Progress in Mathematics
Vol. 48

Edited by
J. Coates and
S. Helgason

Birkhäuser Verlag
Boston · Basel · Stuttgart

A. Fröhlich

Classgroups and Hermitian Modules

1984

Birkhäuser
Boston · Basel · Stuttgart

Author:

A. Fröhlich
Mathematics Department and Mathematics Department
Imperial College Robinson College
London Cambridge
England England

Library of Congress Cataloging in Publication Data

Fröhlich, A. (Albrecht), 1916–
Classgroups and Hermitian modules.

(Progress in mathematics ; vol. 48)
Bibliography: p.
Includes index.
1. Class groups (Mathematics) 2. Modules (Algebra)
I. Title. II. Series: Progress in mathematics (Boston, Mass.) ; vol. 48.
QA247.F7583 1984 512'.74 84-11109
ISBN-13: 978-1-4684-6742-0

CIP-Kurztitelaufnahme der Deutschen Bibliothek

Fröhlich, Albrecht:
Classgroups and hermitian modules / A. Fröhlich.
– Boston ; Basel ; Stuttgart : Birkhäuser, 1984.
(Progress in mathematics ; Vol. 48)
ISBN-13: 978-1-4684-6742-0

NE: GT

Softcover reprint of the hardcover 1st edition 1984

ISBN-13: 978-1-4684-6742-0 e-ISBN-13: 978-1-4684-6740-6
DOI: 10.1007/978-1-4684-6740-6

9 8 7 6 5 4 3 2 1

To

Ruth, Sorrel and Shaun

An earlier version of these notes has been circulated and quoted under the title "Classgroups, in particular Hermitian Classgroups" .

PREFACE

These notes are an expanded and updated version of a course of lectures which I gave at King's College London during the summer term 1979. The main topic is the Hermitian classgroup of orders, and in particular of group rings. Most of this work is published here for the first time.

The primary motivation came from the connection with the Galois module structure of rings of algebraic integers. The principal aim was to lay the theoretical basis for attacking what may be called the "converse problem" of Galois module structure theory: to express the symplectic local and global root numbers and conductors as algebraic invariants. A previous edition of these notes was circulated privately among a few collaborators. Based on this, and following a partial solution of the problem by the author, Ph. Cassou-Noguès and M. Taylor succeeded in obtaining a complete solution. In a different direction J. Ritter published a paper, answering certain character theoretic questions raised in the earlier version. I myself disapprove of "secret circulation", but the pressure of other work led to a delay in publication; I hope this volume will make amends. One advantage of the delay is that the relevant recent work can be included. In a sense this is a companion volume to my recent Springer-Ergebnisse-Bericht, where the Hermitian theory was not dealt with.

Our approach is via "Hom-groups", analogous to that followed in recent work on locally free classgroups. In fact our notes also include the first really systematic and comprehensive account of this approach to classgroups in general. Moreover, the theory of the Hermitian classgroup has some new arithmetic features of independent interest in themselves, and one of our aims was to elaborate on these.

I want to record my thanks to all those involved in the new Mathematics Institute in Augsburg, who took over so willingly and efficiently the physical production of these notes.

TABLE OF CONTENTS

INTRODUCTION

The original motivation for the theory described in these notes stems from the study of "Hermitian modules" over integral group rings, and more generally over orders. The forms considered are more general than those on which the main interest of topologists and K-theorists had been focused, in that now no condition of non-singularity in terms of the order (rather than the algebra) is attached. The significance of such more general forms comes in the first place from algebraic number theory: the ring of integers in a normal extension is a Galois module with an invariant form, in terms of the trace. Topologists have however also had to consider such forms.

Apart from this application, our results are of independent arithmetic interest in that they generalise classical ones on quadratic or Hermitian lattices. The central theme is the "discriminant problem" which we shall discuss in some detail later in this introduction, and the central concept for its solution is the Hermitian classgroup. Here, as already in preceding work in a purely module theoretic context (cf. [F7]) we work with locally free modules rather than with projectives, and classgroups are consistently described in terms of "Hom-groups", i.e., of groups of Galois homomorphisms, also to be discussed in some further remarks later in this introduction. It will then become worthwhile, and even unavoidable, to look systematically also at those other classgroups, which are defined before Hermitian structure is introduced, from this new general point of view and within this new convenient language. The reader whose interest is restricted to these pre-Hermitian aspects should read Chapter I and the relevant parts of Chapters IV and V.

The approach to classgroups which we are developing arose out of the investigation of the Galois module structure of algebraic integer rings in tame normal extensions and its connection with the functional equation of the Artin L-function (cf. [F7]; [F12]).

