Preface to the English Edition

This book is a translation of the second edition of my German book *Algebra für Einsteiger: Von der Gleichungsauflösung zur Galois-Theorie*, Vieweg, 2004. The original German edition has been expanded by the addition of exercises. The goal of the book is described in the original preface. In a few words it can be sketched as follows: Galois theory is presented in the most elementary way, following the historical evolution. The main focus is always the classical application to algebraic equations and their solutions by radicals. I am grateful to David Kramer, who did more than translate the present book, having also offered several suggestions for improvements. My thanks are also directed to Ulrike Schmickler-Hirzebruch, of Vieweg, who first proposed a translation to the American Mathematical Society, and to Edward Dunne, of the AMS, for managing the translation.

Jörg Bewersdorff

Translator's Note

I wish to express my appreciation to Jörg Bewersdorff for his helpful collaboration on the translation and to the following individuals at the American Mathematical Society: Edward Dunne for entrusting me with this project, Barbara Beeton for her friendly and intelligent TEXnical support, and Arlene O'Sean for her careful copyediting of the translation.

David Kramer

Prefaces to the German Editions

Math is like love; a simple idea, but it can get complicated.

— R. Drabek

Preface to the First German Edition

The subject of this book is the history of a classical problem in algebra. We will recount the search for formulas describing the solutions of polynomial equations in one unknown and how a succession of failures led finally to knowledge of a quite unexpected sort, and indeed, of fundamental importance in mathematics.

Let us look briefly at the object that enticed many of the world's best mathematicians over a period of three centuries. Perhaps, dear reader, you recall from your school days quadratic equations of the form

$$x^2 - 6x + 1 = 0$$

as well as the "quadratic formula"

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

for the solution of the "general" quadratic equation

$$x^2 + px + q = 0.$$

If we apply this formula to our example, we obtain the two solutions

$$x_1 = 3 + 2\sqrt{2} \quad \text{and} \quad x_2 = 3 - 2\sqrt{2}.$$

If you are interested in a numerical solution, you can pull out your handy pocket calculator (or perhaps you know how to compute square roots by hand) and obtain the decimal representations $x_1 = 5.828427\ldots$ and $x_2 = 0.171572\ldots$. You could also use your calculator to verify that these values are in fact solutions to the original equation. A skeptic who wished to verify that the solutions derived from the formula are the exact solutions would have to substitute the expressions containing the square roots into the equation and demonstrate that the quadratic polynomial $x^2 - 6x + 1 = 0$ actually vanishes—that is, assumes the value zero—at the values $x = x_1$ and $x = x_2$.

The Solution of Equations of Higher Degree. It has long been known how to solve cubic equations such as

$$x^3 - 3x^2 - 3x - 1 = 0$$

by means of a formula similar to the quadratic formula. Indeed, such formulas were first published in 1545 by Cardano (1501–1676) in his book *Ars Magna*. However, they are quite complicated, and have little use for numerical calculation. In an age of practically unlimited computing power, we can do without such explicit formulas in practical applications, since it suffices completely to determine the solutions by means of numeric algorithms. Indeed, for every such equation in a single variable there exist approximation methods that iteratively, that is, step by step, compute the desired solution more and more precisely. Such a procedure is run until the solution has reached an accuracy suitable for the given application.

However such iterative numeric procedures are unsuitable when not only the numerical value of a solution is sought, such as $x_1 = 3.847322\ldots$ in the previous example, but the "exact" value

$$x_1 = 1 + \sqrt[3]{2} + \sqrt[3]{4}.$$

It is not only that such an algebraic representation possesses a certain aesthetic quality, but in addition, a numeric solution is insufficient if one hopes to derive mathematical knowledge and principles from the solution of the equation. Let us hypothesize, for example, based on numeric calculation, the following identities:

$$\sqrt[3]{\sqrt[3]{2}-1} = \frac{1}{3}\left(\sqrt[3]{3}-\sqrt[3]{6}+\sqrt[3]{12}\right),$$

$$e^{\pi\sqrt{163}} = 262537412640768744,$$

and

$$2\cos\frac{2\pi}{17} = -\frac{1}{8}+\frac{1}{8}\sqrt{17}+\frac{1}{8}\sqrt{34-2\sqrt{17}} + \frac{1}{4}\sqrt{17+3\sqrt{17}-\sqrt{34-\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

