



FIELDS INSTITUTE MONOGRAPHS

THE FIELDS INSTITUTE FOR RESEARCH IN MATHEMATICAL SCIENCES

Brauer Type Embedding Problems

Arne Ledet



American Mathematical Society



FIELDS INSTITUTE MONOGRAPHS

THE FIELDS INSTITUTE FOR RESEARCH IN MATHEMATICAL SCIENCES

Brauer Type Embedding Problems

Arne Ledet



American Mathematical Society
Providence, Rhode Island

The Fields Institute for Research in Mathematical Sciences

The Fields Institute is a center for mathematical research activity, located in Toronto, Canada. Our mission is to provide a supportive and stimulating environment for mathematics research, innovation and education. The Institute is supported by the Ontario Ministry of Training, Colleges and Universities, the Natural Sciences and Engineering Research Council of Canada, and seven Ontario universities (Carleton, McMaster, Ottawa, Toronto, Waterloo, Western Ontario, and York). In addition there are several affiliated universities and corporate sponsors in both Canada and the United States.

Fields Institute Editorial Board: Carl R. Riehm (Managing Editor), Barbara Lee Keyfitz (Director of the Institute), Thomas S. Salisbury (Deputy Director), John Bland (Toronto), Kenneth R. Davidson (Waterloo), Joel Feldman (UBC), R. Mark Goresky (Institute for Advanced Study, Princeton), Cameron Stewart (Waterloo), Noriko Yui (Queen's).

The author was supported in part by a Queen's University Advisory Research Committee Postdoctoral Fellowship.

2000 *Mathematics Subject Classification*. Primary 12F12, 16K50; Secondary 16S35, 12G05.

For additional information and updates on this book, visit
www.ams.org/bookpages/fim-21

Library of Congress Cataloging-in-Publication Data

Ledet, Arne, 1967–

Brauer type embedding problems / Arne Ledet.

p. cm. (Fields Institute monographs, ISSN 1069-5273; 21)

Includes bibliographical references and index.

ISBN 0-8218-3726-5 (alk. paper)

1. Inverse Galois theory. 2. Brauer groups. I. Title. II. Series.

QA247 +

2005042813

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 2005 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

This publication was prepared by The Fields Institute.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 10 09 08 07 06 05

Contents

Introduction	v
Acknowledgments	viii
Chapter 1. Galois Theory	1
Notation	1
1.1. Integral elements	1
1.2. Algebraic extensions and splitting fields	2
1.3. Separability	4
1.4. Galois extensions	6
1.5. The Galois group as permutation group	9
1.6. Reduction modulo primes	11
1.7. Cyclotomic fields	13
1.8. Cyclic extensions and Hilbert Satz 90	15
1.9. Radical extensions and solvability	17
1.10. The normal basis theorem	19
Exercises	21
Chapter 2. Inverse Galois Theory and Embedding Problems	27
2.1. Inverse Galois theory	27
2.2. Definition of Galois theoretical embedding problems	29
2.3. Group cohomology	30
2.4. Brauer type embedding problems	34
Exercises	40
Chapter 3. Brauer Groups	43
3.1. Basic facts about algebras	43
3.2. Simple Artinian rings	44
3.3. Finite-dimensional central simple algebras	46
3.4. The Brauer group	50
3.5. Cyclic algebras	53
3.6. Brauer type embedding problems revisited	56
3.7. Extensions of the dihedral group	59
Exercises	62
Chapter 4. Group Cohomology	67
4.1. The cohomologies in dimensions 0 and 1	67
4.2. Galois Twist	68
4.3. The long-exact cohomology sequence	70
4.4. The corestriction map	72

Exercises	73
Chapter 5. Quadratic Forms	77
5.1. Basic theory of quadratic forms	77
5.2. Clifford algebras	81
5.3. Quadratic forms and non-abelian cohomology	83
Exercises	85
Chapter 6. Decomposing the Obstruction	87
6.1. Decomposition along a direct product	87
6.2. Orthogonal representations	95
6.3. Projective representations	98
Exercises	102
Chapter 7. Quadratic Forms and Embedding Problems	105
7.1. Groups of exponent 4	105
7.2. Witt's Criterion	108
7.3. Groups of exponent 8	114
Exercises	121
Chapter 8. Reducing the Embedding Problem	123
8.1. Reduction to Brauer type embedding problems	123
8.2. Examples: The holomorph of the quaternion group	133
8.3. Embedding problems with cyclic kernel of order 4	141
Exercises	148
Appendix A. Pro-finite Galois Theory	151
Introduction	151
A.1. The separable closure of a field	151
A.2. Galois extensions	152
A.3. Pro-finite groups	154
A.4. Pro-finite Galois theory	156
A.5. Pro-finite group cohomology	157
A.6. Pro-finite cohomology and the Brauer group	158
Exercises	160
Bibliography	163
Index	167

Introduction

Consider a Galois theoretical embedding problem, i.e., the question of embedding a Galois extension M/K with Galois group $G = \text{Gal}(M/K)$ into a larger Galois extension F/K , such that the Galois group $\text{Gal}(F/K)$ is isomorphic to a specified group E and the restriction map from $\text{Gal}(F/K)$ to G corresponds to a given homomorphism $\pi: E \rightarrow G$. How do we approach such a problem? How do we determine whether such an extension F/K exists? How do we find it if it does? Or (preferably) how do we find all of them if there are any?

