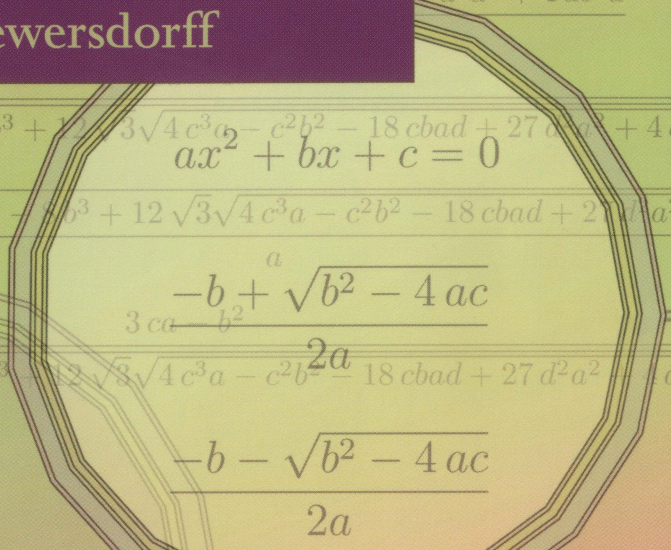
STUDENT MATHEMATICAL LIBRARY
Volume 35

Galois Theory for Beginners

A Historical Perspective

Jörg Bewersdorff



$a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$

AMS
American Mathematical Society

http://dx.doi.org/10.1090/stml/035

Galois Theory for Beginners

A Historical Perspective

This page intentionally left blank

STUDENT MATHEMATICAL LIBRARY
Volume 35

Galois Theory for Beginners

A Historical Perspective

Jörg Bewersdorff

Translated by David Kramer

American Mathematical Society
Providence, Rhode Island

Originally published in the German language by
Friedr. Vieweg & Sohn Verlag, 65189 Wiesbaden, Germany,
as "Jörg Bewersdorff: Algebra für Einsteiger. 2. Auflage (2^{nd} edition)".

Translated by David Kramer with additions and corrections
by the author.

2000 *Mathematics Subject Classification.* Primary 12–01;
Secondary 12F10.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-35

Library of Congress Cataloging-in-Publication Data

Bewersdorff, Jörg.
[Algebra für Einsteiger. English]
Galois theory for beginners : a historical perspective / Jörg Bewersdorff ; translated by David Kramer.
p. cm. — (Student mathematical library, ISSN 1520-9121 ; v. 35)
Includes index.
ISBN-13: 978-0-8218-3817-4 (acid-free paper)
1. Galois theory. 2. Polynomials. I. Title.

QA214.B49 2006
512′.32—dc22 2006048423

---

10 9 8 7 6 5 4 3 2 15 14 13 12 11 10

Contents

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 (1501–1576) 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

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

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 is 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.

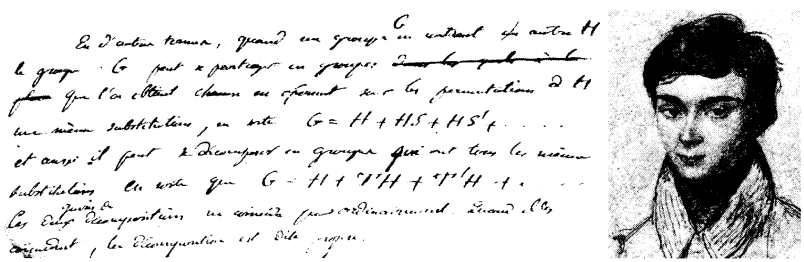


Figure 0.2. Évariste Galois and a fragment from his last letter. In this passage he describes how a group G can be decomposed with the help of the subgroup H. See Section 10.4.

