Harold M. Edwards

Essays in Constructive Mathematics

With Contribution by David A. Cox

Second Edition

Springer

Essays in Constructive Mathematics

Harold M. Edwards

Essays in Constructive Mathematics

Second Edition

With Contribution by David A. Cox

Springer

Harold M. Edwards (Deceased)
New York, NY, USA

With Contribution by
David A. Cox
Department of Mathematics and Statistics
Amherst College
Amherst, MA, USA

ISBN 978-3-030-98557-8 ISBN 978-3-030-98558-5 (eBook)
https://doi.org/10.1007/978-3-030-98558-5

Mathematics Subject Classification: 00A35, 00-01, 01A55, 03F65, 12-01, 12F10, 14H05, 14K20

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

For Betty

To the Reader

Harold Edwards published his book *Essays in Constructive Mathematics* in 2005 but continued to think deeply about the themes discussed in the essays. At the time of his death in November 2020, Edwards was completing a long essay that contained his final thoughts on three of his favorite topics: Galois's first memoir, points on an algebraic curve, and Abel's theorem.

The literary form of the essay goes back to Michel de Montaigne, whose *Essais* were first published in 1580. The 1588 edition added new essays, and the 1595 posthumous edition was heavily revised. In other words, Montaigne's *Essais* were not static—they evolved and grew in scope as his thoughts developed over the years. The same is true for Professor Edwards and how he thought about his *Essays*.

This new edition of the *Essays* consists of two parts. Part I contains of the original *Essays* from 2005 with typographical corrections. Part II is based primarily on Edwards's final manuscript, with additions that supply missing details and enhance the connection to the essays in Part I. However, the two parts are largely independent of each other, so either part can be read without having to worry about the other. The Postscript describes the changes and additions made to Edwards's manuscript.

Part I consists of Chapters 1–5, each divided into sections that are the essays. Part II has a similar structure, with Chapters 6–9 also divided into essays. Thus, "Essay 2.3" means the third essay of Chapter 2.

More details about the precise contents of Parts I and II can be found in the synopses of each part. The reader should also consult the preface of each part to hear Edwards's unique voice as he introduces the mathematics to follow.

Harold Edwards and I interacted often over the years, sometimes in person at the Joint Meetings but more typically by email. We shared interests in algorithmic algebra and the history of mathematics, though we had different points of view. For example, I love the Hilbert basis theorem, which Edwards did not regard as being remotely constructive. In spite of our differences, I came to respect and admire his approach to constructive mathematics.

Let me give an example of his approach. Chapters 4 and 9 discuss Abel's theorem from his 1826 Paris memoir. This paper is not easy reading for many reasons. Morris Kline, one of Edwards's mentors at NYU, wrote in his book *Mathematical Thought from Ancient to Modern Times* that Abel's paper "was very difficult to understand, partly because he tried to prove what we would today call an existence theorem by actually computing the result" [51, p.655]. For Edwards, the *only* way to prove existence is via an explicit construction or algorithm, i.e., by "computing the result" or by giving an algorithm for doing so. His way of doing mathematics is consequently not always easy, but it is deeply satisfying—when you are done, you know how to compute explicitly everything you have done. This is good mathematics.

But these are my words. It is now time to turn the stage over to Harold Edwards to see what he has to say about this wonderful subject that we all love.

Acknowledgements I am grateful to Betty Rollin and Michael Edwards for making Edwards's manuscript available to me. Thanks also to Michael Singer for making me aware of the reference [17].

Amherst, MA, USA David A. Cox
2022

Harold M. Edwards
1936–2020

Harold Edwards was born in 1936 in Champaign, Illinois. After getting a B.A. from the University of Wisconsin and a M.A. from Columbia University, he went on to earn a Ph.D. from Harvard in 1961, writing a thesis under the direction of Raoul Bott. He taught at New York University from 1966 until his retirement in 2002. He lived in New York City with his wife, writer and journalist Betty Rollin.

His first book *Advanced Calculus* was published in 1969. This was followed by *Riemann's Zeta Function* in 1974 and *Fermat's Last Theorem* in 1977. These two books earned him the Leroy P. Steele Prize for Mathematical Exposition in 1980. He went on to write numerous other books, including the *Essays* in 2005 and *Higher Arithmetic: An Algorithmic Introduction to Number Theory* in 2008.

He also wrote many papers on the history of mathematics, with Galois and Kronecker among his favorite subjects. In 2005, he was awarded the Albert Leon Whiteman Memorial Prize, which recognizes notable exposition and exceptional scholarship in the history of mathematics.

When the American Mathematical Society began its Fellows program, he was among the inaugural class of Fellows in 2013.

Contents

Part I
The Original Essays

Preface to Part I

> *He* [Kronecker] *was, in fact, attempting to describe and to initiate a new branch of mathematics, which would contain both number theory and algebraic geometry as special cases.*—André Weil [83]

This book is about mathematics, not the history or philosophy of mathematics. Still, history and philosophy were prominent among my motives for writing it, and historical and philosophical issues will be major factors in determining whether it wins acceptance.

Most mathematicians prefer constructive methods. Given two proofs of the same statement, one constructive and the other not, most will prefer the constructive proof. The real philosophical disagreement over the role of constructions in mathematics is between those—the majority—who believe that to exclude from mathematics all statements that cannot be proved constructively would omit far too much, and those of us who believe, on the contrary, that the most interesting parts of mathematics can be dealt with constructively, and that the greater rigor and precision of mathematics done in that way adds immensely to its value.

Mathematics came to a fork in the road around 1880. On one side, Dedekind, Cantor, and Weierstrass advocated accepting transfinite "constructions" like those needed to prove the Bolzano–Weierstrass "theorem." On the other, Kronecker argued that no such departure from the standards of proof adhered to by Dirichlet and Gauss was necessary and that the Aristotelian exclusion of completed infinites could be maintained. As we all know, the first group carried the day, and the Dedekind–Cantor–Weierstrass road was the one taken.

The new orthodoxy was consolidated by Hilbert a century ago, and has reigned ever since, despite occasional challenges, notably from Brouwer and Bishop. During this century, the phrase "foundations of mathematics" has come to mean for most working mathematicians the complex of ideas surrounding the axioms of set theory and the axiom of choice, matters that for Kronecker had no mathematical meaning at all, much less foundational meaning.

