

RESEARCH NOTES IN MATHEMATICS

TOPICS IN GALOIS THEORY

JEAN-PIERRE SERRE

Topics in Galois Theory

Research Notes in Mathematics

Volume 1

Topics in Galois Theory

Second Edition

Jean-Pierre Serre

Collège de France

Notes written by Henri Darmon

McGill University



A K Peters, Ltd.

Wellesley, Massachusetts

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2007 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20140313

International Standard Book Number-13: 978-1-4398-6525-5 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Contents

Foreword	ix
Notation	xi
Introduction	xiii
1 Examples in low degree	1
1.1 The groups $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, and S_3	1
1.2 The group C_4	2
1.3 Application of tori to abelian Galois groups of exponent 2, 3, 4, 6	6
2 Nilpotent and solvable groups as Galois groups over $\mathbf{Q}$	9
2.1 A theorem of Scholz-Reichardt	9
2.2 The Frattini subgroup of a finite group	16
3 Hilbert's irreducibility theorem	19
3.1 The Hilbert property	19
3.2 Properties of thin sets	21
3.3 Irreducibility theorem and thin sets	23
3.4 Hilbert's irreducibility theorem	25
3.5 Hilbert property and weak approximation	28
3.6 Proofs of prop. 3.5.1 and 3.5.2	31
4 Galois extensions of $\mathbf{Q}(T)$: first examples	35
4.1 The property Gal_T	35
4.2 Abelian groups	36
4.3 Example: the quaternion group Q_8	38
4.4 Symmetric groups	39

4.5	The alternating group A_n	43
4.6	Finding good specializations of T	44
5	Galois extensions of $\mathbf{Q}(T)$ given by torsion on elliptic curves	47
5.1	Statement of Shih's theorem	47
5.2	An auxiliary construction	48
5.3	Proof of Shih's theorem	49
5.4	A complement	52
5.5	Further results on $\mathbf{PSL}_2(\mathbf{F}_q)$ and $\mathbf{SL}_2(\mathbf{F}_q)$ as Galois groups	53
6	Galois extensions of $\mathbf{C}(T)$	55
6.1	The GAGA principle	55
6.2	Coverings of Riemann surfaces	57
6.3	From $\mathbf{C}$ to $\bar{\mathbf{Q}}$	57
6.4	Appendix: universal ramified coverings of Riemann surfaces with signature	60
7	Rigidity and rationality on finite groups	65
7.1	Rationality	65
7.2	Counting solutions of equations in finite groups	67
7.3	Rigidity of a family of conjugacy classes	70
7.4	Examples of rigidity	72
8	Construction of Galois extensions of $\mathbf{Q}(T)$ by the rigidity method	81
8.1	The main theorem	81
8.2	Two variants	84
8.3	Examples	85
8.4	Local properties	89
9	The form $\mathrm{Tr}(x^2)$ and its applications	95
9.1	Preliminaries	95
9.2	The quadratic form $\mathrm{Tr}(x^2)$	98
9.3	Application to extensions with Galois group $\tilde{A}_n$	100
10	Appendix: the large sieve inequality	103
10.1	Statement of the theorem	103
10.2	A lemma on finite groups	105
10.3	The Davenport-Halberstam theorem	105
10.4	Combining the information	107

Contents

vii

Bibliography

109

Foreword

These notes are based on “Topics in Galois Theory,” a course given by J-P. Serre at Harvard University in the Fall semester of 1988 and written down by H. Darmon. The course focused on the inverse problem of Galois theory: the construction of field extensions having a given finite group G as Galois group, typically over $\mathbf{Q}$ but also over fields such as $\mathbf{Q}(T)$.

Chapter 1 discusses examples for certain groups G of small order. The method of Scholz and Reichardt, which works over $\mathbf{Q}$ when G is a p -group of odd order, is given in chapter 2. Chapter 3 is devoted to the Hilbert irreducibility theorem and its connection with weak approximation and the large sieve inequality. Chapters 4 and 5 describe methods for showing that G is the Galois group of a regular extension of $\mathbf{Q}(T)$ (one then says that G has property Gal_T). Elementary constructions (e.g. when G is a symmetric or alternating group) are given in chapter 4, while the method of Shih, which works for $G = \mathbf{PSL}_2(p)$ in some cases, is outlined in chapter 5. Chapter 6 describes the GAGA principle and the relation between the topological and algebraic fundamental groups of complex curves. Chapters 7 and 8 are devoted to the rationality and rigidity criteria and their application to proving the property Gal_T for certain groups (notably, many of the sporadic simple groups, including the Fischer-Griess Monster). The relation between the Hasse-Witt invariant of the quadratic form $\text{Tr}(x^2)$ and certain embedding problems is the topic of chapter 9, and an application to showing that A_n has property Gal_T is given. An appendix (chapter 10) gives a proof of the large sieve inequality used in chapter 3.

