Jean-Pierre Tignol

Galois' Theory of Algebraic Equations

Second Edition

World Scientific

Galois' Theory of Algebraic Equations

Second Edition

Jean-Pierre Tignol

Université Catholique de Louvain, Belgium

World Scientific

NEW JERSEY · LONDON · SINGAPORE · BEIJING · SHANGHAI · HONG KONG · TAIPEI · CHENNAI · TOKYO

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

Library of Congress Cataloging-in-Publication Data

Names: Tignol, Jean-Pierre, author.

Title: Galois' theory of algebraic equations / by Jean-Pierre Tignol
(Université Catholique de Louvain, Belgium).

Other titles: Leçons sur la théorie des équations. English | Lectures on the theory of equations

Description: 2nd World Scientific edition. | New Jersey : World Scientific, 2016. |
Originally published in English in 1988 jointly by: Harlow, Essex, England :
Longman Scientific & Technical; and, New York : Wiley. |
Includes bibliographical references and index.

Identifiers: LCCN 2015038537 | ISBN 9789814704694 (hardcover : alk. paper)

Subjects: LCSH: Equations, Theory of. | Galois theory.

Classification: LCC QA211 .T5413 2016 | DDC 512/.32--dc23

LC record available at http://lccn.loc.gov/2015038537

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

Printed in Singapore by B & Jo Enterprise Pte Ltd

Galois' Theory
of Algebraic Equations

Second Edition

à Paul

For inquire, I pray thee, of the former age,
and prepare thyself to the search of their fathers:
For we are but of yesterday, and know nothing,
because our days upon earth are a shadow.

Job 8, 8–9.

Preface to the Second Edition

After the first edition of this book was published, the bicentennial of Galois' birth (in 2011) occasioned a renewal of interest in his highly atypical oeuvre. Scholarship on the theory of equations and Galois theory has been significantly expanded, notably by Stedall's and Ehrhardt's monographs [68] and [27], and through the publication of a new edition of Galois' mathematical writings by Neumann [55]. While these circumstances influenced my decision to prepare a second edition of this book, the crucial factor in this regard stems from an uncanny experience that I had while working on a completely different project: as Max Knus and I were studying constructions on étale algebras inspired by the representation theory of linear algebraic groups, it dawned on me that some of the constructions were *exact analogues* of those that Galois had used to attach groups to equations. Revisiting Galois' memoir with this analogy in mind, I was awed by the efficiency of this perspective in elucidating Galois' statements and enabling the presentation of full proofs of his propositions.

In this new edition, the chapter on Galois has been completely rewritten to take advantage of this viewpoint. The exposition is now much closer to his memoir, and remarkably elementary.[1] It is also mostly free of anachronisms, although I did not refrain from using a few modern notions when I felt they could illuminate Galois' words without overextending his vision. Thus, for the reader in search of a precise idea of what Galois wrote, my account is no substitute for the original,[2] but I hope it will foster a better

[1] Keep in mind that "elementary" is not the same as "easy"; in this case (as often), it is in fact the opposite: Galois' elementary arguments are remarkably ingenious and sometimes quite intricate.

[2] Galois' memoir is now readily available on the web site of the *Bibliothèque nationale de France*, `http://gallica.bnf.fr/` or the *Bibliothèque de l'Institut de France*, `http://www.bibliotheque-institutdefrance.fr/`, or in translation [26] and [55, Ch. IV].

understanding of this difficult text. To the epilogue (Chapter 15), I have added a new appendix to indicate the close relation between Galois' definition of the group of an equation and the modern notion of torsor that inspired my new analysis of his memoir.

Chapters 1–13 are mostly unchanged, except for a few slight revisions in the wording, which I hope are improvements. The more significant alterations occur in the discussion of elimination theory in §5.6, and of radical extensions in §13.1.

This second edition also gives me the opportunity to acknowledge input from several people who gave me feedback on various aspects of the first edition. I am especially grateful to Benjamin Barras, Oscar Luis Palacios-Vélez, and Robert Perlis for lists of typographical errors and valuable comments, which have been taken into account in this new edition. I am also indebted to Karim-Johannes Becher and James O'Shea, who kindly read and commented the revised version of Chapter 14. Their numerous constructive suggestions allowed me to eliminate mistakes and to improve the exposition in several places.