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

This page intentionally left blank

Epilogue

In the end was the beginning. Both historically and in relation to the thematic framework of this introduction, the end result creates a new beginning: Although the problem of solving polynomial equations in radicals posed by Cardano and Ferrari was able to be answered, the objects involved in the solution, groups and fields, raise many new questions about their general properties, and not only in the sense of "art for art's sake." The knowledge that these objects, and the associated applications and techniques, are applicable in many fields of inquiry has allowed algebra, that is, the subfield of mathematics that deals with basic arithmetic operations, to establish itself as a major mathematical discipline. In the field of abstract algebra, the objects of consideration are defined and "classified" in the broadest possible generality and categorized according to their basic structure. To do this with maximum efficiency, general classifications are refined as needed, for example, groups and fields with their subcategories abelian groups and finite fields; and such classifications are also generalized, for example, with the definition of a commutative ring, which satisfies all the requirements of a field except for the invertibility of multiplication.[1]

[1] The best-known examples of rings that are not fields are the integers, the set of polynomials in one or several variables, and the set of residue classes $\mathbb{Z}/n\mathbb{Z}$ for n not a prime.

There are several advantages to developing mathematical objects by such an axiomatic method:

- Mathematics becomes more transparent. In particular, one can recognize fundamental properties in a collection of various mathematical objects that exhibit a number of properties in common.
- Mathematics becomes liberated from fundamental "truths" taken for granted once it has been freed from particular interpretations and applications. Thus, for example, it was with the generalization of the parallel postulate to non-Euclidean geometries that it became possible to establish the unprovability of the parallel axiom, a problem that had been festering since antiquity.
- Such an approach is more economical, at least with respect to mathematics as a whole, since important facts do not have to be proved over and over in different situations. Moreover, these general principles, which in fact are of central interest in mathematics, can often be derived as special cases from more generally valid theorems.

Although such an axiomatically constituted mathematics diverges from the descriptive natural sciences in being only indirectly connected with our physical perception of the world, one should note that classification plays an important role in those sciences as well, from the Linnaean taxonomic system of biological classification to the periodic table of the elements to the classification of symmetries of fundamental particles.

If this book employed such a structural approach only in the last chapter, and perhaps half-heartedly but pragmatically in the chapter before that, the reason was to minimize the difficulties for the interested nonmathematician. The multiplicity of definitions and concepts that seem opaque on first contact presents an almost insuperable barrier to the nonmathematician. Perhaps some readers of the last chapter will have received such an impression, despite the contrary intention of the author.

To avoid unnecessary complications, some things were deliberately excluded, some of which are related to polynomials. We tacitly accepted, without a formal definition, a polynomial as a formal sum

of products of one or more variables $X, Y, \ldots$, and coefficients taking values in some fixed set. Generally, this set was a particular field, but one could also have taken the ring of integers or indeed the set of all polynomials in additional variables.

Such formal polynomials are to be distinguished from the functions that such polynomials define when the variables are replaced by concrete values $a, b, \ldots$ from some set of numbers. Now one can calculate both with polynomials themselves, taking their sums and products, and with their functional values. It is clear that the two forms of calculation are compatible, for example that one has $(f \cdot g)(a) = f(a) \cdot g(a)$. However, one should prove that this is the case.

The simplification of our presentation also serves the purpose of specializing the discussion to subfields of the complex numbers. It was clear, on account of the fundamental theorem of algebra, that a splitting field exists for every polynomial with complex coefficients. Despite the practicality of such an approach, and despite the importance of the fundamental theorem of algebra, the form of argumentation has little to do with algebra. It is not only that the fundamental theorem is proved using mathematical analysis (calculus), an argument involving estimates of distance and intermediate values, which renders the theorem's appellation a historical artifact. It is also that a generalization to other cases, for example that of finite fields, cannot be carried out by such methods.