The answers to these questions of course depend on the kind of embedding problem considered, both with respect to the nature of the groups and the nature of the field. For instance, if G and E are cyclic, it takes nothing more than elementary Galois theory to solve the problem over a finite field, whereas it takes class field theory (or at least some reasonably sophisticated algebraic number theory) to solve it over the field of rational numbers.

The methods of algebraic number theory and class field theory have in fact been put to good use in studying these kinds of problems: In the 1920's, Scholz [76] considered various solvable groups (mostly of small order) over algebraic number fields, and in the 1930's Scholz [77] and Reichardt [70] independently proved that all finite groups of odd prime power order could be realised as Galois groups over any algebraic number field, in both cases by building up the extensions through solving embedding problems 'along' a composition series. This approach culminated in the 1950's with Shafarevich's result that all solvable groups are Galois groups over all algebraic number fields; cf. [32] or [66].

Also in the 1930's, Witt [94] considered groups of prime power order p^n over fields of characteristic p , and essentially proved all involved embedding problems to be trivially solvable. We will touch briefly on this in Chapter 2. In the same paper, Witt solved the problem of embedding a biquadratic extension into an extension with the quaternion group as Galois group. We will get considerable mileage out of that result in Chapter 7.

It is clear that an embedding problem is in a sense a 'local' problem: We should be able to investigate it fully using only the extension M/K and the homomorphism $\pi: E \rightarrow G$, without having to consider 'global' structures like separable closures and absolute Galois groups.¹

In 1932, Brauer [7] introduced a type of embedding problem for which the necessary 'local' information is readily available: In these so-called *Brauer type embedding problems*, where the kernel of π can be identified with a group of roots of

¹This is not to say that separable closures and absolute Galois groups are not useful for theoretical considerations—section 6.2 of Chapter 6 is a good example of this—but simply that they tend to be unwieldy, if only because we do not generally know them.

unity inside M ,² this information is contained in the cohomology group $H^2(G, M^*)$, or the relative Brauer group $\text{Br}(M/K)$, whichever one prefers. This is not only decidedly ‘local’, but quite convenient, since both group cohomology and Brauer group theory are well-developed disciplines, providing ample tools for studying embedding problems.

We should mention here that Brauer was not in fact interested in the embedding problems. He was – naturally enough – interested in the Brauer group, and his concern was the classification of finite-dimensional central division algebras over the field K , and the connection to embedding problems was a reduction, as he writes, from ‘non-commutative’ to ‘commutative’ algebra. We will go the other way, using the fact that the structure of Brauer groups is reasonably well understood.

This monograph, then, is about Brauer type embedding problems, primarily the case where $\ker \pi$ has prime order, and some related embedding problem types. This topic brings together Galois theory, Brauer group theory, group cohomology and the theory of quadratic forms, and all of these subjects are covered in the text, in Chapters 1, 3, 4 and 5. (Chapter 1 differs from most introductions to Galois theory by not containing very many examples; on the other hand, there are plenty of explicitly given Galois extensions in later chapters.) In addition, Appendix A gives an introduction to pro-finite Galois theory.

Chapter 2 provides the set-up, i.e., the basic results, the definitions and the first examples. All done in as elementary a fashion as possible.³ Most importantly, it introduces the *obstruction* to the embedding problem. This is an element in $H^2(G, M^*)$ expressing the solvability (or non-solvability) of the embedding problem. The existence of obstructions is what makes Brauer type embedding problems nice.

Chapter 6 deals with the problem of decomposing the obstruction into convenient factors. Again, section 6.1 is fairly elementary, while section 6.2 relies on pro-finite cohomology. This (and the subsequent section 6.3) is, however, the only place in the monograph we make real use of pro-finite cohomology, and it can be skipped without giving it a second thought, should one so desire.

Chapter 7 explores the connection between Brauer type embedding problems and quadratic forms. Specifically, it provides criteria for solvability for a number of embedding problems in terms of equivalences of quadratic forms, and describes how to find the solutions. This includes the famous result by Witt: A bi-quadratic extension $K(\sqrt{a}, \sqrt{b})/K$ in characteristic $\neq 2$ can be embedded in a Q_8 -extension, if and only if the quadratic forms $\langle a, b, ab \rangle$ and $\langle 1, 1, 1 \rangle$ are equivalent (over K).

The final chapter, Chapter 8, is concerned with reducing embedding problems. As it happens, in some cases embedding problems that are not of Brauer type can be reduced to Brauer type embedding problems and solved as such, thus extending the usefulness of Brauer type embedding problems. In particular, if the embedding problem is non-split with kernel of prime order p (and the characteristic of the involved fields is not p), it can be so reduced.

Another kind of embedding problem that can be reduced to Brauer type is the case where $\ker \pi$ is cyclic of order 4. Such an embedding problem reduces to two Brauer type embedding problems, and the results covering this reduction are given in section 8.3 of Chapter 8.

²See section 2.4 in Chapter 2 for details.

³Or at least reasonable. It is perfectly possible to describe Q_8 -extensions without resorting to Brauer groups, but it is hard to motivate the arguments.

There are of course other ways of looking at embedding problems; cf. [55] and [32], which also contains extensive references. Particularly noteworthy is the study of embedding problems over *Hilbertian* fields (as defined in Chapter 1), where it can be shown that split-exact embedding problems with abelian kernel are always solvable. (The proof, while a little tedious, is not particularly deep, and consists mostly of producing so-called *regular* extensions with prescribed abelian Galois group. We refer to [19].) Most of the groups we will consider can be realised easily as Galois groups over \mathbb{Q} (or any Hilbertian field) by invoking this result. This realisation is generally not, however, very explicit.