Why, a hundred years after this choice was made, and made so decisively, do I believe that the road Kronecker proposed might win new consideration? The

advent of computers has had a profound impact on mathematics and mathematicians that has already altered views about the nature and meaning of mathematics in a way favorable to Kronecker. The new technology causes mathematics to be taught and experienced in a much more computational way and directs attention to *algorithms*. In other words, it fosters constructive attitudes. My own preference for constructive formulations was shaped by my experience with computer programming in the 1950s, and computer programming at that time was trivial by today's standards.

No evidence supports the image that is so often presented of Kronecker as a vicious and personal critic of Cantor and Weierstrass—another instance of history being written by the victors. As far as I have been able to discover, Kronecker vigorously opposed the *views* of Cantor and Weierstrass, as well as those of Dedekind, with whom he was on far better terms, but he was not hostile to the men themselves. Moreover, his opposition to their views—which was of course reciprocated—was rarely expressed in his publications. In the rare instances in which he mentioned such issues, he merely stated his belief that the new ways of dealing with infinity that were coming to be accepted were *unnecessary*. Instead of excoriating nonconstructive methods, as legend would have us believe, he concentrated his efforts on backing up his beliefs with concrete mathematical results proved constructively.

No one doubts that Kronecker was one of the giants of nineteenth-century mathematics, but it is often said that he succeeded in his works because he ignored the strictures that he advocated in his philosophy. This view of the relation of Kronecker's mathematics to his philosophy is often ascribed to Poincaré, but as I have written elsewhere, this ascription is based on a misinterpretation of a passage in which Poincaré writes about issues unrelated to the treatment of infinity in mathematics. Indeed, no one who has studied Kronecker's works could believe that he accepted completed infinites or made use of nonconstructive arguments. Like many other mathematicians since, he was impatient with the philosophy of mathematics and wanted only to get on with his mathematics itself, but for him "mathematics" was always constructive.

That attitude inspires these essays. My goal has been not to argue against the prevailing orthodoxy, but to show that substantial mathematics can be done constructively, and that such mathematics is interesting, illuminating, and concordant with the new algorithmic spirit of our times. I have given examples of what I mean by constructive mathematics, without trying to define it. The underlying idea is well expressed in the essay of Poincaré mentioned above, in which he says that the guiding principle for both Kronecker and Weierstrass was to "derive everything from the natural numbers" so that the result would "partake of the certainty of arithmetic." I regard the natural numbers not as a completed infinite set but as a means of describing the activity of *counting*. (See Essay 1.1.) The essence of constructive mathematics for me lies in the insistence upon treating infinity, in Gauss's phrase, as a *façon de parler*, a shorthand way of describing ideas that need to be restated in terms of finite calculations when it comes to writing a formal proof.

It will surely be remarked that almost all of the topics treated in the essays come from algebra and number theory. They not only partake of the certainty of arithmetic, as Poincaré says, they *are* arithmetic—what Kronecker called "general arithmetic." (Again, see Essay 1.1.) But there are three exceptions. In Essay 4.4, Newton's polygon is treated as a method of constructing an infinite series, which means, constructively, as an algorithm for generating arbitrarily many terms of the series. Convergence is not an issue because the theory treats the series themselves, not their limits in any sense. In Essay 5.1, a complex root of a given polynomial—a convergent sequence of rational complex numbers whose limit is a root of the polynomial—is found by an explicit construction. Finally, Essay 5.4, which sketches a proof of the spectral theorem for symmetric matrices of integers, necessarily deals with real numbers, that is, with convergent sequences of rationals.

An essay is "a short literary composition on a single subject, usually presenting the personal views of the author." There is nothing literary about these essays, but they do treat their mathematical subjects from a personal point of view. For example, Essay 5.1 explains why the "fundamental theorem of algebra" is misnamed—in a very real sense it isn't even true—and Essay 1.2 explains why Euclid's statement of Proposition 1 of Book 1 of the *Elements*, "On a given finite straight line to construct an equilateral triangle" is better than "Given a straight line segment, there exists an equilateral triangle of which it is one of the sides," the form in which most of Euclid's present-day successors would state it. These are my opinions. To my dismay, it is incessantly borne in on me how few of my colleagues share them and how completely mathematicians today misunderstand and reject them. These compositions try—they essay—to present them in a way that will permit the reader to see past the preconceptions that stand between what I regard as a commonsense attitude toward the study of mathematics and the attitudes most commonly accepted today. They essay to reopen the Kroneckerian road not taken.

Acknowledgments

I am profoundly grateful to Prof. David Cox, who provided encouragement when it was sorely needed, and backed it up with sound advice. I also thank Professors Bruce Chandler, Ricky Pollack, and Gabriel Stolzenberg for friendship and for many years of stimulating conversation about the history and philosophy of mathematics.

Most of all, I thank my wife, Betty Rollin, to whom this book is dedicated, for more than I could ever enumerate.

New York, New York Harold Edwards
2005

Synopsis of Part I

The essays of Part I are divided into five chapters:

Chapter 1. A Fundamental Theorem
Chapter 2. Topics in Algebra
Chapter 3. Some Quadratic Problems
Chapter 4. The Genus of an Algebraic Curve
Chapter 5. Miscellany

The fundamental theorem of Chapter 1 constructs a splitting field for a given polynomial. As is shown in Chapter 2, the case in which the given polynomial has coefficients in a ring of the form $\mathbf{Z}[c_1, c_2, \ldots, c_v]$—a ring of polynomials in some set of indeterminates $c_1, c_2, \ldots, c_v$ with integer coefficients—suffices for the apparently more general case of a polynomial $f(x)$ whose coefficients are "algebraic quantities" in a very general sense. For this reason, only polynomials with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ are considered in Chapter 1.

Another way to state the problem "Construct a splitting field for a given polynomial" is "Extend the notion of computation with polynomials with integer coefficients in such a way that the given polynomial can be written as a product of linear factors." Computation in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ involves just addition, subtraction, and multiplication, but it extends to computations involving division in the field of quotients of the integral domain $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ in the same way that computation in the ring of integers extends to computation in the field of rational numbers. As Gauss's lemma shows (Essay 1.4), this extension does not affect the factorization of polynomials. A simple *further* extension of $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ is effected by "adjoining" *one* root of a *monic, irreducible* polynomial with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ to the field of rational functions. This simple construction, which Galois used with amazing success, although with some lack of rigor, is generally known as a "simple algebraic extension" of the field of quotients of $\mathbf{Z}[c_1, c_2, \ldots, c_v]$. For the sake of brevity, I have called a field constructed in this way the "root field" of the monic, irreducible polynomial used in its construction (Essay 1.3).

