Universitext

Joseph Rotman

Galois Theory

Second Edition

伽罗瓦理论 第2版

Springer

世界图书出版公司
www.wpcbj.com.cn

Universitext

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Universitext

Editors (North America): S. Axler, F.W. Gehring, and K.A. Ribet

Aksoy/Khamsi: Nonstandard Methods in Fixed Point Theory
Andersson: Topics in Complex Analysis
Aupetit: A Primer on Spectral Theory
Bachman/Narici/Beckenstein: Fourier and Wavelet Analysis
Bădescu: Algebraic Surfaces
Balakrishnan/Ranganathan: A Textbook of Graph Theory
Balser: Formal Power Series and Linear Systems of Meromorphic Ordinary Differential Equations
Bapat: Linear Algebra and Linear Models (2nd ed.)
Berberian: Fundamentals of Real Analysis
Boltyanskiĭ/Efremovich: Intuitive Combinatorial Topology. (Shenitzer, trans.)
Booss/Bleecker: Topology and Analysis
Borkar: Probability Theory: An Advanced Course
Böttcher/Silbermann: Introduction to Large Truncated Toeplitz Matrices
Carleson/Gamelin: Complex Dynamics
Cecil: Lie Sphere Geometry: With Applications to Submanifolds
Chae: Lebesgue Integration (2nd ed.)
Charlap: Bieberbach Groups and Flat Manifolds
Chern: Complex Manifolds Without Potential Theory
Cohn: A Classical Invitation to Algebraic Numbers and Class Fields
Curtis: Abstract Linear Algebra
Curtis: Matrix Groups
Debarre: Higher-Dimensional Algebraic Geometry
DiBenedetto: Degenerate Parabolic Equations
Dimca: Singularities and Topology of Hypersurfaces
Edwards: A Formal Background to Mathematics I a/b
Edwards: A Formal Background to Mathematics II a/b
Farenick: Algebras of Linear Transformations
Foulds: Graph Theory Applications
Friedman: Algebraic Surfaces and Holomorphic Vector Bundles
Fuhrmann: A Polynomial Approach to Linear Algebra
Gardiner: A First Course in Group Theory
Gårding/Tambour: Algebra for Computer Science
Goldblatt: Orthogonality and Spacetime Geometry
Gustafson/Rao: Numerical Range: The Field of Values of Linear Operators and Matrices
Hahn: Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups
Heinonen: Lectures on Analysis on Metric Spaces
Holmgren: A First Course in Discrete Dynamical Systems
Howe/Tan: Non-Abelian Harmonic Analysis: Applications of $SL(2, \mathbb{R})$
Howes: Modern Analysis and Topology
Hsieh/Sibuya: Basic Theory of Ordinary Differential Equations
Humi/Miller: Second Course in Ordinary Differential Equations
Hurwitz/Kritikos: Lectures on Number Theory
Jennings: Modern Geometry with Applications
Jones/Morris/Pearson: Abstract Algebra and Famous Impossibilities
Kannan/Krueger: Advanced Analysis

(continued after index)

图书在版编目（CIP）数据

伽罗瓦理论：第2版 = Galois Theory 2nd ed. ：英文/（美）罗特曼（Rotman，J.）著. —影印本. —北京：世界图书出版公司北京公司，2010.2

ISBN 978-7-5100-0508-4

Ⅰ.①伽… Ⅱ.①罗… Ⅲ.①伽罗瓦理论—英文 Ⅳ.①O153.4

中国版本图书馆 CIP 数据核字（2010）第010705号

书　　名：	Galois Theory 2nd ed.
作　　者：	Joseph Rotman
中 译 名：	伽罗瓦理论 第2版
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街137号　100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@wpcbj.com.cn
开　　本：	24开
印　　张：	7.5
版　　次：	2010年01月
版权登记：	图字：01-2009-1084
书　　号：	978-7-5100-0508-4/O·724　　**定　　价：** 25.00元

Joseph Rotman

Galois Theory

Second Edition

Springer

Joseph Rotman
Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801
USA
rotman@math.uiuc.edu

Mathematics Subject Classification (2000): 12-01, 12F10

With 9 Figures.