For these reasons it is understandable that in algebra a completely different tack is generally taken for constructing the splitting fields that are crucial to Galois theory. Beginning with a field K and a polynomial irreducible over K, a field extension containing the elements that solve the corresponding equation

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = 0$$

is constructed in a completely formal way. One does this by the adjunction of a formal value α, where in calculating with expressions of the form

$$k_0 + k_1\alpha + k_2\alpha^2 + \cdots + k_m\alpha^m,$$

with $k_0, \ldots, k_m \in K$, we employ the simplification

$$\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - -a_1\alpha - \alpha_0,$$

so that it always can be achieved that $m \leq n-1$. One can then show that the set

$$K[\alpha] = \left\{ k_0 + k_1\alpha + k_2\alpha^2 + \cdots + k_{n-1}\alpha^{n-1} \mid k_j \in K \right\}$$

forms a field that clearly contains a solution, namely α, of the given equation.[2] What is tricky here is the proof that the set $K[\alpha]$ is closed under division.[3]

If the polynomial is then factored over the field $K[\alpha]$ into irreducible factors, one can proceed with additional adjunction steps. In this way, one finally obtains a completely algebraically constructed splitting field.[4] It is uniquely determined, as can be shown, in that every other splitting field is isomorphic to this one, that is, that the elements are related by a one-to-one correspondence that is compatible with the basic arithmetic operations.[5]

With the formulation thus described, the general equation can now be made amenable to treatment by Galois theory in terms of purely algebraic methods. We have seen the general equation in Chapter 5 as the equation in which formal variables $x_1, \ldots, x_n$ in

[2] From a formal point of view, this approach is similar to that of a quotient group from a normal subgroup. It is an example of a ring of residue classes, which can be constructed from a ring and a subset of a ring called an *ideal*. It is such methods of constructing new objects that requires the axiomatic definition of such objects as groups and fields, not just as subgroups of the symmetric group, as we were always able to do in the case of finite groups, and subfields of the complex numbers.

[3] Essentially, the arguments from Section 10.9 can be easily extended. That is, one investigates the linear system of equations that corresponds to multiplication by the inverse of an element of $K[\alpha]$. However, it is also necessary for the considerations of Section 10.9 to prove that the product of two nonzero elements is again nonzero.

[4] This purely algebraic construction can in fact be used to prove the fundamental theorem of algebra using complete induction. (The induction is over the highest power of 2 that divides the degree of the equation.) Analytic arguments enter the picture only in the form of that fact, provable by the intermediate value theorem, that every odd-degree polynomial with real coefficients has a real zero. See Jean-Pierre Tignol, *Galois' theory of Algebraic Equations*, Singapore, 2001, pp. 119, 121–122, and Exercise 5 at the end of this chapter.

[5] A field automorphism is simply an isomorphism of a field with itself.

the associated elementary symmetric polynomials

$$\begin{aligned} s_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n, \\ s_2(x_1, \ldots, x_n) &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ &\cdots \\ s_n(x_1, \ldots, x_n) &= x_1x_2 \cdots x_n, \end{aligned}$$

are to be determined.

In the language of field extensions, this corresponds to the situation in which beginning with a field K of polynomial coefficients, one is to investigate the extension of the field $K(s_1, \ldots, s_n)$ to the field $K(x_1, \ldots, x_n)$. Due to the uniqueness theorem for symmetric polynomials (see the section on this topic in Chapter 5), one may treat the elementary symmetric polynomials in $K(s_1, \ldots, s_n)$ as though they were formal variables with no formal polynomial relations among them (one speaks of *algebraically independent* quantities). One thereby obtains an additional, fully equivalent, interpretation of the general equation, in which now the equation's coefficients $a_0, a_1, \ldots, a_{n-1}$ are variables for which, as described, a splitting field can be constructed. Since the solutions have no relations among themselves—in the first place by definition and in the second place by the equivalence[6]—the Galois group of the general equation is the full symmetric group.

