Jahresbericht der Deutschen Mathematiker-Vereinigung (2021) 123:153–181
https://doi.org/10.1365/s13291-021-00233-5

SURVEY ARTICLE

Fitting Ideals in Number Theory and Arithmetic

Cornelius Greither[1]

Accepted: 19 April 2021 / Published online: 27 May 2021

Abstract
We describe classical and recent results concerning the structure of class groups of number fields as modules over the Galois group. When presenting more modern developments, we can only hint at the much broader context and the very powerful general techniques that are involved, but we endeavour to give complete statements or at least examples where feasible. The timeline goes from a classical result proved in 1890 (Stickelberger's Theorem) to a recent (2020) breakthrough: the proof of the Brumer-Stark conjecture by Dasgupta and Kakde.

Keywords Class groups · Fitting ideals · Cohomology · Iwasawa theory

1 Introduction

This survey article intends to describe developments that originate in classical algebraic number theory and by now have established intimate connections with modern arithmetic, involving elaborate concepts (cohomology, derived categories) and deep far-reaching conjectures (equivariant Tamagawa number conjectures, main conjectures, ...). The subject is the study of class groups, using all the "symmetries" that are available.

More concretely, to every algebraic number field K one attaches its class group cl_K. The quickest approach is to take the (multiplicative) group of all nonzero fractional ideals and factor out by the subgroup of principal fractional ideals. Bypassing fractional ideals, one may also take the set of equivalence classes of ideals $0 \neq J \subset \mathcal{O}_K$ (the ring of integers in K), modulo the equivalence relation $J \sim J'$ iff $J' = xJ$ for some $x \in K^*$. Either way one obtains the same finite abelian group cl_K, which is the trivial group iff all ideals are principal; in other words, iff $\mathcal{O}_K$ admits unique factorization into prime elements. Assuming unique factorization in suitable rings of cyclotomic integers was a classical way of attacking Fermat's Last Theorem.

Class groups have been studied for a long time as abelian groups, that is, as $\mathbb{Z}$-modules. When K/k is a Galois extension of number fields with Galois group G

✉ C. Greither
cornelius.greither@unibw.de

[1] Fakultät INF, Universität der Bundeswehr München, 85577 Neubiberg, Germany

(some more details on this below), then cl_K has a natural action of G, and this makes it into a module over the group ring $\mathbb{Z}[G]$. This extra structure is not an impediment but a boon! For example one can show easily using this that the cubic subfield of $\mathbb{Q}(\zeta_{163})$ cannot have class number 2. (It is in fact 4; already Kummer was interested in this.)

Given the $\mathbb{Z}[G]$-module cl_K, one may set oneself various goals. (1) Determine the module up to isomorphism. (2) Determine its cardinality. (3) Find nontrivial annihilators (elements $x \in \mathbb{Z}[G]$ with $x\, cl_K = 0$). (4) Try to find invariants of the module that fall short of describing it up to isomorphism but still convey a lot of information. Now goal (1) is far too ambitious. (In this context an interested reader might look at the Cohen-Lenstra heuristics.) (2) neglects the G-structure so is not what we are looking for. (3) is a very worthwhile goal, and historically the first to be achieved in interesting cases. Even though the statement of goal (4) is until now the haziest, it is the most realistic and the most promising. This is what we will focus on; the invariants to be studied are the so-called Fitting ideals, introduced by Hans Fitting around 1936 (by the way, his main field was group theory, not module theory or number theory).

The formal definition, as well as the discussion of examples and properties of Fitting ideals, will be given in the next section. To give a very first idea, the initial Fitting ideal of a finite $\mathbb{Z}$-module M is the ideal $|M|\mathbb{Z}$, and the smallest i such that the i-th Fitting ideal is "trivial", i.e. equal to $\mathbb{Z}$, equals the minimal number of generators.

In Sect. 3 we enter into the heart of the matter. We review the classical cyclotomic theory and the very explicit definition of Stickelberger elements and ideals; then we formulate Stickelberger's venerable annihilation theorem. By a sort of counting argument, this leads to our first exact calculation of a Fitting ideal of a class group, under a cyclicity assumption. We then explain (and this is already much more recent) how to get rid of that assumption. Very importantly, we also explain the link from Stickelberger elements to values of Dirichlet L-functions at $s = 0$. As soon as we leave the cyclotomic setting, no quick construction of an analog of Stickelberger elements is known, and as a substitute one *defines* generalized Stickelberger elements $\theta_{K/k} \in \mathbb{C}[G]$, prescribing the values $\chi(\theta_{K/k})$ for χ ranging over the characters of G via L-values.