Without going into detail, it seems plausible that behind such identities, if indeed they are correct, lie some mathematical laws. A direct check to determine whether they are in fact correct or are merely the result of chance numeric approximation would be difficult.[1]

But back to Cardano. In addition to the solution for cubic equations, Cardano published in his *Ars Magna* a general formula for quartic equations, that is, equations of the fourth degree, also known as biquadratic equations. Using such formulas, the equation

$$x^4 - 8x + 6 = 0$$

[1] I will reveal that only the first and third identities are correct. The first was discovered by the Indian mathematician Ramanujan (1887–1920) and can be easily checked. The third, which will be discussed in Chapter 7, contains within it a proof that the regular heptadecagon (seventeen-sided polygon) can be constructed with straightedge and compass.

The second equation is not exact. The actual value of the right-hand side is

$$262537412640768743.9999999999992501\ldots.$$

However, this approximate identity is more than mere chance. It is based on some deep number-theoretic relationships. For more on this, see Philip J. Davies, Are there coincidences in mathematics? *American Mathematical Monthly* 88 (1981), pp. 311–320.

can be shown to have the solution

$$x_1 = \frac{\sqrt{2}}{2}\left(\sqrt{\sqrt[3]{4+2\sqrt{2}}+\sqrt[3]{4-2\sqrt{2}}}\right.$$
$$\left.+\sqrt{-\sqrt[3]{4+2\sqrt{2}}-\sqrt[3]{4-\sqrt{2}}+2\sqrt{2\sqrt[3]{3+2\sqrt{2}}+2\sqrt[3]{3-2\sqrt{3}}-2}}\right).$$

With the almost simultaneous discovery of formulas for solving third- and fourth-degree equations came the inevitable problem of finding similar formulas for equations of higher degree. To accomplish this, the techniques that were used for the cubic and quartic equations were systematized, already in Cardano's time, so that they could be applied to equations of the fifth degree. But after three hundred years of failure, mathematicians began to suspect that perhaps there were no such formulas after all.

This question was resolved in 1826 by Niels Henrik Abel (1802–1829), who showed that there cannot exist general solution formulas for equations of the fifth and higher degree that involve only the usual arithmetic operations and extraction of roots. One says that such equations cannot be *solved in radicals*. The heart of Abel's proof is that for the intermediate values that would appear in a hypothetically existing formula, one could prove corresponding symmetries among the various solutions of the equation that would lead to a contradiction.

Galois Theory. A generalization of Abel's approach, which was applicable to all polynomial equations, was found a few years later by the twenty-year-old Évariste Galois (1811–1832). He wrote down the results of his researches of the previous few months on the evening before he was killed in a duel. In these writings are criteria that allow one to investigate any particular equation and determine whether it can be solved in radicals. For example, the solutions to the equation

$$x^5 - x - 1 = 0$$

cannot be so expressed, while the equation

$$x^5 + 15x - 44 = 0$$

has the solution

$$x_1 = \sqrt[5]{-1+\sqrt{2}} + \sqrt[5]{3+2\sqrt{2}} + \sqrt[5]{3-2\sqrt{2}} + \sqrt[5]{-1-\sqrt{2}}.$$

Of much greater significance than such solutions is the method that Galois discovered, which was unorthodox, indeed revolutionary, at the time, but today is quite usual in mathematics. What Galois did was to establish a relationship between two completely different types of mathematical objects and their properties. In this way he was able to read off the properties of one of these objects, namely the solvability of a given equation and the steps in its solution, from those of the corresponding object.

But it was not only the principle of this approach that benefited future mathematics. In addition, the class of mathematical objects that Galois created for the indirect investigation of polynomial equations became an important mathematical object in its own right, one with many important applications. This class, together with similar objects, today forms the foundation of modern algebra, and other subdisciplines of mathematics have also progressed along analogous paths.