Library of Congress Cataloging-in-Publication Data
Rotman, Joseph J., 1934-
Galois theory / Joseph Rotman. — 2nd ed.
p. cm. — (Universitext)
Includes bibliographical references (p. –) and index.
ISBN 0-387-98541-7 (softcover : alk. paper)
1. Galois theory. I. Title.
QA214.R685 1998
512'.3—dc21 98-3967

9 8 7 6 5 4 3 2 (Corrected second printing)

ISBN 0-387-98541-7

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

To my teacher
Irving Kaplansky

Preface to the Second Edition

There are too many errors in the first edition, and so a "corrected nth printing" would have been appropriate. However, given the opportunity to make changes, I felt that a second edition would give me the flexibility to change any portion of the text that I felt I could improve. The first edition aimed to give a geodesic path to the Fundamental Theorem of Galois Theory, and I still think its brevity is valuable. Alas, the book is now a bit longer, but I feel that the changes are worthwhile. I began by rewriting almost all the text, trying to make proofs clearer, and often giving more details than before. Since many students find the road to the Fundamental Theorem an intricate one, the book now begins with a short section on symmetry groups of polygons in the plane; an analogy of polygons and their symmetry groups with polynomials and their Galois groups can serve as a guide by helping readers organize the various definitions and constructions. The exposition has been reorganized so that the discussion of solvability by radicals now appears later; this makes the proof of the Abel-Ruffini theorem easier to digest. I have also included several theorems not in the first edition. For example, the *Casus Irreducibilis* is now proved, in keeping with a historical interest lurking in these pages.

I am indebted to Gareth Jones at the University of Southampton who, after having taught a course with the first edition as text, sent me a detailed list of errata along with perspicacious comments and suggestions. I also thank Evan Houston, Adam Lewenberg, and Jack Shamash who made valuable comments as well. This new edition owes much to the generosity of these readers, and I am grateful to them.

Joseph Rotman
Urbana, Illinois, 1998

I thank everyone, especially Abe Seika and Bao Luong, who apprised me of errors in the first printing. I have corrected all mistakes that have been found.

Joseph Rotman
Urbana, Illinois, 2001

Preface to the First Edition

This little book is designed to teach the basic results of Galois theory—fundamental theorem; insolvability of the quintic; characterization of polynomials solvable by radicals; applications; Galois groups of polynomials of low degree—efficiently and lucidly. It is assumed that the reader has had introductory courses in linear algebra (the idea of the dimension of a vector space over an arbitrary field of scalars should be familiar) and "abstract algebra" (that is, a first course which mentions rings, groups, and homomorphisms). In spite of this, a discussion of commutative rings, starting from the definition, begins the text. This account is written in the spirit of a review of things past, and so, even though it is complete, it may be too rapid for one who has not seen any of it before. The high number of exercises accompanying this material permits a quicker exposition of it. When I teach this course, I usually begin with a leisurely account of group theory, also from the definition, which includes some theorems and examples that are not needed for this text. Here I have decided to relegate needed results of group theory to appendices: a glossary of terms; proofs of theorems. I have chosen this organization of the text to emphasize the fact that polynomials and fields are the natural setting, and that groups are called in to help.

A thorough discussion of field theory would have delayed the journey to Galois's Great Theorem. Therefore, some important topics receive only a passing nod (separability, cyclotomic polynomials, norms, infinite extensions, symmetric functions) and some are snubbed altogether (algebraic closure, transcendence degree, resultants, traces, normal bases, Kummer theory). My belief is that these subjects should be pursued only after the reader has digested the basics.

My favorite expositions of Galois theory are those of E. Artin, Kaplansky, and van der Waerden, and I owe much to them. For the appendix on

"old-fashioned Galois theory," I relied on recent accounts, especially [Edwards], [Gaal], [Tignol], and [van der Waerden, 1985], and older books, especially [Dehn] (and [Burnside and Panton], [Dickson], and [Netto]). I thank my colleagues at the University of Illinois, Urbana, who, over the years, have clarified obscurities; I also thank Peter Braunfeld for suggestions that improved Appendix C and Peter M. Neumann for his learned comments on Appendix D.

I hope that this monograph will make both the learning and the teaching of Galois theory enjoyable, and that others will be as taken by its beauty as I am.

Joseph Rotman
Urbana, Illinois, 1990

To the Reader

Regard the exercises as part of the text; read their statements and do attempt to solve them all. A result labeled Theorem 1 is the first theorem in the text; Theorem G1 is the first theorem in the appendix on group theory; Theorem R1 is the first theorem in the appendix on ruler-compass constructions; Theorem H1 is the first theorem in the appendix on history.