All existing results on Fitting ideals of class groups "on the minus side" (this will be explained) involve one or many generalized Stickelberger elements. The methods vary a lot and we will not yet go into details in this introduction. The direct approach of the cyclotomic case cannot be transferred; one needs to invoke, or assume (as the status may be) the validity of deep conjectures like the Main Conjecture in Iwasawa theory and the Equivariant Tamagawa Number Conjecture (ETNC). Often a standard approach will not yield the Fitting ideal of the module one wants but only a related module. One particular instance of this is that one often gets (for reasons that can be made plausible) not the class group itself but its Pontryagin dual.

At the end of this article we discuss a result which might look weak at first glance. It establishes, without appealing to unproved conjectures, that a certain generalized Stickelberger element lies in the Fitting ideal of the Pontryagin dual of the class group. But this result due to Dasgupta and Kakde is in fact extremely strong, since it gives an almost completely general proof of the Brumer conjecture. And this conjecture reduces in the cyclotomic case, more or less, to Stickelberger's classical theorem, so that we have come full circle.

For a long time, starting with Artin and Hasse, an important analog of number fields has been studied as well: so-called global functions fields. These are, by definition, finite extensions of $\mathbb{F}(t)$, where $\mathbb{F}$ is any finite field and t a variable. Equivalently, they are characterized as the function fields of algebraic curves over finite fields. Number fields and global function fields are subsumed under the notion "Global Fields", and sometimes both cases are treated simultaneously. The theories (in particular the notions of class groups) are astonishingly similar, but sometimes the function field case is easier. For reasons of space, the function field case will not be treated in this survey.

The experts among the readers will notice at once that our approach is fairly explicit and relatively elementary. This is intentional, for expository reasons, even though it unfortunately entails omitting or glossing over important general concepts. We do not even have room to discuss the relevant parts of class field theory, which is, one might say, the better part of algebraic number theory. Nor do we have room even for the basics of Galois and étale cohomology, which is, one might say, the better part of class field theory, as supported by the mere title of the standard reference [28] by Neukirch, Schmidt and Wingberg. All we can do is to offer a short and arbitrary list of things not covered, at the end of the article. The author would like to thank Alessandro Cobbe and Sören Kleine for a lot of extremely helpful comments.

2 An Introduction to Fitting Ideals

Let us review the basic theory of Fitting ideals, including enough examples (we hope) to give the reader an impression of what is going on. The initial Fitting ideal of a module is an indicator of its "size"; all Fitting ideals, the initial one and the higher ones, convey information about the structure of the module. We abbreviate "finitely generated" to "f.g." consistently. For f.g. torsion modules over a Dedekind ring, the knowledge of *all* Fitting ideals describes the module entirely. Over more general rings, or if one only has the initial Fitting ideal, this cannot be expected. Nevertheless, the initial Fitting ideal is a fairly simple means of conveying a lot of information about a module. Fitting ideals were created by and named after Hans Fitting, see [9]. Among the more recent textbooks, [31] has become the standard reference for the basic theory; but let us try to develop things from scratch now.

We fix a commutative Noetherian ring R and define, as a first step, the *initial Fitting ideal* $\mathrm{Fitt}_{0,R}(M)$ for any f.g. R-module M. This is also called the *zeroth* Fitting ideal. For any $n \in \mathbb{N}$, we will denote by R^n the module of columns vectors with n entries, all in R. This is a free R-module of rank n. A so-called *free presentation* of M is given by an R-linear map $R^m \to R^n$ having cokernel (isomorphic to) M. Written as an exact sequence, this reads

$$R^m \xrightarrow{A\cdot} R^n \longrightarrow M \longrightarrow 0.$$

The map $R^m \to R^n$ is given as multiplication by the $n \times m$ matrix A with coefficients in R, from the left. Now $\mathrm{Fitt}_{0,R}(M)$ is by definition the ideal generated by all n-minors of A; that is, the determinants of all n by n submatrices of A. One immediate observation is that this ideal is zero for $m < n$. If in particular $M = R^n$ with $n > 0$,

then we can take $m = 0$, or any m we like and A the zero matrix, so $\mathrm{Fitt}_{0,R}(R^n)$ is zero for $n > 0$.