Theorem E.1. *The Galois group of the general nth-degree equation is the symmetric group S_n; that is, it contains all permutations of the n solutions $x_1, \ldots, x_n$.*

As a consequence, the results for the general equation, as first discovered by Lagrange, appear as a special case of Galois theory. Here

[6]Of course, a direct proof is also possible: Beginning with a given polynomial $h(X_1, \ldots, X_n)$ with $h(x_1, \ldots, x_n) = 0$, one forms the product

$$g(X_1, \ldots, X_n) = \prod_{\sigma \in S_n} h\left(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right).$$

Since the polynomial g is symmetric in the variables $X_1, \ldots, X_n$, it can be expressed as a polynomial in the elementary symmetric polynomials in these variables. There is thus a polynomial $u(Y_1, \ldots, Y_n)$ such that the polynomial $g(X_1, \ldots, X_n)$ can be expressed in the form $g(X_1, \ldots, X_n) = u\left(s_1(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n)\right)$. If one substitutes the solutions $x_1, \ldots, x_n$ into this identity, then one obtains $0 = g(x_1, \ldots, x_n) = u(a_{n-1}, \ldots, a_0)$. This shows immediately that $u = 0$. The previous polynomial identities finally show that $g = 0$ and $h = 0$.

every intermediate field is generated by polynomials in the variables $x_1, \ldots, x_n$ that remain unchanged under the automorphisms of the associated group of permutations. Furthermore, it naturally follows that the solvability of the general equation of a particular degree n is equivalent to the solvability of the symmetric group S_n. Abel's impossibility theorem thus corresponds to the following group-theoretic theorem.

Theorem E.2. *The symmetric group S_n is not solvable for $n \geq 5$.*

In textbooks, this proof of a group-theoretic theorem usually is used to derive Abel's theorem. A proof is possible with arguments similar to those used by Ruffini (see the section on this topic at the end of Chapter 5). To this end, one first proves the following theorem.

Theorem E.3. *If G is a subgroup of the symmetric group S_n for $n \geq 5$ containing all three-cycles, that is, all cyclic permutations of the form $a \to b \to c \to a$ of three distinct elements a, b, c, and if N is a normal subgroup of G with commutative quotient group G/N, then this normal subgroup also contains all the three-cycles.*

To prove this preparatory theorem one represents an arbitrary three-cycle $a \to b \to c \to a$ as the product

$$(d \to b \to a \to d)^{-1} \circ (a \to e \to c \to a)^{-1} \\ \circ (d \to b \to a \to d) \circ (a \to e \to c \to a),$$

where d and e are arbitrary distinct elements that are also distinct from a, b, c. Since the quotient group is commutative, the product must lie in the coset that represents the identity, that is, in N. As asserted, then, every three-cycle belongs to the normal subgroup N.

On the basis of the theorem just proved, it can now be deduced step by step that every group in an ascending chain corresponding to a solution of the symmetric group S_n must contain all three-cycles. The chain can therefore not end in the trivial group containing a single element, and so the symmetric group cannot be solvable.

Moreover, the same argument can be applied to the alternating group A_n, defined as the group of all even permutations. With reference to the alternating group A_n, we note that it is a normal subgroup

of the symmetric group S_n, since the quotient group is a commutative two-element group. In the case of the general equation, the alternating group corresponds to the intermediate field that arises through adjunction of the square root of the discriminant.

To the extent that the base field K for the general equation is a subfield of the complex numbers, the implicitly assumed possibility of extending Galois theory and its applications to radical extensions is unproblematic. In an extension of Galois theory to arbitrary fields, however, two additional complicating factors need to be considered:

- The generalization works only if every irreducible polynomial possesses distinct zeros. Otherwise, not every automorphism of the splitting field is associated uniquely with a permutation of the zeros, and moreover, the construction of Galois resolvents can be problematic. Nevertheless, fields of characteristic zero and finite fields cause no problems in this respect.
- The characterization of radical extensions in terms of Lagrange resolvents assumes that one can divide by the degree of the field extension (see the end of the proof in Section 10.14). In fields with finite characteristic this is not necessarily possible.[7]

Another hole in the preceding chapter relates to finite fields, which we have used only indirectly, other than giving some examples in Chapter 10, namely, in the form of fields of residue classes modulo a prime. In particular, we made use of the existence of a primitive root modulo n, so that the cyclotomic equation could be solved using suitable sums of roots of unity, that is, the periods. Thus for prime numbers n we assumed the existence of an integer g such that the numbers $g^1, g^2, \ldots, g^{n-1}$ represent distinct nonzero residue classes $1, 2, \ldots, n-1$.