Contents

Galois Theory

Galois theory is the interplay between polynomials, fields, and groups. The quadratic formula giving the roots of a quadratic polynomial was essentially known by the Babylonians. By the middle of the sixteenth century, the cubic and quartic formulas were known. Almost three hundred years later, Abel (1824) proved, using ideas of Lagrange and Cauchy, that there is no analogous formula (involving only algebraic operations on the coefficients of the polynomial) giving the roots of a quintic polynomial (actually Ruffini (1799) outlined a proof of the same result, but his proof had gaps and it was not accepted by his contemporaries). In 1829, Abel gave a sufficient condition that a polynomial (of any degree) have such a formula for its roots (this theorem is the reason that, nowadays, commutative groups are called abelian). Shortly thereafter, Galois (1831) invented groups, associated a group to each polynomial, and used properties of this group to give, for any polynomial, a necessary and sufficient condition that there be a formula of the desired kind for its roots, thereby completely settling the problem. We prove these theorems here.

Symmetry

Although Galois invented groups because he needed them to describe the behavior of polynomials, we realize today that groups are the precise way to describe symmetry. The Greek roots of the word *symmetry* mean, roughly, measuring at the same time. In ordinary parlance, there are at least two meanings of the word, both involving an arrangement of parts somehow balanced with respect to the whole and to each other. One of these meanings attributes an aesthetic quality to the arrangement, implying that sym-

metry is harmonious and well-proportioned. This usage is common in many discussions of art, and one sees it in some mathematics books as well (e.g., Weyl's *Symmetry*). Here, however, we focus on arrangements without considering, for example, whether a square is more pleasing to the eye than a rectangle.

Before giving a formal definition of symmetry, we first consider mirror images.

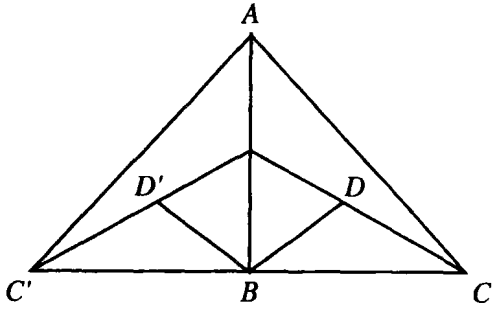

Figure 1

Let F denote the figure pictured in Figure 1. If one regards the line AB as a mirror, then the left half of F is the reflection of the right half. This figure is an example of *bilateral symmetry*: each point P on one side of AB corresponds to a point P' (its mirror image) on the other side of AB; for example, C' corresponds to C and D' corresponds to D. We can describe this symmetry in another way. Regard the plane $\mathbb{R}^2$ as a flat transparent surface in space, having F (without the letters) drawn on it. Imagine turning over this surface by flipping it around the axis AB. If one's eyes were closed before the flip and then reopened after it, one could not know, merely by looking at F in its new position, whether the flip had occurred. Indeed, if F lies in the plane so that AB lies on the y-axis and CC' lies on the x-axis, then the linear transformation $r : \mathbb{R}^2 \to \mathbb{R}^2$, defined by $(x, y) \mapsto (-x, y)$ and called a *reflection*, carries the figure into itself; that is,

$$r(F) = F.$$

On the other hand, if T is some scalene triangle in the plane (say, with its center at the origin), then it is easy to see that there are points P in T whose mirror images $P' = r(P)$ do not lie in T; that is, $r(T) \neq T$.

Another type of symmetry is *rotational symmetry*. Picture an equilateral triangle Δ in the plane with its center at the origin. A (counterclockwise)

rotation ρ by 120° carries Δ into itself; if one's eyes were closed before ρ takes place and then reopened, one could not detect that a motion had occurred.