The object created by Galois that corresponds to a given equation, called today the *Galois group*, can be defined on the basis of relations between the solutions of the equation in the form of identities such as $x_1^2 = x_2 + 2$. Concretely, the Galois group consists of renumberings of the solutions. Such a renumbering belongs to the Galois group precisely if every relationship is transformed by this renumbering into an already existing relationship. Thus for the case of the relation $x_1^2 = x_2 + 2$ in our example, the renumbering corresponding to exchanging the two solutions x_1 and x_2 belongs to the Galois group only if the identity $x_2^2 = x_1 + 2$ is satisfied. Finally, every renumbering belonging to the Galois group corresponds to a symmetry among the solutions of the equation. Moreover, the Galois group can be determined without knowledge of the solutions.

The Galois group can be described by a finite table that is elementary but not particularly elegant. Such a table is called a *group table*, and it can be looked upon as a sort of multiplication table, in which each entry is the result of operating on two elements of the Galois group in succession. An example is shown in Figure 0.1. What is significant about the Galois group, and its corresponding group table, is that it always contains the information about whether, and if so, how, the underlying equation can be solved in radicals. To be sure, the proof of this in a concrete application can be quite involved; nevertheless, it can always be accomplished in a finite number of steps according to a fixed algorithm.

	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	A	J	F	G	H	I
C	C	D	E	A	B	I	J	F	G	H
D	D	E	A	B	C	H	I	J	F	G
E	E	A	B	C	D	G	H	I	J	F
F	F	G	H	I	J	A	B	C	D	E
G	G	H	I	J	F	E	A	B	C	D
H	H	I	J	F	G	D	E	A	B	C
I	I	J	F	G	H	C	D	E	A	B
J	J	F	G	H	I	B	C	D	E	A

Figure 0.1. The Galois group of the equation $x^5 - 5x + 12$ is represented as a table by means of which the solvability in radicals can be determined by purely combinatorial means. This equation will be considered in detail in Section 9.17. Equations of the fifth degree that are not solvable in radicals have tables of size 60×60 or 120×120.

Today, Galois's ideas are described in textbooks in a very abstract setting. Using the class of algebraic objects that we previously mentioned, it became possible at the beginning of the twentieth century to reformulate what has come to be called Galois theory, and indeed in such a way that the problem itself can be posed in terms of such objects. More precisely, the properties of equations and their solution can be characterized in terms of associated sets of numbers whose common characteristic is that they are closed under the four basic arithmetic operations. These sets of numbers are called *fields.*

Thus starting with a given equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

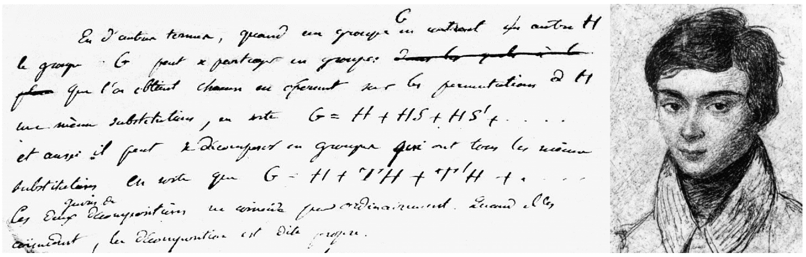
one forms the smallest set of numbers that contains all quantities, such as

$$\frac{a_2}{a_0} - a_1^2 + a_0,$$

that can be obtained from the coefficients of the equation using successive basic arithmetic operations. Then one obtains an enlarged set of numbers that is of particular use in studying the given equation by allowing in one's calculations, in addition to the coefficients of the equation, the solutions $x_1, x_2, \ldots$. This set is therefore formed of all numbers that can be obtained from expressions of the form, for example,

$$\frac{a_0}{a_2}x_1^2 - a_2 x_2 + a_1.$$

If it now possible to represent the solutions of the given equation by nested expressions involving radicals, then one can obtain additional fields of numbers by allowing in addition to the coefficients some of these nested radicals. Thus every solution of an equation corresponds to a series of nested fields of numbers, and these can be found, according to the main theorem of Galois theory, by analysis of the Galois group. Thus by an analysis of the Galois group alone, one can answer the question whether the solutions of an equation can be expressed in radicals.