Using algebraic structures, this fact can be formulated in slightly greater generality.

Theorem E.4. *Every finite subgroup of the multiplicative group of a field is cyclic.*

[7] Indeed, the general quadratic equation over the two-element field $\mathbb{Z}/2\mathbb{Z}$, for example, is not solvable in radicals. See B. L. van der Waerden, *Algebra I*, Section 62.

The application of interest here, relating to subgroups of a finite field $\mathbb{Z}/p\mathbb{Z}$, was first proved, in a formulation as a statement about residue classes, by Legendre (1752–1833). Earlier proofs by Euler must be considered incomplete. Although a proof can be given based on extensive computations in residue classes,[8] we would like to offer a proof of the generalized theorem, which is shorter and more easily understood.

We begin with an investigation of Euler's phi function, which associates with a natural number d the number of integers in the set $\{1, 2, \ldots, d\}$ relatively prime to d. For example, $\varphi(6) = 2$, since 1 and 5 are the only integers between 1 and 6 relatively prime to 6; and $\varphi(8) = 4$, with $1, 3, 5, 7$ relatively prime to 8. Euler's phi function satisfies the relation

$$\sum_{d|n} \varphi(d) = n.$$

We will first justify this formula, where the sum is over all divisors d of n. To this end, consider for each residue class j modulo n, represented for example by the n integers $0, 1, \ldots, n-1$, its order d as an element of the group $\mathbb{Z}/n\mathbb{Z}$. Each such order d must be a divisor of n, and the residue class j will have order d precisely when it is represented by an integer $m \cdot \frac{n}{d}$, so that j must lie in the subgroup generated by the residue class associated with $\frac{n}{d}$. This subgroup is cyclic of order d, and thus isomorphic to $\mathbb{Z}/d\mathbb{Z}$, and therefore contains precisely $\varphi(d)$ elements of order d. The partition of the n-element group $\mathbb{Z}/n\mathbb{Z}$ thus obtained corresponds precisely to the summation formula.

After these preparations we can address the actual content of the theorem, namely, a finite subgroup U of the multiplicative group of a field. If d is a natural number such that there is an element x in U for which the group generated by x is the group $\{1, x, x^2, \ldots, x^{d-1}\}$ of d elements, then according to Section 10.4, d is a divisor of $|U|$, the number of elements in U. Since $x^d = 1$, every element of this group is a zero of the polynomial $X^d - 1$. Since we know from Section 4.2 that for each zero of a polynomial we may split off a linear factor, and thus this polynomial can have at most d zeros, there cannot exist an element of U outside of the subgroup $\{1, x, x^2, \ldots, x^{d-1}\}$ that

[8] See, for example, Jay R. Goldman, *The Queen of Mathematics*, Wellesley, 1998, Chapter 10.

generates a d-element subgroup. Therefore, in the group U there is either no element that generates a d-element subgroup or there are $\varphi(d)$ of them. If one again decomposes the group U as we earlier decomposed the group $\mathbb{Z}/n\mathbb{Z}$ according to the size of the subgroup that each element generates, then for $n = |U|$ we obtain the summation formula

$$n = \sum_{d|n} \varphi(d) \cdot \delta_d,$$

where each of the numbers δ_d is either 0 or 1. One then sees immediately a similarity to the previously derived summation formula, that for divisors d of n we must always have $\delta_d = 1$. In particular, there are $\varphi(n)$ elements of U that generate an n-element subgroup, that is, the entire group U. The group U is therefore cyclic.