Preface to the First Edition (2001)

In spite of the title, the main subject of these lectures is not algebra, even less history, as one could conclude from a glance over the table of contents, but methodology. Their aim is to convey to the audience, which originally consisted of undergraduate students in mathematics, an idea of how mathematics is made. For such an ambitious project, the individual experience of any but the greatest mathematicians seems of little value, so I thought it appropriate to rely instead on the collective experience of generations of mathematicians, on the premise that there is a close analogy between collective and individual experience: the problems over which past mathematicians have stumbled are most likely to cause confusion to modern learners, and the methods which have been tried in the past are those which should come to mind naturally to the (gifted) students of today. The way in which mathematics is made is best learned from the way mathematics has been made, and that premise accounts for the historical perspective on which this work is based.

The theme used as an illustration for general methodology is the theory of equations. The main stages of its evolution, from its origins in ancient times to its completion by Galois around 1830 will be reviewed and discussed. For the purpose of these lectures, the theory of equations seemed like an ideal topic in several respects: first, it is completely elementary, requiring virtually no mathematical background for the statement of its problems, and yet it leads to profound ideas and to fundamental concepts of modern algebra. Secondly, it underwent a very long and eventful evolution, and several gems lie along the road, like Lagrange's 1770 paper, which brought order and method to the theory in a masterly way, and Vandermonde's visionary glimpse of the solution of certain equations of high degree, which hardly unveiled the principles of Galois theory sixty years be-

fore Galois' memoir. Also instructive from a methodological point of view is the relationship between the general theory, as developed by Cardano, Tschirnhaus, Lagrange and Abel, and the attempts by Viète, de Moivre, Vandermonde and Gauss at significant examples, namely the so-called cyclotomic equations, which arise from the division of the circle into equal parts. Works in these two directions are closely intertwined like themes in a counterpoint, until their resolution in Galois' memoir. Finally, the algebraic theory of equations is now a closed subject, which reached complete maturity a long time ago; it is therefore possible to give a fair assessment of its various aspects. This is of course not true of Galois theory, which still provides inspiration for original research in numerous directions, but these lectures are concerned with the theory of equations and not with the Galois theory of fields. The evolution from Galois' theory to modern Galois theory falls beyond the scope of this work; it would certainly fill another book like this one.

As a consequence of emphasis on historical evolution, the exposition of mathematical facts in these lectures is genetic rather than systematic, which means that it aims to retrace the concatenation of ideas by following (roughly) their chronological order of occurrence. Therefore, results which are logically close to each other may be scattered in different chapters, and some topics are discussed several times, by little touches, instead of being given a unique definitive account. The expected reward for these circumlocutions is that the reader could hopefully gain a better insight into the inner workings of the theory, which prompted it to evolve the way it did.

Of course, in order to avoid discussions that are too circuitous, the works of mathematicians of the past—especially the distant past—have been somewhat modernized as regards notation and terminology. Although considering sets of numbers and properties of such sets was clearly alien to the patterns of thinking until the nineteenth century, it would be futile to ignore the fact that (naive) set theory has now pervaded all levels of mathematical education. Therefore, free use will be made of the definitions of some basic algebraic structures such as field and group, at the expense of lessening some of the most original discoveries of Gauss, Abel and Galois. Except for those definitions and some elementary facts of linear algebra which are needed to clarify some proofs, the exposition is completely self-contained, as can be expected from a genetic treatment of an elementary topic.