Another common approach is to realise the finite group G as a Galois group over $\mathbb{C}(t)$ (as mentioned in Chapter 1, this is always possible) and then attempt to *descend* to $\mathbb{Q}(t)$, followed by specialisation to \mathbb{Q} . Most realisations of finite simple groups (sporadic groups, projective special linear groups, etc.) over \mathbb{Q} have been obtained in this manner. Here, a good reference is Malle & Matzat [55].

A powerful method, which we will make some use of, is the more general application of group cohomology. We will use it as it relates to the Brauer group, but it can easily be employed independently. Here, an important paper is Hoechsmann's *Zum Einbettungsproblem* [30], covering the basics of this approach. Also, Neukirch [65] made great contributions here, using the cohomological description of class field theory to consider problems similar to those of Shafarevich.

Acknowledgments

This monograph grew – in a slow and round-about way – out of my Ph.D.-thesis (University of Copenhagen, 1996). Thus, thanks are due to those who (more or less voluntarily) got involved in that project. First and foremost, this means my thesis advisor, Prof. Christian U. Jensen, who – quite apart from being helpful concerning the actual mathematics – spent a good deal of time and effort convincing me that Brauer type embedding problems are interesting. As it happened, he was right. Also, thanks to Prof. Moshe Jarden, Dr. Dan Haran and Dr. Ido Efrat for comments and suggestions regarding my work during my stay in Tel-Aviv in the spring of 1995.

Thanks to Shreeram Abhyankar for asking the questions that led to Chapter 7,⁴ and to Noriko Yui for suggesting that I try making a monograph out of my thesis and various papers.

The work of producing the manuscript was partly supported by a Queen's University Advisory Research Committee Postdoctoral Fellowship.

Finally, two other things should probably be mentioned here as well: The manuscript was written in $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$, and computer calculations relating to examples were performed using Maple V.

Arne Ledet

⁴Although, unfortunately, his questions are not actually *answered* there.

Bibliography

- [1] A. A. Albert, *Modern Higher Algebra*, Cambridge University Press, 1938.
- [2] J. K. Arason, B. Fein, M. Schacher & J. Sonn, *Cyclic extensions of $K(\sqrt{-1})/K$* , Trans. AMS **313** (1989), 843–851.
- [3] E. Artin, *Galois Theory*, Dover Publications, 1998.
- [4] M. Aschbacher, *Finite Group Theory*, Cambridge Studies in Advanced Mathematics 10, Cambridge University Press, 1986.
- [5] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. Reine Angew. Math. **268/269** (1974), 41–52.
- [6] G. Brattström, *On p -groups as Galois groups*, Math. Scand. **65** (1989), 165–174.
- [7] R. Brauer, *Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind*, J. Reine Angew. Math. **168** (1932), 44–64.
- [8] K. S. Brown, *Cohomology of Groups*, Graduate Texts in Mathematics 87, Springer-Verlag, 1982.
- [9] A. A. Bruen, C. U. Jensen & N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II*, J. Number Theory **24** (1986), 305–359.
- [10] G. Butler & J. McKay, *The transitive groups of degree up to eleven*, Comm. Alg. **11** (1983), 863–911.
- [11] T. Crespo, *Explicit Construction of \tilde{A}_n Type Fields*, J. Algebra **127** (1989), 452–461.
- [12] ———, *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. **409** (1990), 180–189.
- [13] ———, *Embedding Galois problems and reduced norms*, Proc. AMS **112** (1991), 637–639.
- [14] R. Dedekind, *Konstruktion von Quaternionenkörpern*, Gesammelte mathematische Werke, II. Band, Vieweg, Braunschweig, 1931, 376–384.
- [15] F. DeMeyer & E. Ingraham, *Separable Algebras over Commutative Rings*, Lecture Notes in Mathematics 181, Springer-Verlag, 1971.
- [16] J. Diller & A. Dress, *Zur Galois-theorie pythagoreischer Körper*, Archiv der Mathematik **16** (1965), 148–152.
- [17] Ebbinghaus, H.-D., et al., *Numbers*, Graduate Texts in Mathematics 123, Springer 1991.
- [18] D. K. Faddeyev, *Constructions of Fields of Algebraic Numbers whose Galois Group is a Group of Quaternion Units*, C. R. (Dokl.) Acad. Sci. URSS **47** (1945), 390–392.
- [19] M. D. Fried & M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik 11, Springer-Verlag, 1986.
- [20] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.
- [21] H. G. Grundman & T. L. Smith, *Automatic realizability of Galois groups of order 16*, Proc. Amer. Math. Soc. **124** (1996), 2631–2640.
- [22] H. G. Grundman, T. L. Smith & J. R. Swallow, *Groups of order 16 as Galois groups*, Expo. Math. **13** (1995), 289–319.
- [23] R. Guralnick, M. Schacher & J. Sonn, *Irreducible polynomials which are locally reducible everywhere*, preprint, 2004.
- [24] C. R. Hadlock, *Field Theory and its classical Problems*, Carus Mathematical Monographs 19, Mathematical Association of America, 1978.
- [25] H. Hasse, *Invariante Kennzeichnung relativ-abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers*, Abh. Deutsche Akad. Wiss., math.-naturw. Kl. 1947(8), 1–56.