Exercises

(1) Prove *Fermat's little theorem*: For a prime number n and a positive integer a relatively prime to n, the number $a^{n-1} - 1$ is divisible by n.

(2) Prove *Wilson's theorem*: For a prime number n, the number $(n-1)! + 1$ is divisible by n. Then conclude from this that a natural number $n \geq 2$ is prime if and only if $(n-1)! + 1$ is divisible by n.

(3) Prove the generalization of Fermat's little theorem that for a natural number n and a natural number a relatively prime to n, the number $a^{\varphi(n)} - 1$ is divisible by n. Hint: First show that the residue classes in $\mathbb{Z}/n\mathbb{Z}$ represented by integers relatively prime to n form a group under multiplication.

(4) Prove that if $n = pq$ is a product of two distinct prime numbers p and q and if u and v are two natural numbers such that $uv - 1$ is divisible by $(p-1)(q-1)$, then for every natural number a, the number $a^{uv} - a$ is divisible by n.[9] In such a case, the pairs (u, n) and (v, n) can serve as cryptographic keys, where one is

[9] The significance of this exercise is that the two residue class mappings $x \mapsto x^u$ and $x \mapsto x^v$ of $\mathbb{Z}/n\mathbb{Z}$ into itself are inverses of each other. Such a construction is used in cryptography, in the *RSA encryption procedure*. Here very large primes, that is, of several hundred digits each, are used, so that determining two such prime numbers p, q given their product $n = pq$ would be impossible even after millions of years of computation on today's fastest computers.

used for encryption, the other for decryption. One speaks of an *asymmetric cryptographic algorithm.* In contrast to symmetric algorithms, in which encryption and decryption use a single key, with the RSA algorithm one of the keys, that for encoding, say, can be published without fear that unauthorized persons will be able to decode encrypted messages. One therefore refers to the RSA algorithm as *public key encryption.* Hint: The assertion can be reduced to that of Exercise 3. To include the case in which a is divisible by p or q, one might demonstrate the divisibility of $a^{uv} - a$ by p and by q separately.

(5) Prove the fundamental theorem of algebra in an algebraic way by proving that for a nonconstant polynomial $f(X)$ with complex coefficients, if one factors $f(x)$ into linear factors as

$$f(X) = (X - x_1) \cdots (X - x_n)$$

in some algebraic extension field of $\mathbb{C}$ (which is always possible via an algebraic construction), one in fact has that $x_1, \ldots, x_n \in \mathbb{C}$. First show the following:

- The theorem holds for quadratic polynomials $f(X)$ (see also Exercise 1 in Chapter 2).
- It suffices to prove the existence of a single complex solution x_j. Moreover, one can restrict attention to polynomials with real coefficients.

Now the proof can be carried out using mathematical induction on the highest power of 2 that divides the degree of the polynomial. For the base step of the induction, one uses the version of the theorem for real polynomials of odd degree, which is proved using mathematical analysis (calculus). For the induction step, one investigates polynomials of the form

$$g_c(X) = \prod_{i<j} \left(X - (x_i + x_j + c x_i x_j)\right)$$

for a suitably chosen parameter c.

(6) For a prime number m and a natural number a relatively prime to m, the *Legendre symbol* is defined as follows:

$$\left(\frac{a}{m}\right) = \begin{cases} +1 & \text{if } a = s^2 + km \text{ for suitable integers } s \text{ and } k, \\ -1 & \text{if } a \text{ does not have such representation.} \end{cases}$$

The Legendre symbol therefore tells whether the residue class represented by a is a square in the multiplicative group of residue classes $\mathbb{Z}/m\mathbb{Z} - \{0\}$. Even though the value of the Legendre symbol can be determined by finite trial and error, one is naturally interested in a direct calculation. Therefore, show first that

$$a^{(m-1)/2} - \left(\frac{a}{m}\right)$$

is divisible by m.