Subsequently a parallel theory came into being, in the first place in the local context, in which the Hermitian module structure became the principal object of study (cf. [F8], [F10]); here the form comes from a relative trace, more conveniently expressed however as a form into the appropriate group ring. Again the crux of the theory lies in the connections with (now) local root numbers and Galois Gauss sums. Both in the global case and in the local Hermitian case the crucial link between the arithmetic constants on the one hand and the classgroup invariants on the other is formed by the generalised resolvents, and it is at this stage that the new Hom language for classgroups becomes absolutely vital.

Let then F be a field (say of characteristic zero), F_c its algebraic closure, $\Omega_F = \mathrm{Gal}(F_c/F)$ the absolute Galois group over F. Let Γ be a finite group - which turns up as relative Galois group over F - and R_Γ the additive group of virtual characters. Then the various classgroups are to be described in terms of groups such as $\mathrm{Hom}_{\Omega_F}(R_\Gamma, G)$ for varying Ω_F-modules G. Resolvents give rise to elements of such groups, or of related ones. On the other hand if e.g., F is a numberfield with ring of integers $\mathcal{O}$ then the classgroup $\mathrm{Cl}(\mathcal{O}\Gamma)$ of the integral group ring $\mathcal{O}\Gamma$ appears as a quotient of $\mathrm{Hom}_{\Omega_F}(R_\Gamma, J(F_c))$, J the idele group. The class in $\mathrm{Cl}(\mathcal{O}\Gamma)$ of the ring of integers in a tame, normal extension of F, with Galois group Γ is then described in terms of the above Hom-group via the resolvents. Going beyond group rings, if we consider orders in a semisimple algebra A over F, we have to replace R_Γ by a corresponding object, the Grothendieck group $K_{A,F}$ of (equivalence classes of) matrix representations of A over F_c, i.e., we study Hom groups $\mathrm{Hom}_{\Omega_F}(K_{A,F}, G)$. In this language the determinant of a matrix, or more generally the reduced norm of an element a of $A^* = GL_1(A)$ or of $GL_n(A)$ is replaced by a Galois homomorphism $K_{A,F} \to F_c^*$ (multiplicative group), again called the determinant and denoted by $\mathrm{Det}(a)$. It maps the representation class χ (in the group case the character χ) given by a matrix T into the determinant $\mathrm{Det}_\chi(a) = \mathrm{Det}\, T(a) \in F_c^*$.

Even apart from its suitability for the arithmetic applications, the advantages of a consistent use of the Hom language are tremendous.

Thus the behaviour of classgroups under change of algebra or order (going up or going down) has a very natural description and becomes much more transparent than hitherto, in terms of Hom groups. The crucial point here is that previous descriptions - whether ideal theoretic or idele theoretic - were formulated essentially in terms of the simple components, i.e., of the set of irreducible representations, and these are not preserved. To give but one example, let Δ be a subgroup of the group Γ. Then extension of scalars from $\mathfrak{o}\Delta$ ($\mathfrak{o}$ as above) to $\mathfrak{o}\Gamma$ yields a map $\mathrm{Cl}(\mathfrak{o}\Delta) \to \mathrm{Cl}(\mathfrak{o}\Gamma)$, which in terms of the Hom groups is the contravariant image under the functor Hom of the restriction $R_\Gamma \to R_\Delta$ of characters. The other way round, the map $\mathrm{Cl}(\mathfrak{o}\Gamma) \to \mathrm{Cl}(\mathfrak{o}\Delta)$ given by restriction of scalars, comes in our description from the induction $R_\Delta \to R_\Gamma$ of characters. Neither $R_\Gamma \to R_\Delta$, nor $R_\Delta \to R_\Gamma$ can be described by considering only irreducible characters, and this is the reason why the old way of looking at the classgroup $\mathrm{Cl}(\mathfrak{o}\Gamma)$ was useless in this context. Precisely analogous formalisms also apply to all the other classgroups which we shall consider. In the case of group rings, the Hom groups admit also multiplication by appropriate character rings, and this makes the property of classgroups to define Frobenious modules more accessible. We shall presently also indicate the usefulness of the Hom-language in a unified description of discriminants for Hermitian modules.

In a different direction the presentation of classgroups by Galois homomorphisms has led to the discovery of certain natural subgroups and quotients, which have provided new insights and helped considerably in explicit calculations. Indeed the methods of computation which arise are far-reaching generalisations of the old fibre diagram techniques.