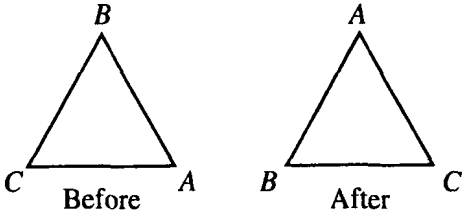

Figure 2

If we identify the plane with the complex numbers $\mathbb{C}$, then the rotation $\rho : \mathbb{C} \to \mathbb{C}$ can be described by $\rho : re^{i\theta} \mapsto re^{i(\theta+2\pi/3)}$, and

$$\rho(\Delta) = \Delta.$$

Definition. A linear transformation $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ is called ***orthogonal*** if it is distance preserving; that is, if $|U - V|$ denotes the distance between points U and V, then

$$|\sigma(U) - \sigma(V)| = |U - V|.$$

There are distance preserving functions that are not linear transformations; for example, a ***translation*** is defined by $(x, y) \mapsto (x + a, y + b)$ for fixed numbers a and b; geometrically, this translation sends any vector (x, y) into $(x, y) + (a, b)$. (It is a theorem that every distance preserving function is a composite of reflections, rotations, and translations and, if it fixes the origin, then it is a composite of reflections and rotations alone.)

It can be shown that every orthogonal transformation σ is a bijection,[1] so that its inverse function σ^{-1} exists; moreover, one can prove that σ^{-1} is also orthogonal. The set $O(2, \mathbb{R})$ of all orthogonal transformations is a group under composition, called the *real orthogonal group*.

[1] A function $f : X \to Y$ is an ***injection*** (one also says that f is *one-to-one*) if distinct points have distinct images; that is, if $x \neq x'$, then $f(x) \neq f(x')$; the contrapositive, $f(x) = f(x')$ implies $x = x'$, is often the more useful statement. A function f is a ***surjection*** (one also says f is *onto*) if, for each $y \in Y$, there exists $x \in X$ with $f(x) = y$. A function f is a ***bijection*** (one also says f is a *one-to-one correspondence*) if it is both an injection and a surjection. Finally, a function $f : X \to Y$ is a bijection if and only if it has an ***inverse***; that is, there is a function $g : Y \to X$ with both composites gf and fg identity functions.

Lemma 1. *Every orthogonal transformation σ preserves angles: if A, V and B are points, then $\angle AVB = \angle A'V'B'$, where $A' = \sigma(A)$, $V' = \sigma(V)$, and $B' = \sigma(B)$.*

Proof. We begin by proving the special case when V is the origin O. First, identify a point X with the vector starting at O and ending at X. Recall the formula relating lengths and dot product: $|X|^2 = (X, X)$, so that

$$|A - B|^2 = (A - B, A - B) = |A|^2 - 2(A, B) + |B|^2.$$

There is a similar equation for A' and B'. Since, by hypothesis, $|A' - B'| = |A - B|$, $|A'| = |A|$, and $|B'| = |B|$, it follows that $(A', B') = (A, B)$. But $(A, B) = |A||B| \cos\theta$, where $\theta = \angle AOB$. Therefore, $\angle AOB = \angle A'OB'$. But $O' = \sigma(O) = O$, because σ is a linear transformation, and so $\angle A'OB' = \angle A'O'B'$, as desired.

Now consider $\angle AVB$, where V need not be the origin O. If $\tau : W \mapsto W - V$ is the translation taking V to the origin, and if $\tau' : W \mapsto W + \sigma(V)$ is the translation taking the origin to $\sigma(V) = V'$, then the composite $\tau'\sigma\tau$ takes

$$W \mapsto W - V \mapsto \sigma(W - V) = \sigma(W) - \sigma(V) \mapsto \sigma(W) - \sigma(V) + \sigma(V) = \sigma(W).$$

Thus, $\sigma(W) = \tau'\sigma\tau(W)$ for all W, so that $\sigma = \tau'\sigma\tau$. Since the translations τ and τ' preserve all angles, not merely those with vertex at the origin, the composite preserves $\angle AVB$. •

The following definition of a *symmetry*, a common generalization of reflections and rotations, should now seem natural.

Definition. Given a figure F in the plane,[2] its ***symmetry group*** $\Sigma(F)$ is the family of all orthogonal transformations $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ for which

$$\sigma(F) = F.$$

The elements of $\Sigma(F)$ are called ***symmetries***.

[2]It is clear that these definitions can be generalized: for every $n \geq 1$, there is an n–dimensional real orthogonal group $O(n, \mathbf{R})$ consisting of all the distance preserving linear transformations of $\mathbf{R}^n$, and symmetry groups of figures in higher dimensional euclidean space are defined as for planar figures.