Other properties of the Legendre symbol can be obtained with the use of roots of unity. For a second prime number $n \geq 3$ we again let ζ denote the nth root of unity $\zeta = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$, while the periods of length $(n-1)/2$ (see Section 7.2) are denoted by $\eta_0 = P_{(n-1)/2}(\zeta)$ and $\eta_1 = P_{(n-1)/2}(\zeta^g)$, where the integer g again represents a primitive root modulo n. Show that

$$(\eta_0 - \eta_1)^m - \left(\frac{m}{n}\right)(\eta_0 - \eta_1) = m\left(a_0 + a_1\zeta + \cdots + a_{n-2}\zeta^{n-2}\right)$$

with integers $a_0, a_1, \ldots, a_{n-2}$. Show also (if you have not already done so in Exercise 2 of Chapter 7) that

$$(\eta_0 - \eta_1)^2 = (-1)^{(n-1)/2} n.$$

Finally, show how the resulting identity

$$\left[(-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right) - \left(\frac{m}{n}\right)\right](\eta_0 - \eta_1)^2 = m\left(b_0 + b_1\zeta + \cdots + b_{n-2}\zeta^{n-2}\right),$$

with integers $b_0, b_1, \ldots, b_{n-2}$, yields the *law of quadratic reciprocity*[10]

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right).$$

(7) For a group G whose number of elements $|G|$ is divisible by a prime number p, one defines the mapping

$$\varphi(g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$$

[10]The law of quadratic reciprocity was first proved by Carl Friedrich Gauss on April 8, 1796, as documented by an entry in his diary. It is a fundamental result of number theory with many ramifications. Furthermore, using the law of quadratic reciprocity together with some other elementary properties of integers, one can compute the values of arbitrary Legendre symbols rather quickly.

for $g_1, g_2, \ldots, g_p \in G$, as well as the set

$$X = \{ (g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = \epsilon \},$$

where ϵ again denotes the group identity.

Prove the following:

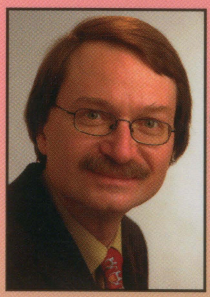
- $|X| = |G|^{p-1}$.
- The mapping φ maps the set X into itself.
- If the identity $\varphi^k(x) = x$ holds for an element $x \in G^p$ and an integer k not divisible by p, then all the coordinates of x are equal.
- Every *orbit* $\{ x, \varphi(x), \varphi^2(x), \ldots \}$, where $x \in G^p$, consists of either one element or p elements.
- The number of one-element orbits in X is divisible by p.

Assuming that there exists an element $x \in X$ with a one-element orbit, conclude that there exists at least one other element with a one-element orbit, and thereby prove the existence of an element of G of order p (Cauchy's theorem).[11]

[11] Cauchy's theorem is usually formulated in a more general form, which is named after Ludwig Sylow (1832–1918). The Sylow theorems make assertions about subgroups of a group of order the power of a prime.

Index

Galois theory is the culmination of a centuries-long search for a solution to the classical problem of solving algebraic equations by radicals. In this book, Bewersdorff follows the historical development of the theory, emphasizing concrete examples along the way. As a result, many mathematical abstractions are now seen as the natural consequence of particular investigations.



Few prerequisites are needed beyond general college mathematics, since the necessary ideas and properties of groups and fields are provided as needed. Results in Galois theory are formulated first in a concrete, elementary way, then in the modern form. Each chapter begins with a simple question that gives the reader an idea of the nature and difficulty of what lies ahead. The applications of the theory to geometric constructions, including the ancient problems of squaring the circle, duplicating the cube, and trisecting an angle, and the construction of regular n-gons are also presented.

This book is suitable for undergraduates and beginning graduate students.

ISBN 978-0-8218-3817-4

9 780821 838174

STML/35