With this specific description of the way in which computations in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ are to be extended, the construction problem to be solved becomes, "Given a polynomial f with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$, find an auxiliary polynomial g with coefficients in the same ring such that g is monic and irreducible and such that its root field splits f" in the sense that f can be written as a product of linear factors with coefficients in the root field of g.

The problem, then, is, "Given f construct g." The solution in Chapter 1 is iterative. Suppose that g is a failed attempt at a solution. Thus, the factorization of f over the root field of g contains at least one irreducible factor of degree greater than 1. The iteration needs to construct a *better* attempt at a solution. Specifically, it needs to construct a new auxiliary polynomial, call it g_1, with the property that the factorization of f over the root field of g_1 contains more linear factors than does the factorization of f over the root field of g. If g_1 fails to split f, the same procedure can be applied again to find a g_2 that gives f more linear factors than g_1 did. Since the number of linear factors of f increases with each new g, and since the number of such factors is bounded above by the degree of f, such an iteration must eventually reach a solution of the problem—an attempted g that does not fail.

To make this sketch into an actual iterative construction of a splitting field for f requires two main steps. First, given f and an attempt at g, one needs to be able to *factor f when it is regarded as a polynomial with coefficients not in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ but in its extension, the root field of g*. The difficult step in the construction of a splitting field for f is the algorithmic solution of this factorization problem. The algorithm is set forth in Essay 1.5, with examples, and the proof that it achieves its objective is in Essay 1.6. The relation of the algorithm to Kronecker's solution of the same factorization problem is among the subjects discussed in Essay 1.7. Second, one needs to describe explicitly how to pass from a g that fails to split f to a new g_1 that comes closer to splitting f. The underlying idea of the construction is simple: Because g does not split f, there is an irreducible factor, call it ϕ, of f over the root field of g whose degree is greater than 1. *Adjoin to the root field of g a root of ϕ*. This double adjunction, first of a root of g and then of a root of ϕ, gives a field over which f has more linear factors—a field in which f has more roots—because it contains a root of ϕ, and the root field of g did not. The problem is to write this double adjunction as a simple one—specifically as the field obtained by adjoining a root of a new g_1 with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$. The construction of such a g_1 is given in Essay 1.8.

Finally, although there are infinitely many polynomials g that split f, there is only one *splitting field* of f in the sense that if g is a *minimal* splitting polynomial of f—one that is itself split by any polynomial that splits f—the root field of g is isomorphic to the root field of any other minimal splitting polynomial of f.

The end result is a theorem that in my opinion deserves the name "Fundamental Theorem of Algebra" much more than the theorem that is and probably always will be known by that name: *Given a polynomial f* (in one variable) *with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ there is an explicit way to extend rational computations in $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ so that f factors into linear factors; moreover, any two minimal*

ways of doing this are isomorphic. For the relation of this theorem to the "Fundamental Theorem of Algebra" see Essay 5.1.

The theorem of Chapter 1 that has just been described is implicitly contained—with no hint of a proof—in Lemma III of Galois's treatise [42] on the algebraic solution of equations (see [34]). In this sense, it is the foundation of Galois theory. The connection is explained in Essays 2.1 and 2.3. Essay 2.2 is devoted to justifying Kronecker's assertion that *every field of algebraic quantities is isomorphic to the root field of a polynomial with coefficients in some* $\mathbf{Z}[c_1, c_2, \ldots, c_v]$ as that concept was defined in Chapter 1. This fact is the basis of Kronecker's later view—despite the fact that he had previously given the title *Foundations of an Arithmetical Theory of Algebraic Quantities* to his major publication—that "algebraic quantities" were unnecessary in mathematics and that algebraic questions should be studied using "general arithmetic" instead (see Essay 1.1).

The algorithmic description of fields of algebraic quantities in terms of "adjunction relations" in Essay 2.3 gives a construction of the splitting field of a polynomial that is very close to Chebotarev's in his excellent but little-known book on Galois theory [15].

The construction of the splitting field of a *general* monic polynomial of degree n in Essay 2.4 proves another basic theorem of Galois—another to which Galois gave no hint of a proof—that the Galois group of an nth-degree polynomial $f(x)$ whose coefficients are 'letters' is the full symmetric group. The splitting field is explicitly given by adjunction relations $f_i(\alpha_i) = 0$, where

$$f_i(x) = \frac{f(x)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{i-1})} \tag{1}$$

is the irreducible polynomial satisfied by a root α_i of $f(x)$ whose coefficients are polynomials in the roots $\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$ already adjoined. (The right side of (1), as it stands, is of course not a polynomial; it becomes one once $i-1$ roots $\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$ of $f(x)$ have been adjoined and the divisions (1) calls for have been performed.) The degree $n!$ of the extension is of course the product of the degrees of these adjunction relations. The nub of the matter is the proof that each $f_i(x)$ is *irreducible* over the field generated by $\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$. These ideas stem from Kronecker, as does the fundamental theorem of divisor theory in Essay 2.5.

Chapter 3 deals with different matters altogether. Its primary inspiration is Gauss's proof of quadratic reciprocity in Section 5 of the *Disquisitiones Arithmeticae* [43], but the proof is recast by translating it from a study of *quadratic forms* and their *composition* to a study of *modules* and their *multiplication*. The "modules" involved are entities of the following type. With "number" meaning a number $0, 1, 2, \ldots$, let a "hypernumber" for a given A mean an expression $y + x\sqrt{A}$ in which x and y are numbers. Such hypernumbers can be added and multiplied, and, when the sizes of the coefficients allow it, subtracted as well. It is natural to assume that the given A is *not a square*, because otherwise, $y + x\sqrt{A}$ would be a number, and nothing new would be found by computing with hypernumbers. It will also be

assumed that A is *positive*, but this assumption is made for the sake of simplicity and has no particular justification except that the case of positive A suffices for the proof of quadratic reciprocity.