Next we come to the "discriminant problem". We first consider the well known classical situation of a quadratic lattice (X,h) - either for numberfields or for, say, their p-adic completions. Here h is a non-singular quadratic form over the given field F and X a lattice over its ring $\mathfrak{o}$ of integers spanning the underlying vector space of h. There is a classical notion of the discriminant of (X,h), as a fractional ideal of $\mathfrak{o}$, i.e., a non zero element (locally) or an idele (globally) modulo units (units ideles) of $\mathfrak{o}$. This however can be strengthened appreciably by defining the discriminant modulo unit squares (unit idele squares) (cf. [F1] - and it is this latter, stronger concept which we want to generalise - and we discuss the problem in these terms, (although in fact a further improvement is needed as we shall indicate below). We now consider a Hermitian form h over a (semisimple) algebra A with involution, together with a locally free module X over the given order A, where X spans the A-module underlying h. To simplify matters we shall assume that X is actually free over A - and indeed the general definition of the discriminant reduces to this case and all the essential features already appear. As in the classical case of quadratic lattices, one then forms the discriminant matrix $(h(x_i,x_j))$ corresponding to an A-basis $\{x_i\}$ of X. The obvious approach would now be to define the discriminant analogously to the classical one, just using the generalisation of determinants mentioned already, i.e., as the Galois homomorphism $\mathrm{Det}(h(x_i,x_j))$ with values $\mathrm{Det}_\chi(h(x_i,x_j))$. Here however a difficulty is encountered, which is absent in the classical case. To illustrate this, suppose for the moment that A is simple, χ the corresponding irreducible representation class, and so Det_χ essentially the reduced norm. The involution is then of one of three possible types: Orthogonal, unitary or symplectic. For the first two everything works fine, but in the symplectic case the values of Det_χ on symmetric elements are squares. If e.g., A is a quaternion algebra with the standard involution then the symmetric elements a are those in the centre F, and for $a \in F^*$, $\mathrm{Det}_\chi(a) =$ reduced norm $(a) = a^2$. Thus Det_χ has a canonical square root on symmetric elements in this case, namely $\sqrt{\mathrm{Det}_\chi(a)} = a$. This generalises - via the almost ancient notion of a Pfaffian Pf(S) which we view here as attached in the first place to a matrix S symmetric under a symplectic involution. In this context Pfaffians were already introduced by C.T.C. Wall in certain cases, specifically for the classification of based skew-symmetric forms over a field (cf. [Wa2] and of Hermitian forms over a quaternion algebra (cf. [Wa3]). Just as in the description of ordinary classgroups, we want however to get away from the restriction to simple or more generally indecomposable involution algebras. We are aiming at a unified definition of a discriminant, not one "by cases", i.e. one which covers indecomposable algebras with orthogonal, unitary as well as with symplectic involutions and works smoothly for semisimple algebras when all these three types may simultaneously be involved. The correct language is again that of

Galois homomorphisms and the definition is then obtained via a generalisation of a Pfaffian essentially analogous to that given for determinants. In the classical case of a quadratic lattice our discriminant then indeed reduces to the "strong" discriminant, i.e., taken modulo unit squares, or unit idele squares. In fact however our discriminant is an even stronger invariant than might appear from this analogy - there is a further refinement involved which e.g. in the classical case of a Hermitian lattice, with respect to a non-trivial involution of the field, yields a better discriminant than the obvious one. The details are too technical to be discussed here.

The results of the Hermitian theory are of some arithmetic interest. One aspect is a deviation from Hasse Principle, best described in terms of a map from the global Hermitian classgroup into what we call the adelic Hermitian classgroup, i.e., essentially a restricted product of the local groups. This has in general both a non-trivial kernel and a non-trivial cokernel. Contrary to previous belief of experts, there is thus a genuine global aspect to the theory. In the case of ordinary quadratic lattices one of the consequences is the theorem (Hecke) that the ideal class of a discriminant is a square. A generalisation of this theorem is thus one of the Corollaries of our global-local set up. Moreover although, as pointed out initially, the forms considered here are not in general non-singular over the order, as they are in the usual Hermitian K-theory, some of our results are both new and relevant in the latter context - in particular those at the level of algebras, rather than orders.

The main arithmetic motivation comes of course from the study of rings of integers and trace forms under the action of a Galois group. The applications in this direction lead to deep results, expressing a connection with the functional equation of the Artin L-functions.