The reader should be warned that most proofs only give the main ideas; details have been left out. Moreover, a number of relevant topics have been omitted, for lack of time (and understanding), namely:

- a) The theory of generic extensions, cf. [Sa1].
- b) Shafarevich’s theorem on the existence of extensions of $\mathbf{Q}$ with a given solvable Galois group, cf. [NSW], chap. IX.
- c) The Hurwitz schemes which parametrize extensions with a given Galois group and a given ramification structure, cf. [Fr1], [Fr2], [Ma3].

d) The computation of explicit equations for extensions with Galois group $\mathbf{PSL}_2(\mathbf{F}_7)$, $\mathbf{SL}_2(\mathbf{F}_8)$, M_{11} , ..., cf. [LM], [Ma3], [Ma4], [M1], ...

e) Mestre's results [Me3] on extensions of $\mathbf{Q}(T)$ with Galois group $6 \cdot A_6$, $6 \cdot A_7$, and $\mathbf{SL}_2(\mathbf{F}_7)$.

We wish to thank Larry Washington for his helpful comments on an earlier version of these notes.

Paris, August 1991.

H. Darmon

J-P. Serre

For the second edition of these Notes, some corrections have been made, and the references have been updated.

Paris, June 2004

J-P. Serre

Notation

If V is an algebraic variety over the field K , and L is an extension of K , we denote by $V(L)$ the set of L -points of V and by V/L the L -variety obtained from V by base change from K to L . All the varieties are supposed reduced and quasi-projective.

$\mathbf{A}^n$ is the affine n -space; $\mathbf{A}^n(L) = L^n$.

$\mathbf{P}_n$ is the projective n -space; $\mathbf{P}_n(L) = (L^{(n+1)} - \{0\})/L^*$; the group of automorphisms of $\mathbf{P}_n$ is $\mathbf{PGL}_n = \mathbf{GL}_n/\mathbf{G}_m$.

If X is a finite set, $|X|$ denotes the cardinality of X .

Introduction

The question of whether all finite groups can occur as Galois groups of an extension of the rationals (known as the *inverse problem* of Galois theory) is still unsolved, in spite of substantial progress in recent years.

In the 1930's, Emmy Noether proposed the following strategy to attack the inverse problem [Noe]: by embedding G in S_n , the permutation group on n letters, one defines a G -action on the field $\mathbf{Q}(X_1, \dots, X_n) = \mathbf{Q}(\underline{X})$. Let E be the fixed field under this action. Then $\mathbf{Q}(\underline{X})$ is a Galois extension of E with Galois group G .

In geometric terms, the extension $\mathbf{Q}(\underline{X})$ of E corresponds to the projection of varieties: $\pi : \mathbf{A}^n \longrightarrow \mathbf{A}^n/G$, where $\mathbf{A}^n$ is affine n -space over $\mathbf{Q}$. Let P be a $\mathbf{Q}$ -rational point of $\mathbf{A}^n/G$ for which π is unramified, and lift it to $Q \in \mathbf{A}^n(\bar{\mathbf{Q}})$. The conjugates of Q under the action of $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ are the sQ where $s \in H_Q \subset G$, and H_Q is the decomposition group at Q . If $H_Q = G$, then Q generates a field extension of $\mathbf{Q}$ with Galois group G .

A variety is said to be *rational over $\mathbf{Q}$* (or *$\mathbf{Q}$ -rational*) if it is birationally isomorphic over $\mathbf{Q}$ to the affine space $\mathbf{A}^n$ for some n , or equivalently, if its function field is isomorphic to $\mathbf{Q}(T_1, \dots, T_n)$, where the T_i are indeterminates.

Theorem 1 (Hilbert, [Hi]) *If $\mathbf{A}^n/G$ is $\mathbf{Q}$ -rational, then there are infinitely many points P, Q as above such that $H_Q = G$.*

This follows from Hilbert's irreducibility theorem, cf. §3.4.

Example: Let $G = S_n$, acting on $\mathbf{Q}(X_1, \dots, X_n)$. The field E of S_n -invariants is $\mathbf{Q}(T_1, \dots, T_n)$, where T_i is the i th symmetric polynomial, and $\mathbf{Q}(X_1, \dots, X_n)$ has Galois group S_n over E : it is the splitting field of the polynomial

$$X^n - T_1 X^{n-1} + T_2 X^{n-2} + \cdots + (-1)^n T_n.$$

Hilbert's irreducibility theorem says that the T_i can be specialized to infinitely many values $t_i \in \mathbf{Q}$ (or even $t_i \in \mathbf{Z}$) such that the equation

$$X^n - t_1 X^{n-1} + t_2 X^{n-2} + \cdots + (-1)^n t_n = 0$$