Of course one has to make sure that the Fitting ideal is well defined. We will not give a full proof, but some explanation. A free presentation arises by taking an epimorphism $\pi : R^n \to M$ and choosing a system of R-generators of the kernel of π; these generators then make up the columns of A. One first shows that the ideal generated by the n-minors of A is independent of the particular choice of A, in other words, it only depends on the submodule $\ker(\pi)$. Then one considers what happens if one generator is added; that is, if R^n is replaced by R^{n+1}. Of course the kernel of the surjection will also change, but one can show that the resulting ideal is unchanged. This "adding of generators" can of course be repeated. Finally one takes two surjections $\pi : R^n \to M$ and $\pi' : R^{n'} \to M$ and looks at the combined surjection $\psi = (\pi, \pi') : R^{n+n'} = R^n \oplus R^{n'} \to M$. The previous arguments then allow to see that the ideal generated by the appropriate minors arising from the kernel of π agrees with that arising from the kernel of ψ; and likewise for π' and ψ.

Good examples are afforded by f.g. torsion modules over $\mathbb{Z}$. It is well known that every such module is isomorphic to a direct product of cyclic ones:

$$M \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}.$$

This leads to an obvious presentation $\mathbb{Z}^n \to \mathbb{Z}^n \to M \to 0$, involving the diagonal matrix $A = diag(a_1, \ldots, a_n)$. There is only one n-minor of this matrix, namely $\det(A)$ itself. So the (initial) Fitting ideal of M over $\mathbb{Z}$ is the ideal generated by $a_1 \ldots a_n$; and if we pick this number to be positive, it also happens to equal the order of the module M! Most of this can be generalized to modules over Dedekind rings.

We now list a few general properties of initial Fitting ideals and give some of the proofs.

Lemma 1 (a) *For any ideal I of R we have* $\mathrm{Fitt}_{0,R}(R/I) = I$.
(b) *If M' is an epimorphic image of the R-module M, then* $\mathrm{Fitt}_{0,R}(M) \subset \mathrm{Fitt}_{0,R}(M')$.
(c) Fitt *is multiplicative on direct sums*: *for any two f.g. R-modules M and N we have* $\mathrm{Fitt}_{0,R}(M \oplus N) = \mathrm{Fitt}_{0,R}(M) \cdot \mathrm{Fitt}_{0,R}(N)$.
(d) *This does not generalize to short exact sequences. If $0 \to M \to X \to N \to 0$ is a short exact sequence of R-modules* (*this simply means X surjects onto N with kernel isomorphic to M*), *then it does not follow that* $\mathrm{Fitt}_{0,R}(X) = \mathrm{Fitt}_{0,R}(M) \cdot \mathrm{Fitt}_{0,R}(N)$.
(e) *Fitting ideals commute with base change. Explicitly, if S is a commutative ring extension of the ring R and M is any f.g. R-module, then we have*

$$\mathrm{Fitt}_{0,S}(S \otimes_R M) = S\,\mathrm{Fitt}_{0,R}(M) \subset S.$$

Proof (a) We can take $n = 1$ and A the row containing a list of generators $x_1, \ldots, x_m$ for the ideal I, and we get $\mathrm{Fitt}_{0,R}(R/I) = I$.

(b) Take a presentation of M, that is, an epimorphism $\pi : R^n \to M$. This leads to a matrix A, whose columns are a system of generators of $\ker(\pi)$. Now suppose M surjects onto M' and let $\pi' : R^n \to M'$ be the composed surjection. Of course then $\ker(\pi')$ contains $\ker(\pi)$. This means that the corresponding matrix A' can be gotten

from A just by adjoining some more columns. And then clearly every n-minor of A is an n-minor of A', which proves the claimed inclusion.

(c) This is a fairly simple calculation involving determinants which we omit.

(d) We give a counterexample. Assume R is a local ring whose maximal ideal $\mathfrak{m}$ requires two generators, x and y say. Then $N = \mathfrak{m}/\mathfrak{m}^2$ is isomorphic to $R/\mathfrak{m} \oplus R/\mathfrak{m}$, hence its Fitting ideal is $\mathfrak{m}^2$ (the square of the Fitting ideal of $R/\mathfrak{m}$). On the other hand, $X = R/\mathfrak{m}^2$ sits in a short exact sequence

$$0 \to N \to X = R/\mathfrak{m}^2 \to M = R/\mathfrak{m} \to 0.$$

The product of the Fitting ideals of N and of M gives $\mathfrak{m}^3$, hence Fitt is not multiplicative on this s.e.s.

(e) Straightforward. □

The Fitting ideal of a module has another very important property, which deserves being stated as a separate lemma. Throughout we assume that R is a commutative Noetherian ring.

Lemma 2 *Every f.g. R-Module M is annihilated by* $\mathrm{Fitt}_{0,R}(M)$.