Let $m_1, m_2, \ldots, m_\mu$ be a list of hypernumbers. Two hypernumbers a and b will be said to be *congruent mod* $[m_1, m_2, \ldots, m_k]$, denoted by $a \equiv b \bmod [m_1, m_2, \ldots, m_\mu]$, if they can be made equal by adding sums of multiples (with multipliers that are hypernumbers) of $m_1, m_2, \ldots, m_\mu$ to each. This is a simple generalization of Gauss's definition of $a \equiv b \bmod m$, which means that a and b can be made equal by adding multiples of m to each. (This form of the definition eliminates the need for negative numbers in the discussion of congruences.) A **module** is a list of hypernumbers $[m_1, m_2, \ldots, m_\mu]$ written between square brackets to indicate that they are to be used to define a congruence relation in this way. Two modules are **equal** if they define the same congruence relation. Essay 3.2 gives all these definitions, along with an algorithm for determining whether two given modules are equal.

When the product of two lists is defined to be the list that contains all products with one term from the first list and one from the second, the module determined by the product depends only on the modules determined by the factors, so the operation gives a way to multiply *modules*. Since the multiplication defined in this way is clearly associative and commutative, the modules for a given A form a *commutative semigroup* in which the module $[1]$ is an identity.

One more level of abstraction is needed for the most interesting construction. Let a module be called **principal** if it can be represented by a list $[y + x\sqrt{A}]$ with just one hypernumber and if, in addition, that hypernumber satisfies $y^2 > Ax^2$. The principal modules are a *subsemigroup* of the semigroup of modules—which means simply that a product of principal modules is principal—so there is an associated quotient structure: Two modules are **equivalent** if they can be made equal by multiplying each by a principal module. (That is, $M_1 \sim M_2$ means there are principal modules P_1 and P_2 for which $M_1P_1 = M_2P_2$.) The equivalence classes of modules for a given A defined in this way form a *finite semigroup*, which I call the **class semigroup**. It can be determined for each given A by algorithms described in Essay 3.3. These algorithms are essentially the same as Gauss's methods in Section 5 of the *Disquisitiones* for determining the equivalence classes of binary quadratic forms for a given "determinant" A, but in my opinion they are simpler in conception. Some rudimentary facts about class semigroups are proved in Essay 3.4 that are then used in Essay 3.5 to prove the law of quadratic reciprocity.

The final two essays of Chapter 3 relate the multiplication of modules to Gauss's composition of binary quadratic forms by showing how, given two binary quadratic forms, the theory of multiplication of modules can be used to *determine whether there is a third binary quadratic form that composes them* in Gauss's sense, and, if so, *to find all such compositions*. Once this connection is clearly made, it seems to me that the module-and-multiplication formulation will have more appeal than the form-and-composition formulation. But whether or not the module-and-multiplication version is preferred over Gauss's, it has the advantage

of relating directly to Gauss's, thereby making Gauss's masterpiece more accessible to modern readers whose familiarity with Dirichlet's simplification of it may, for reasons explained in Essay 3.6, be an impediment.

Chapter 4, on the genus of an algebraic curve, is inspired by Abel's great memoir of 1826 [2] (first published, thanks to the negligence of the Paris Academy, in 1841). The inspiration for the algorithmic method of Chapter 4 goes back even further, to Newton's method of constructing infinite series expansions of algebraic functions, commonly known today as "Newton's polygon."

The construction used in Chapter 4 (see Essay 4.1) to describe the genus of a curve is based on ideas of Abel that predate the theory of Riemann surfaces by many years, and it makes no reference to complex numbers, much less to Riemann surfaces. Let an algebraic curve $\chi(x, y) = 0$ be given (where χ is an irreducible polynomial with integer coefficients that contains both x and y and, for simplicity, is monic in y), and let a large number N of points on the curve also be given. Choose a rational function θ on the curve with many zeros (it will have equally many poles, of course) including zeros at all of the N given points. An **algebraic variation** of the N points is a variation of the N points that can be achieved as a variation of the N special zeros of the rational function θ when the coefficients of θ are varied in such a way that the remaining zeros and all of the poles remain unchanged. (It is assumed that the N given zeros are points where x is finite, and the poles are specifically taken to be the poles of x^v for some large v, but in fact any set of poles will do, as long as there are enough of them, and the zeros can also be at points where x is infinite.) The N zeros then vary with $N - g$ degrees of freedom, where the number g, the **genus** of the curve, depends only on the curve, not on the other choices.

To make this rough *idea* of the genus of $\chi(x, y) = 0$ into a *definition* requires, of course, that much more be said. Although the natural first step might seem to be the introduction of complex numbers in order to deal rigorously with the zeros and poles of θ on $\chi(x, y) = 0$, the approach taken in Chapter 4 is quite the opposite: It dispenses with the notion of zeros and poles altogether. Just as the degree of a polynomial determines the number of its roots, general conditions on rational functions θ can be related heuristically to the notions of zeros and poles of θ on the curve $\chi(x, y) = 0$ and their locations. On this basis, one can give a satisfactory description of rational functions θ on $\chi(x, y) = 0$ with prescribed poles of prescribed multiplicity, all in terms of "general arithmetic"—the arithmetic of polynomials with integer coefficients. Then Abel's description of the genus can be given solid, constructive meaning in terms of the number of free coefficients in θ when conditions are placed on its zeros and poles, a description that uses nothing but general arithmetic. Essay 4.2 relates Abel's construction to Euler's addition formula for elliptic curves and to the geometric description of addition on an elliptic curve that is so familiar in the present time of great interest in elliptic curves. Essay 4.3 gives the details of the definition of the genus of $\chi(x, y) = 0$ in these terms.

Essay 4.4 is an exposition of the Newton algorithm. The task of the algorithm is to construct a solution y of $\chi(x, y) = 0$ as an infinite series of (possibly) fractional powers of x. In constructive mathematics an infinite series must of course be presented as an *algorithm* that generates the successive terms of the series, and this

is what the Newton algorithm does. More precisely, the input to the algorithm is a truncated series solution y of $\chi(x, y) = 0$ and the algorithm generates one further term of the series. In the early stages, a truncated solution may be *ambiguous*, meaning that it may be extended in more than one way, and the algorithm must determine all possible extensions; eventually, as is proved in the essay, a set of *unambiguous* truncated solutions is reached, each of which is prolonged by the algorithm with the addition of one more term in just one way and therefore represents an infinite series solution. (Note that convergence is not an issue, because the series itself—not any kind of limit of the series—is the objective.)