- [26] ———, *Existenz und Mannigfältigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers I–III*, Math. Nachr. **1** (1948), 40–61, 213–217, 277–283.
- [27] F.-P. Heider & P. Kolvenbach, *The Construction of $SL(2, 3)$ -Polynomials*, J. Number Theory **19** (1984), 392–411.
- [28] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.
- [29] P. J. Hilton & U. Stammbach, *A Course in Homological Algebra*, Graduate Texts in Mathematics 4, Springer-Verlag, 1971.
- [30] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.
- [31] B. Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften 134, Springer-Verlag, 1967.
- [32] V. V. Ishkhanov, B. B. Lur'e & D. K. Faddeev, *The Embedding Problem in Galois Theory*, Translations of Mathematical Monographs 165, American Mathematical Society, 1997.
- [33] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, New York, 1985.
- [34] ———, *Basic Algebra II*, W. H. Freeman and Company, New York, 1989.
- [35] C. U. Jensen, *On the representations of a group as a Galois group over an arbitrary field*, Théorie des nombres Number Theory (eds. J.-M. De Koninck & C. Levesque), Walter de Gruyter, 1989, 441–458.
- [36] ———, *Finite groups as Galois groups over arbitrary fields*, Contemporary Mathematics 131: Proceedings of the international conference of algebra 1989, part 2, American Mathematical Society (1992), 435–448.
- [37] C. U. Jensen, A. Ledet & N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, MSRI Publication Series 45, Cambridge University Press, 2002.
- [38] C. U. Jensen & N. Yui, *Quaternion Extensions*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, Kinokuniya, Tokyo, 1987, 155–182.
- [39] G. Kemper & G. Malle, *Invariant fields of finite irreducible reflection groups*, Preprint, 1999.
- [40] I. Kiming, *Explicit Classifications of some 2-Extensions of a Field of Characteristic different from 2*, Canad. J. Math. **42** (1990), 825–855.
- [41] R. Kochendörffer, *Zwei Reduktionssätze zum Einbettungsproblem für abelsche Algebren*, Math. Nachr. **10** (1953), 75–84.
- [42] W. Kuyk & H. W. Lenstra, Jr., *Abelian extensions of arbitrary fields*, Math. Ann. **216** (1975), 99–104.
- [43] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.
- [44] S. Lang, *Diophantine Geometry*, Wiley-Interscience, New York, 1962.
- [45] A. Ledet, *Is Whaples' Theorem a Group Theoretical Result?*, Beitr. Algebra Geom. **34** (1993), 157–161.
- [46] A. Ledet, *On 2-Groups as Galois Groups*, Canad. J. Math. **47** (1995), 1253–1273.
- [47] ———, *Subgroups of $\text{Hol } Q_8$ as Galois Groups*, J. Algebra **181** (1996), 478–506.
- [48] ———, *Embedding Problems with Cyclic Kernel of Order 4*, Israel Jour. Math. **106** (1998), 109–132.
- [49] ———, *Embedding Problems and Equivalence of Quadratic Forms*, Math. Scand. **88** (2001), 279–302.
- [50] ———, *On a Theorem by Serre*, Proc. Amer. Math. Soc. **128** (2000), 27–29.
- [51] H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325.
- [52] F. Lorenz, *Einführung in die Algebra I*, B. I. Wissenschaftsverlag, Mannheim, 1992.
- [53] ———, *Einführung in die Algebra II*, B. I. Wissenschaftsverlag, Mannheim, 1990.
- [54] ———, *Algebraische Zahlentheorie*, B. I. Wissenschaftsverlag, Mannheim, 1993.
- [55] G. Malle & B. H. Matzat, *Inverse Galois Theory*, Monographs in Mathematics, Springer-Verlag, 1999.
- [56] R. Massy, *Construction de p -extensions Galoisiennes d'un corps de caractéristique différente de p* , J. Algebra **109** (1987), 508–535.
- [57] J. C. McConnell, *Division algebras – Beyond the quaternions*, Amer. Math. Monthly **105** (1998), 154–162.
- [58] J. McKay & L. Soicher, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