It is fortunate to those who want to study the theory of equations that

its long evolution is well documented: original works by Cardano, Viète, Descartes, Newton, Lagrange, Waring, Gauss, Ruffini, Abel, Galois are readily available through modern publications, some even in English translations. Besides these original works and those of Girard, Cotes, Tschirnhaus and Vandermonde, I relied on several sources, mainly on Bourbaki's Note historique [7] for the general outline, on van der Waerden's "Science Awakening" [79] for the ancient times and on Edwards' "Galois theory" [26] for the proofs of some propositions in Galois' memoir. For systematic expositions of Galois theory, with applications to the solution of algebraic equations by radicals, the reader can be referred to any of the fine existing accounts, such as Artin's classical booklet [2], Kaplansky's monograph [42], the books by Morandi [54], Rotman [63] or Stewart [70], or the relevant chapters of algebra textbooks by Cohn [17], Jacobson [40], [41] or van der Waerden [77], and presumably to many others I am not aware of. In the present lectures, however, the reader will find a thorough treatment of cyclotomic equations after Gauss, of Abel's theorem on the impossibility of solving the general equation of degree 5 by radicals, and of the conditions for solvability of algebraic equations after Galois, with complete proofs. The point of view differs from the one in the quoted references in that it is strictly utilitarian, focusing (albeit to a lesser extent than the original papers) on the concrete problem at hand, which is to solve equations. Incidentally, it is striking to observe, in comparison, what kind of acrobatic tricks are needed to apply modern Galois theory to the solution of algebraic equations.

The exercises at the end of some chapters point to some extensions of the theory and occasionally provide the proof of some technical fact which is alluded to in the text. They are never indispensable for a good understanding of the text. Solutions to selected exercises are given at the end of the book.

This monograph is based on a course taught at the Université catholique de Louvain from 1978 to 1989, and was first published by Longman Scientific & Technical in 1988. It is a much expanded and completely revised version of my "Leçons sur la théorie des équations" published in 1980 by the (now vanished) Cabay editions in Louvain-la-Neuve. The wording of the Longman edition has been recast in a few places, but no major alteration has been made to the text.

I am greatly indebted to Francis Borceux, who invited me to give my first lectures in 1978, to the many students who endured them over the years, and to the readers who shared with me their views on the 1988 edition.

Their valuable criticism and encouraging comments were all-important in my decision to prepare this new edition for publication. Through the various versions of this text, I was privileged to receive help from quite a few friends, in particular from Pasquale Mammone and Nicole Vast, who read parts of the manuscript, and from Murray Schacher and David Saltman, for advice on (American-) English usage. Hearty thanks to all of them. I owe special thanks also to T.S. Blyth, who edited the manuscript of the Longman edition, to the staffs of the Centre général de Documentation (Université catholique de Louvain) and of the Bibliothèque Royale Albert 1er (Brussels) for their helpfulness and for allowing me to reproduce parts of their books, and to Nicolas Rouche, who gave me access to the riches of his private library.

On the TEXnical side, I am grateful to Suzanne D'Addato (who also typed the 1988 edition) and to Béatrice Van den Haute, and also to Camille Debiève for his help in drawing the figures.

Finally, my warmest thanks to Céline, Paul, Ève and Jean for their infectious joy of living and to Astrid for her patience and constant encouragement. The preparation of the 1988 edition for publication spanned the whole life of our little Paul. I wish to dedicate this book to his memory.

Contents

Chapter 1

Quadratic Equations

Since the solution of a linear equation $ax = b$ does not use anything more than a division, it hardly belongs to the algebraic theory of equations; it is therefore appropriate to begin our discussion with quadratic equations

$$ax^2 + bx + c = 0 \qquad (a \neq 0).$$

Dividing each side by a, we reduce to the case where the coefficient of x^2 is 1:

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

The solution of this equation is well-known: when $\left(\frac{p}{2}\right)^2$ is added to each side, the square of $x + \frac{p}{2}$ appears and the equation can be written

$$\left(x + \frac{p}{2}\right)^2 + q = \left(\frac{p}{2}\right)^2.$$

(This procedure is called "completion of the square.") The values of x easily follow:

$$x = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}.$$

This formula is so well-known that it may be rather surprising to note that the solution of quadratic equations could not have been written in this form before the seventeenth century.[1] Nevertheless, mathematicians had been solving quadratic equations for about 40 centuries before. The purpose of this first chapter is to give a brief outline of this "prehistory" of the theory of quadratic equations.

[1]The first uniform solution for quadratic equations (regardless of the signs of coefficients) is due to Simon Stevin in "L'Arithmetique" [69, p. 595], published in 1585. However, Stevin does not use literal coefficients, which were introduced some years later by François Viète: see Chapter 4, §4.1.