En d'autres termes, quand un groupe G en contient un autre H
le groupe G peut se partager en groupes ~~dans les quels il entre~~
~~par~~ que l'on obtient chacun en opérant sur les permutations de H
une même substitution, en sorte $G = H + HS + HS' + \ldots$
et aussi il peut se décomposer en groupes qui ont tous les mêmes
substitutions en sorte que $G = H + TH + T'H + \ldots$
Ces deux genres de décompositions ne coïncide pas ordinairement. Quand elles
coïncident, la décomposition est dite propre.

Figure 0.2. Évariste Galois and a fragment from his last letter. In this passage he describes how a group G can be decomposed with the help of the subgroup H. See Section 10.4.

This abstraction achieved at the beginning of the twentieth century and today basically unchanged marks both the end of a historical process during which interest in the problem that we have described has shifted in focus: For Cardano and his contemporaries the main problem was to find concrete solutions to explicit problems using procedures of general applicability. But soon the point of view shifted and the focus was on the important properties of the equations. Beginning with Galois, but in full force only after the turn of the twentieth century, the focus shifted drastically. Now abstract classes of objects such as groups and fields became the basis for the formulation of a host of problems, including those that inspired the creation of these objects in the first place.[2]

About This Book. In order to reach as wide an audience as possible (assumed is only general knowledge obtained from college courses in mathematics), no attempt has been made to achieve the level of generality, precision, and completeness that are the hallmarks of mathematical textbooks. The focus will be rather on ideas, concepts, and techniques, which will be presented only insofar as they are applicable to some concrete application and make further reading in the extensive literature possible. In such a presentation, complicated proofs have no place. However, proofs are without doubt the backbone of any serious engagement with mathematics. In the spirit of compromise, difficult proofs, except those in the last chapter, are set off from the main text so that gaps in the logic can be avoided without the flow of the narrative being interrupted.

Considerable emphasis is placed on the historical development of the subject, especially since the development of modern mathematics in recent centuries is much less well known than that of the natural sciences, and also because it can be very interesting to be able to give a time-lapse view of false starts and important discoveries.

[2] In particular, many important applications have been found in modern information theory, in particular in cryptography, as in, for example, the public key codes realized in 1978. In these asymmetric encryption procedures, the key for encoding is made public without creating the risk of unauthorized decoding. The mathematical basis for such public key encryption algorithms as RSA and ElGamal is computations carried out in special algebraic objects with a very large—but finite—number of elements (precisely, the objects are residue class rings and elliptic curves defined over finite fields). An introduction to this subject can be obtained from Johannes Buchmann, *Introduction to Cryptography*, Springer, 2004.

And furthermore, a presentation that follows the historical development has the advantage of making many mathematical abstractions seem the natural consequence of individual investigations, so that one never gets the impression of starting with an unmotivated definition somehow descended from heaven in a completely arbitrary manner. At the same time, we are able to leave out a great deal of material that would be necessary to include in a work seeking great generality. However, we must mention a significant drawback to our approach: Many complicated calculations will be necessary, even if they are of an elementary nature, whose results would be more simply derived from a qualitative point of view on the basis of general principles.

In order to make this book as distinct as possible from mathematical textbooks, I have chosen the same style of presentation as in my book *Luck, Logic, and White Lies.* Every chapter begins with a simple, usually more or less rhetorical, question that gives the reader an idea of the nature and level of difficulty of the chapter ahead, even if the chapter usually goes far beyond simply answering the question posed. This structure should also offer the more mathematically sophisticated reader, for whom the overview offered here will often be too superficial and incomplete, a quick way of determining which parts of the book are of particular interest, after which the references to the literature will indicate a path of additional reading.

The topics of the individual chapters are too closely woven together to make it possible to read the chapters independently of one another. Nevertheless, the reader who is interested in only a particular aspect of the subject is encouraged to plunge directly into the relevant chapter. Even if one then encounters a reference to another chapter, at least the details of the calculations carried out there will be unnecessary for an understanding of the following chapters. Of course, the beginning of every chapter offers the opportunity to start over if the details of the previous chapter became too difficult.

The reader who wishes to keep the very abstract passages at a greater distance might adhere to the following plan:

- In Chapters 1 through 6 the proofs in the set-off sections may be skipped.