- [59] A. Merkurjev, *On the norm residue symbol of degree 2*, Soviet Math. (Doklady) **24** (1981), 546–551.
- [60] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois \tilde{A}_n* , J. Alg. **131** (1990), 483–495.
- [61] I. M. Michailov, *Embedding problems with cyclic 2-kernel*, preprint.
- [62] ———, *Embedding obstructions for the dihedral, semidihedral and quaternion 2-groups*, J. Alg. **245** (2001), 355–369.
- [63] J. Mináč & T. L. Smith, *A characterization of C -fields via Galois groups*, J. Algebra **137** (1991), 1–11.
- [64] S. Monier, *Descente de p -extensions galoisiennes kummériennes*, Math. Scand. **79** (1996), 5–24.
- [65] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Inventiones Math. **21** (1973), 59–116.
- [66] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.
- [67] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1916), 221–229.
- [68] G. K. Pedersen, *Analysis Now*, Graduate Texts in Mathematics 118, Springer-Verlag, 1989.
- [69] F. Pop, *Galoissche Kennzeichnung p -adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145–175.
- [70] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math. **177** (1937), 1–5.
- [71] L. Ribes, *Introduction of Profinite Groups and Galois Cohomology*, Queen's Papers in Pure and Applied Mathematics 24, Queen's University, 1970.
- [72] G. Roland, N. Yui & D. Zagier, *A parametric family of quintic polynomials with Galois group D_5* , J. Number Theory **15** (1982), 137–142.
- [73] J. Rotman, *Galois Theory*, Universitext, Springer-Verlag, 1998.
- [74] D. Saltman, *Lectures on Division Algebras*, Regional Conference Series in Mathematics 94, AMS, 1999.
- [75] Leila Schneps, *Explicit Realisations of Subgroups of $GL_2(\mathbb{F}_3)$ as Galois Groups*, J. Number Theory **39** (1991), 5–13.
- [76] A. Scholz, *Über die Bildung algebraischer Zahlkörper mit auflösbarer galoisscher Gruppe*, Math. Z. **30** (1929), 332–356.
- [77] ———, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung*, Math. Z. **42** (1937), 161–188.
- [78] W. R. Scott, *Group Theory*, Dover Publications, New York, 1987.
- [79] J.-P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970.
- [80] ———, *Galois Cohomology*, Springer Monographs in Mathematics, Springer-Verlag, 2002.
- [81] ———, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, 1979.
- [82] ———, *L'invariant de Witt de la forme $\text{Tr}(x^2)$* , Comm. Math. Helv. **59** (1984), 651–676.
- [83] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones & Bartlett, 1992.
- [84] T. L. Smith, *Extra-special groups of order 32 as Galois groups*, Canad. J. Math. **46** (1994), 886–896.
- [85] J. Sonn, *Central extensions of S_n as Galois groups of regular extensions of $\mathbb{Q}(T)$* , J. Alg. **140** (1991), 355–359.
- [86] T. A. Springer, *On the Equivalence of Quadratic Forms*, Proc. Neder. Acad. Sci. **62** (1959), 241–253.
- [87] J. R. Swallow, *Solutions to central embedding problems are constructible*, J. Alg. **184** (1996), 1041–1051.
- [88] ———, *Central p -extensions of (p, p, \dots, p) -type Galois Groups*, J. Alg. **186** (1996), 277–298.
- [89] R. G. Swan, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (eds. B. Srinivasan & J. Sally), Springer-Verlag, New York, 1983, 21–40.
- [90] B. L. van der Waerden, *Einführung in die algebraische Geometrie*, Grundlehren der mathematischen Wissenschaften 51, Springer-Verlag, 1939.
- [91] E. Weiss, *Cohomology of Groups*, Pure and applied mathematics 34, Academic Press, New York, 1969.
- [92] G. Whaples, *Algebraic extensions of arbitrary fields*, Duke Math. J. **24** (1957), 201–204.
- [93] C. J. Williamson, *Odd degree polynomials with dihedral Galois groups*, J. Number Theory **34** (1990), 153–173.

- [94] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f* , J. Reine Angew. Math. **174** (1936), 237–245.

Index

- [c] (cohomology class), 31, 32
- (M, G, c) (crossed product algebra), 47
- (M, σ, b) (cyclic algebra), 47
- $K(n)$ (cyclotomic field), 13
- $[- : K]$ (degree), 2, 49, 155
- $f'(X)$ (formal derivative), 5
- $\langle a_1, \dots, a_n \rangle$ (diagonal form), 77
- \sim , 50, 77
- $[\mathfrak{A}]$ (equivalence class of algebra), 51
- $-^G$ (fixed points), 4, 30, 67
- $[G : H]$ (index), 155
- (a/p) (Legendre symbol), 14
- M^\times , 142
- $M^\times/4$, 142
- R^* (multiplicative group), 2
- n_K , 83
- \mathfrak{A}^{op} (opposite algebra), 48
- U^\perp (orthogonal complement), 78
- $\mathbf{u} \perp \mathbf{v}$ (orthogonal vectors), 78
- $(a, b/K)_p$ (p -cyclic algebra), 55
- $a \equiv_p b$ (p -equivalence), 56
- K^*/p (p -equivalence class group), 56
- $(a, b)_p$ (class of p -cyclic algebra), 56
- $E \times_{(\pi, \kappa)} G$ (pull-back), 33
- $(a, b/K)$ (quaternion algebra), 54
- (a, b) (quaternion class), 55
- $\sqrt[n]{a}$ (radical), 16
- $-_L$ (scalar extension), 44, 68
- $E \rtimes G$ (semi-direct product), 32, 67
- \bar{K}_{sep} (separable closure), 152
- $K^*/2$ (square class group), 55
- A_n (alternating group), 97
- \tilde{A}_n (covering group of A_n), 97
- Abel-Steinitz' Theorem, 7
- Abelian extension, 17
- Absolute Galois group, 152
- Algebra, 43
 - homomorphism, 43
- Algebraic, 2, 43
- Algebraic closure, 160
- Algebraic number field, 13
- Algebraically closed field, 160
- Algebraically independent elements, 10
- Alternating group, 97
 - A_4 as Galois group, 134
- Anisotropic,
 - form, 78
 - vector, 78
- Artin-Schreier, 41
- Artinian ring, 45
- $\text{Aut}_K(M)$ (automorphism group), 4
- Automatic realisation, 102
- $\text{Aut } Q_8$, 133
- $B^1(G, -)$, 31, 68
- $B^2(G, -)$, 32
- $\text{Br}(-)$ (Brauer group), 51
- $\text{Br}_m(-)$ (m -torsion of Brauer group), 55, 56
- Brauer group, 51
- Brauer type embedding problem, 34
- Brauer's Theorem, 30
- \mathbb{C} (field of complex numbers), 9
- $C(q)$ (Clifford algebra), 81
- $C_0(q)$ (even Clifford algebra), 81
- $C_0^*(q)$ (even Clifford group), 82
- $C^*(q)$ (Clifford group), 82
- $C_{\mathfrak{A}}(-)$ (centraliser), 43
- Cardano's Formula, 17
- Casus Irreducibilis, 19
- Cayley's Theorem, 86
- $C \rtimes C$ (semi-direct product), 59
- CDA (central division algebra), 46
- Center, 15, 43
- Central,
 - algebra, 43
 - division algebra, 46
 - simple algebra, 46
- Central extension, 31
- Central product, 93
 - of order 16 as Galois group, 106, 111
 - obstruction, 94
 - of order 32 as Galois group, 107, 109
- Centraliser, 43
- Chinese Remainder Theorem, 160
- Clifford algebra, 81
- Clifford group, 82
- Cohomology class, 31, 32
 - of group extension, 32
- $\text{Coind}^G(-)$ (co-induced module), 76