Essay 4.5 gives an algebraic method of evaluating the genus as it was defined in Essay 4.3. Essay 4.6 gives a simpler description of the genus as the dimension of the vector space of **holomorphic differentials** on the curve. These differentials are the ones that have no poles, and they have the property that the algebraic variations of a set of N points on the curve are described by the differential equations

$$\sum_{i=1}^{N} h_j(x_i, y_i)\, dx_i = 0 \quad \text{for } j = 1, 2, \ldots, g,$$

where the differentials $h_j(x, y)\, dx$ are a basis of the space of holomorphic differentials. Essay 4.7 uses the holomorphic differentials on a curve to state and prove the Riemann–Roch theorem as a formula for the number of arbitrary constants in a rational function with given poles.

The last essay of Chapter 4 proves that the genus is a birational invariant, even though the method of Essay 4.5 for computing it depends on the choice of a parameter x on the curve. This important result can be stated as follows: In the terminology of Essay 2.2, the field of rational functions on an algebraic curve is an algebraic field of transcendence degree one. The **genus** as it is defined above depends only on this field itself, not on the particular presentation of it as a root field that is used in the definition. This conclusion is established, in essence, by showing that if x and z are different parameters on the curve then $h\, dx$ is a holomorphic differential (relative to the parameter x) if and only if $h \cdot \frac{dx}{dz} \cdot dz$ is a holomorphic differential (relative to the parameter z), so the spaces of holomorphic differentials in the two cases are isomorphic.

The miscellany of Chapter 5 begins with a proof of what is called the Fundamental Theorem of Algebra—in fact two proofs of it. But my main point in that essay is that this theorem is not truly a theorem of algebra at all because it relates in an essential way to the nonalgebraic notion of complex numbers. The next essay gives a proof of the Sylow theorems in the theory of finite groups, and the following two summarize the constructive and algorithmic approach of my 1995 book on linear algebra. My hope is that *Linear Algebra* [35] and the present book will reinforce one another—this book making the case for the clarifying power of algorithmic methods and *Linear Algebra* giving yet another example of that power. The final essay is a further correction to the Kronecker legend.

Chapter 1
A Fundamental Theorem

Essay 1.1 General Arithmetic

> *La dernière chose qu'on trouve en faisant un ouvrage c'est de savoir celle qu'il fallait mettre la première.* (The last thing one discovers in composing a work is what should be put first.)—Pascal, *Penseés*

Kronecker quoted this saying of Pascal in the first of a series of lectures he gave on the concept of number.[1] It may have been a somewhat rueful reflection on his own experience with his 1881 treatise *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (Elements of an Arithmetical Theory of Algebraic Quantities) [56], which contains at least two indications that he altered his point of view profoundly while writing it, deciding ultimately that the subject of his title was not the one he should be dealing with at all. In his introduction to the treatise and in point IV of its last section he speaks of reducing the entire theory of "algebraic quantities" to the theory of rational functions of variables. In later works he did just that. For example, in *Ein Fundamentalsatz der allgemeinen Arithmetik* [60] and *Über den Zahlbegriff* [61], both published in 1887, he emphasized the importance of rational computation with polynomials with integer coefficients and again stated that theories of algebraic numbers and algebraic quantities could be reduced to such rational computations. Thus, whether or not it was the last thing he discovered in writing his 1881 treatise, Kronecker came to believe that he should have begun with rational algebra. That is where these essays begin.

Elsewhere Kronecker said, "In mathematics, I recognize true scientific value only in concrete mathematical truths, or, to put it more pointedly, only in mathematical formulas" (see [33]). I would rather say "computations" than "formulas," but my view is essentially the same. Computation, in turn, is an outgrowth of counting, and in this sense mathematics is founded on *numbers*, not as abstract "objects" of any

[1] These lectures, given in the last year of Kronecker's life, 1891, are preserved in the form of a handwritten transcript in the archives of the mathematics library of the University of Strasbourg, and were published in 2001 [63].

H. M. Edwards, *Essays in Constructive Mathematics*,
https://doi.org/10.1007/978-3-030-98558-5_1

Fig. 1.1 Kronecker

kind, but as the system of symbols by which we record the results of counts. We learn to use and understand the symbols 0, 1, 2, 3, . . . at an early age, and most of us understand fairly soon that the important thing is not the actual names or symbols that are used, or even the decimal system on which they are based, but the mere fact that there are agreed-upon symbols and names and an agreed-upon system for counting. In this essay, the word "number" will mean a number 0, 1, 2, . . . in this most basic sense.

The more sophisticated computations that we learn later in life grow out of counting. First, the operations of addition and multiplication are grounded in counting. (Counting first to a then to b is the same as counting to $a + b$. Counting a times to b is the same as counting to ab.) Subtraction—the inverse of addition—of course makes sense only when the number being subtracted is not larger than the one from which it is to be subtracted. However, experience teaches us to widen our horizon in such a way that this limitation on subtraction can be put in the background and for the most part ignored. This can be done very conveniently in the way Kronecker (shown in Fig. 1.1) does it in the essay *Über den Zahlbegriff* (On the Concept of Number), mentioned above.

He first introduces "*Buchstabenrechnung*," calculation with letters, in the following way: "The same laws [that govern the addition and multiplication of numbers] needed to be regarded as valid for calculation with letters as soon as letters began to be used to represent numbers whose determination might or should be postponed. With the introduction of the principle of computing with indeterminates *as such*, which originated with Gauss, the special theory of whole numbers broadened into the general arithmetical theory of polynomials with whole number coefficients."[2]

[2] Dieselben Gesetze mussten für die sogenannte Buchstabenrechnung als maassgebend angenommen werden, sobald man anfing, die Buchstaben zur Bezeichnung von Zahlen zu verwenden, deren Bestimmung vorbehalten bleiben kann oder soll. Aber mit der *principiellen* Einführung der "Unbestimmten" (indeterminatae), welche von *Gauss* herrührt, hat sich die specielle Theorie der

In particular, we can compute with—add and multiply—polynomials in a single indeterminate t whose coefficients are numbers. When we use Gauss's notation $f(t) \equiv g(t) \bmod (t+1)$ to mean that $f(t)$ can be transformed into $g(t)$ using the identity $t+1 \equiv 0 \bmod (t+1)$, we then have a system of computation in which t plays the role of -1. This system of computation is what we mean by *the ring of integers*.