In the rapid development, over the last twelve years, of the theory of global Galois module structure one has mainly considered the ring of algebraic integers in a tame, relative Galois extension with Galois group Γ, as a module over the integral group ring $\mathbb{Z}\Gamma$. Its class was shown to be determined by the values of the Artin root number, i.e. the constants in the functional equation, for symplectic characters. Conversely, however, this class of the Galois module does not in general determine the symplectic root numbers.

I guessed early on that one would have to introduce further structure, and that this would have to be the Hermitian structure given by the trace form. The theory as developped previously by K-theorists, with applications mainly on topology, was entirely unsuitable. It could only have dealt with unimodular trace forms, i.e. with non-ramified extensions. I was thus led to develop a more general Hermitian theory and to apply it in the arithmetic context outlined above. The application is based on (i) a rule I found, which expresses Pfaffians in this particular situation in terms of resolvents and (ii) the relation between my resolvents and the Galois Gauss sums, which forms also the basis of the global Galois module theory. This general formalism and some specific partial results led me to the conjecture, that the given arithmetic Hermitian structure determines the symplectic root numbers both globally and locally. This has now been proved by Ph. Cassou-Noguès and M. Taylor, using (iii) some sharp results on certains Hermitian classgroups and (iv) a theorem on Galois Gauss sums which already formed part of Taylor's proof of the main theorem on global Galois module structure. Here we shall give the details of the aspects under (i) and (iii) above and quote the relevant theorems for (ii) and (iv) - as these really lie outside the scope of these notes.

Definitions and results will be presented on the level of generality best suited our purpose and framework, and this means not necessarily in the widest possible generality. Chapter I is "pre-Hermitian". The basic theory of the discriminant and the Hermitian classgroup is in Chapter II. In Chapter III we study the indecomposable case explicitly and in further detail. Chapter IV is concerned with change of order and in Chapter V we deal with the specific situation of group rings. There follows in Chapter VI a brief outline of the application to Hermitian Galois module structure of rings of integers.

Notation and conventions. Throughout we shall use the standard symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ for the set of natural numbers, the ring of integers, the fields of rationals, p-adic rationals, reals and complex numbers respectively, and for the real quaternion division algebra. All rings R have identities, preserved by homomorphisms, and acting as identities on modules; R^* is the multiplicative group of invertible elements of R, $M_n(R)$ the ring of n by n matrices over R and so $GL_n(R) = M_n(R)^*$. If Γ is a finite group, $R\Gamma$ is its group ring over R .

Throughout $\mathcal{O}$ is a Dedekind domain, F its quotient field, A a finite dimensional separable F-algebra and Λ an order over $\mathcal{O}$ in A , i.e., spanning A - with further conditions imposed and variants of these notations - mostly self-explanatory - introduced, as required. "In principle" F is assumed to have characteristic zero, which means that all definitions and results, stated without further hypothesis are valid in this case. Frequently, but not always, they remain valid in other characteristics. But we do not want to clutter up the exposition, and we leave it to the interested reader to find the true level of generality for himself.

Part of the arithmetic theory will be formulated with stronger restrictions, in terms of the three cases - the ones of real interest to us - namely (i) $\mathcal{O} = F$ (referred to as the "field case"), (ii) F a number field (i.e., finite over $\mathbb{Q}$), $\mathcal{O}$ its ring of algebraic integers (the "global case") (iii) F a local field by which we mean, unless otherwise mentioned, a finite extension of $\mathbb{Q}_p$ for some finite prime p , and $\mathcal{O}$ its valuation ring (the "local case"). Again often definitions and results extend to arbitrary pairs $\mathcal{O}$, F , provided they are suitably reworded.

If F is a field with prime divisor $\mathfrak{p}$, subscript $_{\mathfrak{p}}$ denotes completion at $\mathfrak{p}$. If $\mathfrak{p}$ actually comes from a non zero prime ideal of $\mathcal{O}$, also denoted by $\mathfrak{p}$, i.e., if $\mathfrak{p}$ is a finite prime then $M_{\mathfrak{p}} = M \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$ is the completion of an $\mathcal{O}$-lattice M . If $\mathfrak{p}$ is an infinite prime in a numberfield F , we formally set $M_{\mathfrak{p}} = M \otimes_{\mathcal{O}} F_{\mathfrak{p}}$ for $\mathcal{O}$-lattices M .

As already used earlier, the symbol F_c is the algebraic closure of a field F and $\Omega_F = \mathrm{Gal}(F_c/F)$ the absolute Galois group over F.

Propositions and Lemmata are numbered within each chapter, giving section number and ordinal - and similarly for equations. Back references without roman chapter numerals are within the given chapter. Theorems are numbered consecutively throughout these notes.