- Complement (in semi-direct product), 67
- Completely reducible module, 44
- Composite of fields, 8
- Conjugation, 74
- cor (corestriction), 33, 72, 75
- Corestriction, 33, 72
 - in dimension one, 75
 - in dimension zero, 75
- Covering group,
 - of A_n , 97
 - of S_n , 97
- Crossed homomorphism, 16, 25, 26, 30, 68
- Crossed product algebra, 47
- CSA (central simple algebra), 46
- Cyclic algebra, 47
- Cyclic extension, 15
- Cyclic group,
 - as Galois group, 37
 - obstruction, 57
 - of order 16 as Galois group, 146
 - of order 8 as Galois group, 115, 116, 145
- Cyclotomic field, 13
- ∂x (degree), 81
- $d(-)$ (discriminant), 11
- D_{2^n} (dihedral group), 38, 59, 101, 148
- DC (central product), 94
- $D \wedge C$ (pull-back), 59
- DD (central product), 107
- Decomposition field, 12
- Decomposition group, 11
- Dedekind Independence Theorem, 15
- Dedekind's Theorem, 12
- Degree,
 - of CSA, 49
 - of field extension, 2, 155
- Density Theorem, 45
- Diagonal form, 77
- Different, 11
- Dihedral group, 38, 59, 101, 148
 - D_4 as Galois group, 38
 - obstruction, 58
 - D_8 as Galois group, 116, 118
 - obstruction, 61
- Dimension (of algebra), 43
- Dirichlet's Theorem, 15
- Discrete module, 157
- Discriminant, 11
 - of polynomial, 11
 - of quadratic form, 78
 - of quadratic polynomial, 9
- Division algebra, 43
- Domain, 1
 - extension, 1
 - integrally closed, 2
- Double Commutator Theorem, 49
- Dual space, 78
- Eisenstein's Criterion, 4
- Elementary symmetric symbols, 10
- Embedding problem, 29
- Epimorphism, 29
- Equivalence,
 - of algebras, 50
 - of crossed homomorphisms, 68
 - of extensions, 31
 - of quadratic forms, 77
- Étale algebra, 74
- Euler's Lemma, 14
- Euler's parametrisation of $SO_3(\mathbb{R})$, 86
- Even Clifford algebra, 81
- Even Clifford group, 82
- Expressing equivalence, 78
- Extension of group with module, 31
- \mathbb{F}_q (finite field), 6
- Factor system, 31
- Faddeyev, 136
- Field, 1
 - extension, 2
- First cohomology, 68
- First cohomology group, 31
- First Kochendörffer Theorem, 161
- First Supplement, 14
- Fixed point field, 4
- Fixed point group, 30, 67
- Formal derivative, 5
- Frobenius automorphism, 8
- Frobenius' Theorem, 63
- Fröhlich's Theorem, 96
- Fundamental Theorem of Algebra, 9
- Fundamental Theorem of Galois Theory, 7, 156
- G -extension, 6
- G -group, 67
- G -homomorphism, 67
- G -module, 30
- Gal (Galois group), 6, 10, 152
- Galois algebra, 34
- Galois closure, 7
- Galois extension, 6, 152
- Galois group, 6, 10, 152
- Galois twist, 69
 - of CSA, 69
 - of quadratic form, 84
- Gauss' Quadratic Reciprocity Theorem, 14
- General linear group, 26
 - $GL(2, 3)$ as Galois group, 136ff
- GL (general linear group), 26, 49
- $GL(2, 3)$, 134
- Group extension, 29
- \mathbb{H} (Hamiltonian quaternions), 54, 63
- H_{p^3} (Heisenberg group), 39
- $H^0(G, -)$, 30, 67
- $H^1(G, -)$, 31, 68
- $H^2(G, -)$, 32

- Hamilton's Theorem, 86
- Hamilton-Cayley's Theorem, 43
- Hamiltonian quaternions, 54, 63
- Hasse invariant
 - of quadratic form, 85
- Hasse-Witt invariant, 85
- Heisenberg group, 39
 - as Galois group, 39
 - obstruction, 58
 - of order 27 as Galois group, 131
- Hilbert Satz 90, 16
 - additive, 25
- Hilbert's Irreducibility Theorem, 13
- Hilbertian field, 12
- Hochschild-Serre sequence, 126
- Hol (holomorph), 133
- Holomorph, 133
 - of Q_8 as Galois group, 139ff
- Hol Q_8 , 134
- Homogeneous element, 81
- hw(q) (Hasse-Witt invariant), 85

- $I_S(R)$ (integral closure), 2
- Index (of subgroup), 155
- inf (inflation), 33
- Inflation, 33
- Inner product, 77
- Integral
 - closure, 2
 - element, 1
 - extension, 1
- Invariant basis, 26
- Invariant Basis Lemma, 26
- Inverse Galois theory, 27
- Irreducible module, 44
- Isometry, 77
- Isotropic form, 78
- Isotropy vector, 78