In modern notation, these observations can be abbreviated $\mathbf{Z} = \mathbf{N}[t] \bmod (t+1)$, meaning that an element of $\mathbf{Z}$—an integer—is represented by an expression of the form $a_0 t^n + a_1 t^{n-1} + \cdots + a_n$, where $\mathbf{N}$ denotes the set of numbers $\{0, 1, 2, \ldots\}$, where t is an indeterminate, and where $n, a_0, a_1, \ldots, a_n$ are numbers. Two such representations *by definition* represent the same element of $\mathbf{Z}$ if one can be transformed into the other using $t+1 \equiv 0 \bmod (t+1)$ in conjunction with the usual laws that govern addition and multiplication of numbers. Since $t^2 \equiv t^2 + (t+1) \equiv t^2 + t + 1 \equiv t(t+1) + 1 \equiv 1 \bmod (t+1)$, we can always replace t^2 with 1. Therefore, we can replace t^3 with t, t^4 with t^2 and then with 1, and so forth, to represent any integer by an expression of the form $at + b$, where a and b are numbers. Two such expressions represent the same integer, that is, $at + b \equiv ct + d \bmod (t+1)$, if and only if $at + b + a + c \equiv ct + d + a + c \bmod (t+1)$, which is to say $b + c \equiv d + a \bmod (t+1)$. Since this congruence does not involve t, it is equivalent to the equation $b + c = d + a$. In short, the simple device of computation with polynomials in $t \bmod t+1$ is all that is needed to describe the usual construction of the ring of integers as ordered pairs of numbers (a, b) subject to the equivalence relation "$(a, b) \equiv (c, d)$ means $a + d = b + c$" when equivalence classes are added and multiplied in the obvious ways. As Kronecker observes, the interpretation of the equation $7 - 9 = 3 - 5$ truly involves this *new meaning* of the equal sign.

In essence, the device of using integers instead of numbers makes it possible to do computations without bothering about whether particular subtractions are possible unless a reason arises to examine that issue. Similarly, it makes possible writing all terms of an equation on one side of the equal sign, which greatly simplifies reasoning by eliminating the need to consider separately cases in which the terms would appear on different sides of the equation if numbers were used instead of integers.

The fourth rational operation, division, is the most interesting one. The division of *numbers* naturally takes the form of *division with remainder*: Two numbers a and b with $b \neq 0$ determine numbers q and r by the conditions $a = qb + r$ and $r < b$. This operation is of course very closely connected to the original meaning of Gauss's congruence concept $a \equiv r \bmod b$.

In the more general setting of *Buchstabenrechnung*—computing with polynomials in several indeterminates whose coefficients are numbers—the notion of *divisibility* has a clear meaning, but the more useful concept of division with remainder does not. An exception is the case of division by a polynomial with integer coefficients that is *monic* in one of its indeterminates, meaning that $b = x^n +$ terms of degree less than n in x. In this case, for any polynomial a with integer coefficients, there are unique polynomials q and r with integer coefficients for which $a = qb + r$ and for which the degree of r in x is less than the degree n of b in x.

---

ganzen Zahlen zu der allgemeinen arithmetischen Theorie der ganzen ganzzahligen Functionen von Unbestimmten erweitert.

Another role played by division in elementary arithmetic is the *cancellation law of multiplication*: If $ab = ac$ and $a \neq 0$, then $b = c$. This law is obviously valid for numbers—even for integers. Its validity in other contexts, when equality is replaced by some kind of congruence, is often a crucial issue. When it is valid, the ring of congruence classes under addition and multiplication is an **integral domain**. For an integral domain one can construct a *field of quotients*, the set of all formal quotients p/q in which $q \neq 0$, when $p/q = p'/q'$ is defined to mean $pq' = p'q$ and when addition and multiplication are defined by $(p/q) + (p'/q') = (pq' + p'q)/qq'$ and $(p/q)\cdot(p'/q') = pp'/qq'$. However, for the most part fields of quotients themselves—for example, the field of rational numbers—will be avoided. The *potential* of one, the ability to compute with formal quotients of elements of an integral domain, is enough.

Toward the end of his life, Kronecker adopted the term "general arithmetic" (*allgemeine Arithmetik*) for the arithmetic of rings of the form $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$, which is to say rings of polynomials in some set of indeterminates $c_1, c_2, \ldots, c_\nu$ with integer coefficients (or, in conformity with the approach above, rings $\mathbf{N}[t, c_1, c_2, \ldots, c_\nu] \bmod (t + 1)$, where $\mathbf{N}$ denotes the set of numbers). Of course there is little to be said about these rings themselves; rather, the substance of general arithmetic lies in the study of certain further constructions that use them.

Kronecker wrote a number of papers about what he called **module systems**, and he formulated his proof of his *Fundamentalsatz* of general arithmetic in terms of module systems. For me, however, his module systems pose difficulties. For one thing, a module system in its simplest form—namely, a ring of the form $\mathbf{Z}[c_1, c_2, \ldots, c_\nu] \bmod [M_1, M_2, \ldots, M_\mu]$, a polynomial ring in which computations are done modulo a finite number of given relations $M_i \equiv 0$—is not normally a field because division is not normally possible. Therefore, one needs to enlarge the realm of objects with which one computes in some way in order to allow the computations to use the most convenient and natural representations of them—for example to allow the use of $\omega = \frac{-1+\sqrt{-3}}{2}$ in computations with $\sqrt{-3}$. For another thing, this description $\mathbf{Z}[c_1, c_2, \ldots, c_\nu] \bmod [M_1, M_2, \ldots, M_\mu]$ of module systems opens the door to the problem of determining *whether two such module systems are isomorphic*, which is tantamount to the "ideal membership problem" for rings of the form $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$, a problem that poses serious difficulties[3] from a constructive point of view.

For these reasons, I have avoided module systems[4] and have instead used the concrete notion of a simple algebraic extension of the field of quotients of a ring $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$; such simple algebraic extensions are described and given the name "root fields" in Essay 1.3. As will be shown in Essay 2.2—using an argument Kronecker himself gave [56, §2]—fields of this type provide a setting for all algebraic computations.