Proof Let $x_1, \ldots, x_n$ generate M over R, and consider the R-epimorphism $\pi : R^n \to M$ that sends the i-th standard basis element e_i to x_i. Let $v_1, \ldots, v_m \in R^n$ be a list of column vectors that generates the kernel of π, and let A be the matrix whose columns are exactly these vectors. We have to show: For any n times n submatrix B of A, $\det(B)$ annihilates M. Picking such a submatrix simply amounts to picking n vectors among the v_i; without loss we may say that we picked $v_1, \ldots, v_n$. (Note that for $m < n$ there is nothing to prove.) The fact that $\pi(v_i) = 0$ can be rewritten as follows: the product "row times column" $(x_1, \ldots, x_n)v_i$ is zero. This implies $(x_1, \ldots, x_n)B = 0$. If we multiply this with the adjunct matrix B^{ad} of B on the right and recall that $BB^{ad} = det(B)I_n$, we obtain $\det(B) \cdot (x_1, \ldots, x_n) = 0$, which simply says $\det(B)M = 0$. □

Later in this article we will also have to consider *duals*. In our context this will only be applied to finite modules M and understood to be Pontryagin duality, $M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$, with the R-action given by $(r\varphi)(x) = \varphi(rx)$ for $r \in R$, $\varphi \in M^\vee$ and $x \in M$. (In representation theory another type of dual is important, the k-linear dual of finite-dimensional modules over a k-algebra.) We want to point out already here that the Fitting ideal cannot be expected to be invariant under dualization. (We will see special cases where this does hold in Sect. 4.1.) It seems worthwhile to discuss such a case.

Example We take $R = \mathbb{Z}[x, y]$ and $M = R/J$ where J is the ideal generated by x^2, xy, y^2 and a prime p. In other words, we take $\bar{R} = R/pR = \mathbb{F}_p[x, y]$ and $M = \bar{R}/\mathfrak{m}^2$ with $\mathfrak{m} = (x, y)$. Then $\mathrm{Fitt}_{0,R}(M) = J$. We consider $M^\vee$. One can check easily that $M^\vee$ has a presentation over $\bar{R}$ by two generators a and b, subject to three relations $xa = 0$, $ya = xb$, $yb = 0$. The relation matrix $\bar{A}$ for $M^\vee$ as an $\bar{R}$-module is therefore

$$\begin{pmatrix} x & y & 0 \\ 0 & -x & y \end{pmatrix}.$$

The 2-minors of $\bar{A}$ do generate the ideal $\mathfrak{m}^2$, so considered as $\bar{R}$-modules, M and $M^\vee$ have the same Fitting ideal. But this is different over the ring R. There we also have to impose relations expressing that $M^\vee$ is annihilated by p. This gives two extra relations, and we get the matrix

$$\begin{pmatrix} x & y & 0 & p & 0 \\ 0 & -x & y & 0 & p \end{pmatrix}.$$

From this one gets

$$\mathrm{Fitt}_{0,R}(M^\vee) = (x^2, xy, y^2, px, py, p^2),$$

and this ideal is properly contained (with index p) in the ideal $\mathrm{Fitt}_{0,R}(M) = (x^2, xy, y^2, p)$.

To round off this section, we introduce higher Fitting ideals. They will appear on stage later, but not too prominently.

Fix a nonnegative integer d. The d-th Fitting ideal of an R-module M is defined by slightly twisting the previous definition. Take as before a presentation $R^m \to R^n \to M \to 0$, the map $R^m \to R^n$ given by $A \in R^{n\times m}$. Then the *d-th higher Fitting ideal* $\mathrm{Fitt}_{d,R}(M)$ is the ideal generated by the $(n-d)$-minors of A. (For $d = 0$ we get what we had before, of course.) It should be said for clarity that a 0-minor, i.e. the determinant of the empty matrix, is 1, by convention.

Example We take $R = \mathbb{Z}$, p any prime, and $M = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}$. We already mentioned how one gets a presentation of a finite $\mathbb{Z}$-module; here we have $n = m = 2$ and the matrix is $A = \begin{pmatrix} p & 0 \\ 0 & p^2 \end{pmatrix}$. It only has one 2-minor, and this gives $\mathrm{Fitt}_{0,R}(M) = p^3\mathbb{Z}$. It has four 1-minors, basically given by the four entries. This gives $\mathrm{Fitt}_{1,R}(M) = p\mathbb{Z}$. For $d \geq 2$ one finds $\mathrm{Fitt}_{d,R}(M) = \mathbb{Z}$. Note that $\mathrm{Fitt}_{0,R}(M)$ is strictly contained in $\mathrm{Fitt}_{1,R}(M)$ and the latter is not the unit ideal.