- $K_2(K)$ (second K -group), 55
- K -isomorphic, 3
- Kernel, 29
- Kiming, 75
- Klein Vierergruppe, 38
- Kronecker delta, 88
- Krull theory, 151
- Krull topology, 152
- Künneth Formula, 89
- Kummer Theory, 17

- Lagrange's Theorem, 155
- Laurent series, 54, 156
- Legendre symbol, 14
- Leibniz' Rule, 5
- Local-global principle, 57
- Long-exact cohomology sequence, 70

- μ_n (group of roots of unity), 13
- M_{2^n} (modular group), 40

- $\text{Mat}_n(-)$ (matrix ring), 43
- Merkurjev's Theorem, 55
- Merkurjev-Souslin, 56
- Min (minimal polynomial), 3
- Minimal polynomial, 3, 43
- M/K -vector space, 26, 68
- Modular group, 40
 - of order 16 as Galois group, 119, 120
 - obstruction, 92

- N (norm), 16, 30, 44, 83
- Newton power sum, 102
- Newton-Puiseux' Theorem, 161
- Noether equations, 16
- Noether's Problem, 13
- Non-quadratic residue, 14
- Norm,
 - of field extension, 16
 - on algebra, 44
 - on Clifford group, 83
 - on G -module, 30
- Normal basis, 19
- Normal Basis Theorem, 20
 - finite fields, 20
- Normalised factor system, 74
- $\text{Nrd}_{\mathfrak{A}/K}$ (reduced norm), 63
- Numerical decomposition, 91

- $O(q)$ (orthogonal group), 77
- $O_n(K)$ (orthogonal group), 83
- Obstruction (to embedding problem), 56
- Opposite algebra, 48
- Order (of pro-finite group), 155
- Orthogonal,
 - basis, 79
 - complement, 78
 - group, 77
 - representation, 95
 - vectors, 78
- Other non-abelian group of order p^3 , 91
- Other non-abelian group of order twenty-seven, 132

- φ (Euler φ -function), 14
- p -cyclic algebra, 55
- p -equivalence, 56
 - class, 56
- p -independence, 56
- Partial solution (to embedding problem), 34
- Perfect field, 5
- Pfister form, 86
- PGL (projective general linear group), 26, 49
- Pin(q) (Pin-group), 83
- Pin(n)(K) (Pin group), 83
- Prime field, 6
- Primitive element, 7
- Principal crossed homomorphism, 16, 25, 26, 31, 68

- Principal involution, 83
- Pro-finite group, 154
- Projective general linear group, 26
- Projective representations, 98
- Prüfer group, 157
- Pull-back, 33
 - of order sixteen, 59
 - as Galois group, 62
- Purely inseparable, 21
- Purely transcendental, 13
- \mathbb{Q} (field of rational numbers), 11
- Q_L (trace form), 97
- $Q_{2^{n+1}}$ (quaternion group), 59, 91, 101, 148
- QC (central product), 111
- QD_{2^n} (quasi-dihedral group), 59, 148
- QQ (central product), 109
- Quadratic equivalence, 56
- Quadratic extension, 9
- Quadratic form, 77
- Quadratic independence, 56
- Quadratic Reciprocity, 14
- Quadratic residue, 14
- Quadratic space, 77
- Quasi-dihedral group, 59, 148
 - QD_8 as Galois group, 113, 114
 - obstruction, 60
- Quaternion algebra, 54
- Quaternion class, 55
- Quaternion group, 148
 - as Galois group in certain prime characteristics, 101
 - of order 8 as Galois group, 105, 108
 - obstruction, 91
 - of order sixteen, 59
 - as Galois group, 61
- \mathbb{R} (field of real numbers), 9
- Radical, 16
 - extension, 17
- Re (scalar part), 54
- Reduced group extension, 30
- Reduced norm, 63
- Reflection, 79
- Regular module, 73
- Regular quadratic form, 78
- Relative Brauer group, 51
- Relative norm, 126
- Relative trace, 75
- Representing a quadratic form, 78
- Representing an element, 80
- res (restriction), 33, 51
- Restriction,
 - on Brauer groups, 51
 - on cohomology groups, 33
- Restriction-corestriction, 73
- Root field, 3
- Roots of unity, 13
 - primitive, 13
- S (supernatural numbers), 155
- $s(-)$ (Schur index), 49
- σ_F (Frobenius automorphism), 8
- S_n (symmetric group), 10
- \tilde{S}_n (covering group of S_n), 97
- S_p -polynomial, 13
- Scalar extension, 44, 68
- Scalar part (of quaternion), 54
- Schur index, 49
- Schur's Lemma, 44
- Second cohomology group, 32
- Second K -group, 55
- Second Kochendörffer Theorem, 129, 161
- Second Stiefel-Whitney class, 85
- Second Supplement, 24
- Section (of group extension), 31
- Semi-direct product, 32, 67
 - of order sixteen, 59
 - as Galois group, 62
- Semi-linear action, 69
- Separable, 4
- Separable closure, 151
- Separably closed field, 151
- Serre's Theorem, 97
- Shafarevich, 27
- Short-exact sequence, 29
- Simple extension, 7
- Simple ring, 45
- Skew field, 1
- Skolem-Noether's Theorem, 49
- SL (special linear group), 99
- $SL(2, 3)$, 134
- $SO(q)$ (special orthogonal group), 79
- $SO_n(K)$ (special orthogonal group), 83
- Solution (to embedding problem), 29
- Solvability by radicals, 18
- sp (spin norm), 83
- Special linear group, 99
 - $SL(2, 3)$ as Galois group, 134ff
- Special orthogonal group, 79
- Speiser's Theorem, 26
- $Spin(q)$ (spin group), 83
- $Spin_n(K)$ (spin group), 83
- Spin group, 83
- Spin norm, 83
- Split exact, 29
- Splitting factor system, 31
- Splitting field, 3
 - for CSA, 48
- Springer's Theorem, 80
- Square class, 55
- Square root, 9
- Standard representation, 30
- Steinitz number, 155
- Subalgebra, 43
- Subextension, 7
- Supernatural number, 155
- Sylow's Theorems, 161