[3] Much serious work has been done on the ideal membership problem and the related problem of constructing Gröbner bases, but since I have not been able to understand this work in a way that is consistent with my notions of constructivity, I am glad that it is unnecessary for the topics I develop here.

[4] *Specific* module systems in which the problems mentioned above do not arise are used in some of the constructions—for example in Essays 1.5 and 2.4.

Essay 1.2 A Fundamental Theorem

> *Proposition V. Problème. Dans quel cas une équation est-elle soluble par de simples radicaux?* (Proposition V. Problem. In what case is an equation solvable by simple radicals?—É. Galois [42]

The essays that follow contain applications of general arithmetic to a variety of topics, one of which is the theorem Kronecker stated and proved in his 1887 paper *Ein Fundamentalsatz der allgemeinen Arithmetik* (On a Fundamental Theorem of General Arithmetic) [60]. This theorem states, roughly, that *every polynomial has a splitting field*.

Proposition 1 of Book 1 of Euclid's *Elements* [39] is, in the Heath translation, "On a given finite straight line to construct an equilateral triangle." To modern ears, this seems a strange way to state a proposition. A modern writer would be more likely to say, "Given a finite straight line, there is an equilateral triangle of which it is one of the sides." But Euclid has many such propositions. His propositions fall into two categories, often described as "problems" and "theorems." That Proposition 1 is a "problem" is signaled not only by the form of its statement but also by the fact that its proof ends with "as was to be done" rather than "as was to be proved." Gauss on at least one occasion[5] concludes a proof with QEF ("quod erat faciendum"—that which was to be done) instead of QED ("quod erat demonstrandum"—that which was to be demonstrated), and Galois in his treatise [42] on the algebraic solution of equations presents eight "propositions," five of which are "theorems," two of which are "problems," and one of which is a "lemma," but today the designation "problem" has disappeared from formal mathematical exposition, and the designation "proposition" has become more or less synonymous with "theorem."

The usual definition of "constructive mathematics" is that it requires existence theorems to be proved constructively—that is, constructive mathematics does not accept as a proof of existence an argument that assumes a *disproof* of existence and derives a contradiction. But the very notion of an "existence theorem" reflects a nonconstructive bias. Is it not ridiculous to say, "Every polynomial has a splitting field," and then to stipulate that "The proof will give an actual construction of a splitting field"? Is it not more reasonable to follow the Euclidean model and say "Given a polynomial, construct a splitting field for it," thereby making clear that the proof is a construction?

In these essays I do follow the Euclidean model, except that I have decided to use the word "theorem" for both types of Euclidean "propositions." Mathematicians today regard "theorems" as the fundamental units of mathematics. Kronecker used the term *Fundamentalsatz* even though his theorem was in truth a construction. I doubt that an effort to give another term like "problem" or "construction" the same status as "theorem" would succeed. And a "fundamental problem" or a "fundamental construction" would be much less imposing than a "fundamental theorem." Thus,

[5] See §73 of *Disquisitiones Arithmeticae* [43]. The notation QEF at the end of §73 was omitted from the German translation by Maser.

these essays, although they will not contain "existence theorems," will contain many theorems that are constructions, including the theorem of this essay.

Gauss's doctoral dissertation of 1799 [44] was devoted to a proof of a theorem very close to what is now called the "fundamental theorem of algebra": *A polynomial of degree n has n complex roots* when they are counted with multiplicities. In the dissertation he sharply criticizes earlier attempts to prove the theorem, saying that they used computations with the roots and that such computations virtually assumed the truth of the theorem to be proved. However, as Bashmakova and Rudakov point out in an essay on the history of the theorem [53], Gauss returned to the theorem in 1815 and gave a new proof that took an approach very similar to the one he had criticized in 1799; he justified *on other grounds* certain limited computations with the roots of the given polynomial, and then used such computations to show that the roots could be described as complex numbers. (For this second proof, see Essay 5.1.)

Kronecker, with his *Fundamentalsatz*, came to the realization that *this is the theorem:* what is important is not the complex numbers but, rather, the fact that computations with the roots can be justified. That is, *given a polynomial with integer coefficients, one can describe a system of computation that extends computations with integers in such a way that the polynomial has a number of roots equal to its degree*.

In a pragmatic sense, Galois had realized the same thing more than fifty years earlier. Lemma III of his treatise on the algebraic solution of equations [42], which was written in 1830–1831 even though it was not published until 1846, is in essence a construction of a splitting field for a given polynomial. Unfortunately, Galois does not prove Lemma III. He does give a construction of a splitting field, but the construction uses computations with the roots! Thus, from a foundational point of view, what Galois proved was that *if* there is any valid way to compute with the roots of a polynomial, *then* computations with the roots can always be done using what is now called a Galois resolvent, as in his Lemma III. Until computations with the roots were validated—until Kronecker's *Fundamentalsatz* was proved—Galois theory was without a general foundation, even though splitting fields could be constructed in specific cases.

For example, in the case of the polynomial $x^3 - 2$, the polynomial $y^6 + 108$ is a Galois resolvent, which is to say that computations in $\mathbf{Q}[y] \bmod (y^6 + 108)$ extend computations in the field of rational numbers $\mathbf{Q}$ in such a way that $x^3 - 2$ factors into linear factors, as is shown by the formula

$$(1) \qquad x^3 - 2 \equiv \left(x - \frac{y^4}{18}\right)\left(x + \frac{y^4 - 18y}{36}\right)\left(x + \frac{y^4 + 18y}{36}\right) \bmod (y^6 + 108).$$

Putting aside for the moment the question of how such a formula might be constructed, one can easily check that it is correct; the product of the last two factors is $\frac{1}{36^2}((36x + y^4)^2 - 324y^2) \equiv \frac{1}{36^2}(36^2x^2 + 72xy^4 + y^2(-108) - 324y^2) \equiv x^2 + \frac{x}{18}y^4 - \frac{1}{3}y^2 \bmod (y^6 + 108)$, and multiplication of this result by the first factor gives $x^3 + \frac{x^2}{18}y^4 - \frac{x}{3}y^2 - \frac{x^2}{18}y^4 - \frac{x}{18^2}y^2(-108) + \frac{1}{54}(-108) \equiv x^3 - 2 \bmod (y^6 + 108)$.