- For understanding the following chapters, the only part of Chapter 7 that is necessary is the first part, which deals with the regular heptadecagon (17-gon).
- Chapter 8 can be omitted entirely.
- In Chapter 9 the set-off sections at the end of the chapter may be skipped.
- Chapter 10 and the epilogue may also be omitted.

Readers who wish to follow a typical “Algebra I” course should place Chapters 9 and 10, which deal with Galois theory, as well as the epilogue, at the center of their reading. For a deep understanding of the subject the following are of particular importance: the main theorem on symmetric polynomials (Chapter 5), the factorization of polynomials (Chapter 6), and the ideas around cyclotomy (the division of the circle) (Chapter 7). How much relative attention should be given to the remaining chapters depends on the reader’s interests and prior knowledge.

Following the historical development of the subject, the presentation on the solvability of equations is divided into three parts:

- Classical methods of solution, based on more or less complicated equivalent reformulations of equations, were used historically for deriving the general formulas for quadratic, cubic, and quartic equations (Chapters 1 through 3).
- Systematic investigation of the discovered solution formulas becomes possible when one expresses the intermediate results of the individual calculational steps in terms of the totality of the solutions being sought (Chapters 4 and 5). This leads to the solution of equations in special forms, namely, those that are less complex than those in the general form in that they exhibit particular relationships among the solutions that can be formulated as polynomial identities. In addition to equations that can be broken down into equations of lower degree (Chapter 6), the so-called cyclotomic equations $x^n - 1 = 0$ are examples of such less-complex equations (Chapter 7). Finally, in this part should be included the attempt, described in Chapter 8, at finding a

general solution formula for fifth-degree equations, the result of which is a formula that works only in special cases.

- Based on systematic attempts at finding solution formulas, we finally arrive at the limits of solvability of equations in radicals. These limits, as recognized and investigated by Abel and Galois, are dealt with, aside from a brief preview in Chapter 5, in Chapters 9 and 10. The focus here is on Galois groups.

  With the investigation of Galois groups we reach a level of difficulty well beyond that of the first chapters. Therefore, two different presentations are given. In Chapter 9 a relatively elementary overview is given, supplemented by numerous examples, in which the scope of the concepts introduced is reduced as much as possible. The resulting holes are filled in Chapter 10, which leads to the main theorem of Galois theory, which involves the mathematical objects called fields referred to earlier, which are closed under the four basic arithmetic operations. The discussion of these objects will be limited to those aspects relevant to Galois theory.

The reader who wishes to deepen his or her understanding of Galois theory beyond what is contained in this book can move on to any textbook on modern algebra. One might mention as representatives of these books the two classics *Algebra*, by Bartel Leendert van der Waerden (1903–1996), and *Galois theory*, by Emil Artin (1898–1962), whose first editions appeared in 1930 and 1948. But conversely, the present book can be seen as an extension of the usual algebra textbooks in the direction of providing examples and historical motivation.

Acknowledgments

I would like to thank all those who shared in the creation of this book: I received considerable advice about errors and infelicities from Jürgen Behrndt, Rudolf Ketter, and Franz Lemmermeyer. Thanks to their help I was able to reduce the number of errors considerably, though of course the errors that remain are my fault entirely. I thank Vieweg-Verlag and its program director Ulrike Schmickler-Hirzebruch for having accepted this book for publication. Finally, I thank my

wife, Claudia, without whose often tried patience this book could not have been written.

Preface to the Second German Edition

The pleasant circumstance that this book's first edition sold out in only two years gives me the opportunity to expand the bibliography and to correct some errors spotted by several alert readers, particularly Daniel Adler, Ulrich Brosa, Kurt Ewald, Volker Kern, Ralf Krawczyk, and Heinz Lüneburg.

Preface to the Third German Edition

I again have alert readers to thank for the discovery of errors: Erwin Hartmann, Alfred Moser, and David Kramer, who is also the translator of the English-language edition. Finally, I have fulfilled my frequently mentioned desire to provide the book with a set of exercises for the reader.

The Author's Coordinates. Readers are encouraged to report errors or infelicities via e-mail to `mail@bewersdorff-online.de`. Questions will also be answered to the extent possible. Additions and corrections will be published on my website: `http://www.bewersdorff-online.de`. The AMS will also maintain a web page for this book. The URL can be found on the back cover.

Jörg Bewersdorff