- Symmetric,
 - functions, 10
 - polynomials, 10
- Symmetric group, 10
 - S_4 as Galois group, 136
- Symmetric Polynomial Theorem, 10
- $T(-)$ (tensor algebra), 81
- $T_v(-)$ (reflection), 79
- Tensor algebra, 81
- Theorem of Accessory Irrationalities, 8
- Topological group, 151
- Torsion of Brauer group, 56
- Tr (trace), 25, 30, 75
- Trace,
 - of field extension, 25
 - on G -module, 30
- Trace form, 97
- Transcendental element, 2, 43
- Transitive subgroup, 10
- Translation Theorem, 8
- Trivial module, 30
- Uniformised factor system, 32
- V_4 (Klein Vierergruppe), 38
- Vec (vector part), 54
- Vector part (of quaternion), 54
- Weak solution (to embedding problem), 34
- Wedderburn's Norm Criterion, 65
- Wedderburn's Theorems, 15, 46
- Whaples' Theorem, 28
- Witt invariant, 85
- Witt vectors, 36
- Witt's Cancellation Theorem, 80
- Witt's Chain Equivalence Theorem, 80
- Witt's Theorem, 108
- \mathbb{Z} (ring of integers), 11
- $Z(-)$ (center), 15, 43
- $\hat{\mathbb{Z}}$ (Prüfer group), 157
- $Z^1(G, -)$, 31, 68
- $Z^2(G, -)$, 31
- Zero-dimensional (topological space), 152
- 0^{th} cohomology, 67

This page intentionally left blank

Titles in This Series

- 21 **Arne Ledet**, Brauer type embedding problems, 2005
- 20 **James W. Cogdell, Henry H. Kim, and M. Ram Murty**, Lectures on automorphic L -functions, 2004
- 19 **Jeremy P. Spinrad**, Efficient graph representations, 2003
- 18 **Olavi Nevanlinna**, Meromorphic functions and linear algebra, 2003
- 17 **Vitaly I. Voloshin**, Coloring mixed hypergraphs: theory, algorithms and applications, 2002
- 16 **Neal Madras**, Lectures on Monte Carlo Methods, 2002
- 15 **Bradd Hart and Matthew Valeriote, Editors**, Lectures on algebraic model theory, 2002
- 14 **Frank den Hollander**, Large deviations, 2000
- 13 **B. V. Rajarama Bhat, George A. Elliott, and Peter A. Fillmore, Editors**, Lectures in operator theory, 2000
- 12 **Salma Kuhlmann**, Ordered exponential fields, 2000
- 11 **Tibor Krisztin, Hans-Otto Walther, and Jianhong Wu**, Shape, smoothness and invariant stratification of an attracting set for delayed monotone positive feedback, 1999
- 10 **Jiří Patera, Editor**, Quasicrystals and discrete geometry, 1998
- 9 **Paul Selick**, Introduction to homotopy theory, 1997
- 8 **Terry A. Loring**, Lifting solutions to perturbing problems in C^* -algebras, 1997
- 7 **S. O. Kochman**, Bordism, stable homotopy and Adams spectral sequences, 1996
- 6 **Kenneth R. Davidson**, C^* -Algebras by example, 1996
- 5 **A. Weiss**, Multiplicative Galois module structure, 1996
- 4 **Gérard Besson, Joachim Lohkamp, Pierre Pansu, and Peter Petersen**
Miroslav Lovric, Maung Min-Oo, and McKenzie Y.-K. Wang, Editors,
Riemannian geometry, 1996
- 3 **Albrecht Böttcher, Aad Dijkstra and Heinz Langer, Michael A. Dritschel and**
James Rovnyak, and M. A. Kaashoek
Peter Lancaster, Editor, Lectures on operator theory and its applications, 1996
- 2 **Victor P. Snaith**, Galois module structure, 1994
- 1 **Stephen Wiggins**, Global dynamics, phase space transport, orbits homoclinic to resonances, and applications, 1993

This monograph is concerned with Galois theoretical embedding problems of so-called Brauer type with a focus on 2-groups and on finding explicit criteria for solvability and explicit constructions of the solutions. The advantage of considering Brauer type embedding problems is their comparatively simple condition for solvability in the form of an obstruction in the Brauer group of the ground field.

This book presupposes knowledge of classical Galois theory and the attendant algebra. Before considering questions of reducing the embedding problems and reformulating the solvability criteria, the author provides the necessary theory of Brauer groups, group cohomology and quadratic forms. The book will be suitable for students seeking an introduction to embedding problems and inverse Galois theory. It will also be a useful reference for researchers in the field.



For additional information
and updates on this book, visit

www.ams.org/bookpages/fim-21

ISBN 0-8218-3726-5



9 780821 837269

FIM/21

AMS on the Web
www.ams.org