Otherwise stated, the formula proves that adjunction to the field $\mathbf{Q}$ of a root y of $y^6 + 108 = 0$ gives a field over which $x^3 - 2$ splits into linear factors.

Kronecker states the more general version

$$x^3 - c \equiv \left(x - \frac{y^4}{9c}\right)\left(x + \frac{y^4 - 9cy}{18c}\right)\left(x + \frac{y^4 + 9cy}{18c}\right) \bmod (y^6 + 27c^2) \tag{2}$$

of this formula in his *Fundamentalsatz* paper [60, end of §2]. This version, too, is easy to check even if it is not easy to guess. It proves that adjunction to the field of rational functions in c of a root y of $y^6 + 27c^2$ gives a field over which $x^3 - c$ splits into linear factors.

The general case is developed and proved in the next few essays in the form of the following theorem:

Fundamental Theorem *Given a polynomial f in x with integer coefficients, construct a polynomial g in y with integer coefficients that is irreducible, monic in y, and has the property that a formula of the form*

$$f(x) \equiv a_0 \prod \left(x - \frac{\phi_i(y)}{\psi_i}\right) \bmod g(y) \tag{3}$$

holds, in which the $\phi_i(y)$ are polynomials whose coefficients are integers, the ψ_i are nonzero integers, and a_0 is the leading coefficient of f.

More generally,
Given a polynomial f in $x, c_1, c_2, \ldots, c_\nu$ with integer coefficients, construct a polynomial g in $y, c_1, c_2, \ldots, c_\nu$ with integer coefficients that is irreducible, monic in y, and gives rise to a formula (3), in which the $\phi_i(y)$ are now polynomials in $y, c_1, c_2, \ldots, c_\nu$ with integer coefficients, the ψ_i are nonzero polynomials in $c_1, c_2, \ldots, c_\nu$ with integer coefficients, and a_0 is the leading coefficient of f as a polynomial in x.

To say that $g(y)$ is monic in y means that g has the form $y^n + \cdots$ where the omitted terms all have degree less than n in y. As will be seen in Essay 1.3, this assumption simplifies computations mod $g(y)$. The requirement that g be irreducible guarantees that $\mathbf{Z}[y, c_1, c_2, \ldots, c_\nu] \bmod g(y, c_1, c_2, \ldots, c_\nu)$ (where ν may be zero) will be an integral domain. In modern parlance, the field of quotients of this integral domain is a splitting field of f as a polynomial with coefficients in the field of rational functions in $c_1, c_2, \ldots, c_\nu$. It is obtained by adjoining a root y of g to this field of rational functions.

A familiar example of a splitting of this sort, put in an unfamiliar way, is

$$ax^2 + bx + c \equiv a\left(x - \frac{-b + y}{2a}\right)\left(x - \frac{-b - y}{2a}\right) \bmod (y^2 - b^2 + 4ac).$$

Here use is made of the fact that y is a square root of $b^2 - 4ac \bmod (y^2 - b^2 + 4ac)$ to express the roots of the quadratic polynomial $ax^2 + bx + c$ in the form $(-b \pm y)/2a$. The stated congruence is easily verified by rewriting the right side as $\frac{a}{4a^2}(2ax + b -$

$y)(2ax + b + y) = \frac{1}{4a}(4a^2x^2 + 4abx + b^2 - y^2) \equiv \frac{1}{4a}(4a^2x^2 + 4abx + 4ac) \bmod (y^2 - b^2 + 4ac)$.

Another example that is considerably less simple to verify is

$$\begin{aligned} x^4 - x^2 - 1 \equiv & \left(x - \frac{7y^7 + 220y^5 - 1846y^3 + 9003y}{18966}\right) \\ & \cdot \left(x + \frac{7y^7 + 220y^5 - 1846y^3 + 9003y}{18966}\right) \\ & \cdot \left(x - \frac{7y^7 + 220y^5 - 1846y^3 - 9963y}{2 \cdot 18966}\right) \\ & \cdot \left(x + \frac{7y^7 + 220y^5 - 1846y^3 - 9963y}{2 \cdot 18966}\right) \\ & \bmod (y^8 - 10y^6 + 47y^4 - 110y^2 + 841). \end{aligned}$$

(See Example 1 of Essay 2.3.)

Essay 1.3 Root Fields (Simple Algebraic Extensions)

In brief, one adjoins a root y of $g(y)$ by computing with expressions of the form $p(y)/q$, where $p(y)$ is a polynomial in y and q is nonzero; addition and multiplication are performed in the obvious ways, while division is accomplished by "rationalizing the denominator."

Here the given polynomial $g(y)$ is assumed to be an irreducible polynomial with integer coefficients—or, more generally, with coefficients in the ring $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$ of polynomials with integer coefficients in some given set $c_1, c_2, \ldots, c_\nu$ of indeterminates—that is monic in y. The advantage of assuming that $g(y)$ is monic in y is that it means that division with remainder can be used to find, for any polynomial in y, another polynomial congruent to it mod $g(y)$ whose degree is less than $n = \deg g$. Since a polynomial of degree less than $n = \deg g$ can be divisible by $g(y)$ only if it is zero, it follows that *every polynomial in y with coefficients in $\mathbf{Z}[c_1, c_2, \ldots, c_\nu]$ is congruent mod $g(y)$ to one and only one such polynomial whose degree in y is less than n*. Thus, the ring $\mathbf{Z}[y, c_1, c_2, \ldots, c_\nu] \bmod g(y)$ can be described as the elements of $\mathbf{Z}[y, c_1, c_2, \ldots, c_\nu]$ whose degrees are less than $n = \deg g$, added in the usual way and multiplied by ordinary multiplication of polynomials followed by division with remainder by $g(y)$ to find a polynomial congruent to the product mod $g(y)$ whose degree in y is less than n.

The advantage of the assumption that $g(y)$ is irreducible is that it implies—as will be proved in the next essay—that the ring $\mathbf{Z}[y, c_1, c_2, \ldots, c_\nu] \bmod g(y)$ defined in this way is an *integral domain*. Therefore, as described in Essay 1.1, there is an associated *field of quotients*. It is this field of quotients of the integral domain $\mathbf{Z}[y, c_1, c_2, \ldots, c_\nu] \bmod g(y)$ that I will call the **root field** of $g(y)$. Another way to