole of the "function" x/y on this curve. That the origin is a product of two places expresses the geometrical "fact" that the origin is a double point of the folium of Descartes (§3.13).

A fundamental theorem states that every divisor in the field of functions K on an algebraic curve, can, when suitable constants are adjoined, be written as a product of powers of places (§3.18). (This theorem relates divisors as they are treated in this book to divisors as they are customarily defined in the theory of algebraic curves as formal sums of places with integer coefficients, or, equivalently, as formal products of places with integer exponents.) The *degree* of a divisor is equal to the number of places in the numerator of such a representation of the divisor minus the number of places in the denominator. The degree of the divisor of an element x of K is always 0, and the places in its numerator are naturally thought of as "the points where x is zero" and the places in its denominator as "the points where x has poles."

Divisor theory also provides the following natural formulation of Abel's theorem: For any given function field (of one variable, over $\mathbf{Q}$) there is a least integer g, the genus of the field, such that every divisor of degree g is equivalent to an integral divisor. Otherwise stated, given a set of zeros and a set of poles, there is a function on the curve with poles, at most, at the given poles and zeros at the given zeros (plus, possibly, other zeros) provided the number of given poles is at least g greater than the number of given zeros. This theorem is not immediately recognizable as Abel's theorem, but the connection with Abel's own statement is explained in §3.25. (See also the Corollary of §3.27.)

An element of K can be expanded in a natural way in powers of a local parameter at a place P in K (§3.16). The *principal part* of an element of K at P, relative to a given local parameter at P, is the terms of this power series expansion which have negative degree. (In particular, the element of K has a pole at P if and only if its principal part at P, relative to any local parameter at P, is nonzero.) Let $P_1, P_2, \ldots, P_k$ be a given set of places in the field K of rational functions on an algebraic curve, and let Γ be the elements of K which have poles only at the P_i and whose poles at the P_i have order N at most. The principal parts of an element of Γ are described by Nk constants of K. Abel's theorem easily implies that the principal parts of elements of Γ form a subspace of codimension at most g of K_0^{Nk}. The Appendix is devoted to proving that *this subspace of K_0^{Nk} can be described in terms of differentials.* Specifically, differentials are defined in the Appendix, and it is shown that (1) g is the dimension of the vector space (over the field of constants K_0 of K) of holomorphic differentials, (2) the sum of the residues of any differential is zero, and (3) the conditions "any element of K times any holomorphic differential must have the sum of its residues equal to zero" give necessary and sufficient conditions for determining which elements of K_0^{Nk} are principal parts of elements of Γ. (For N large, these conditions are also independent, so that the codimension is exactly g when N is large.) The Riemann-Roch theorem is a simple corollary of this method of determining the principal parts of elements of Γ.

I wish once again to thank the Vaughn Foundation for more than a decade of support which made an enormous difference in my life and work.

Contents