As a pretty exercise, the reader might like to check that for any f.g. R-module M, we have

$$\mathrm{Fitt}_{1,R}(R \oplus M) = \mathrm{Fitt}_{0,R}(M);$$

and have fun finding some generalizations of this.

We quickly summarize some properties of higher Fitting ideals, omitting all proofs.

Lemma 3 (a) *For any f.g. R-module M, we have an increasing chain*

$$\mathrm{Fitt}_{0,R}(M) \subset \mathrm{Fitt}_{1,R}(M) \subset \mathrm{Fitt}_{2,R}(M) \subset \ldots,$$

and if M can be generated by n elements, then $\mathrm{Fitt}_{d,R}(M)$ is the unit ideal for all $d \geq n$.

(b) *Higher Fitting ideals commute with base change, just as in case $d = 0$.*

(c) *If $R = \mathbb{Z}$ (or more generally R is a Dedekind ring), then the isomorphism class of a f.g. torsion module M over R is completely determined by the collection of its Fitting ideals. In particular M is zero iff its zeroth (=initial) Fitting ideal is the unit ideal, and M is cyclic iff its first Fitting ideal is the unit ideal.*

3 Stickelberger's Theorem and L-Functions

Our goal is to understand Fitting ideals of class groups and other objects in algebraic number theory. Determining the (initial) Fitting ideal of such an object is a canonical but potentially hard way of obtaining annihilators. But apparently the story began long before the advent of Fitting ideals, with a remarkable annihilation result. Let us describe this (we need to quickly review some basics of cyclotomic theory), and then try to link it up with our main drift.

While we are interested in general number fields, so-called cyclotomic fields have always played a distinguished role. For any natural number n let ζ_n be a primitive n-th root of unity, taken in $\mathbb{C}$ if one likes. So one choice would be $\zeta_n = \exp(2\pi i/n)$. We study the number fields $\mathbb{Q}(\zeta_n)$, the so-called full cyclotomic fields, and their subfields; we assume that the reader has some acquaintance with basic Galois theory.

The key fact in this context is the following: $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ with abelian Galois group. More concretely, for every a coprime to n, there is an automorphism σ_a of $\mathbb{Q}(\zeta_n)$ characterized by $\sigma_a(\zeta_n) = \zeta_n^a$. Indeed σ_a only depends on the residue class of a modulo n. Even more precisely, the map

$$(\mathbb{Z}/n\mathbb{Z})^* \ni [a] \mapsto \sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

is an isomorphism of groups, and no element in $\mathbb{Q}(\zeta_n) \setminus \mathbb{Q}$ is fixed by every σ_a. This says that $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$ of degree $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, and its Galois group is abelian, isomorphic to the group of invertible elements in the ring $\mathbb{Z}/n\mathbb{Z}$.

The smallest nontrivial example is $n = 3$. As $\zeta_3 = (-1 \pm \sqrt{-3})/2$, we have $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. The non-identity automorphism $\sigma_2 = \sigma_{-1}$ inverts ζ_3; equivalently, it sends $\sqrt{-3}$ to $-\sqrt{-3}$.

The class group of $\mathbb{Q}(\zeta_p)$ (p a varying prime) was already studied in the 19th century (Kummer et al.) in the context of attempts to prove Fermat's last theorem. We assume that our readers have seen the definition of a class group, the fact that they are finite, and have a glimpse of their relevance for the (non)uniqueness of factoring in rings of algebraic integers; that problem in turn is intimately linked to Fermat's last theorem. Notation: cl_K denotes the class group of a number field K, and $h_K = |cl_K|$ denotes its class number.

Before stating Stickelberger's theorem we discuss so-called "minus parts". If we pick the particular value $a = -1$, then σ_a sends every root of unity to its inverse; but this is the same as its complex conjugate. That is, σ_a coincides with complex conjugation, which induces an automorphism of any normal field extension of $\mathbb{Q}$ inside $\mathbb{C}$, and which is commonly denoted j. The fixed field of j inside $\mathbb{Q}(\zeta_n)$ is denoted $\mathbb{Q}(\zeta_n)^+$ and coincides with the intersection $\mathbb{Q}(\zeta_n) \cap \mathbb{R}$. In fact one may show $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\cos(2\pi/n))$. Now it can be proved that $h_{\mathbb{Q}(\zeta_n)^+}$ is always a divisor of $h_{\mathbb{Q}(\zeta_n)}$. This numerical statement has an algebraic underpinning, as follows:

Lemma 4 *The natural map (induced by inclusion of fields) $cl_{\mathbb{Q}(\zeta_n)^+} \to cl_{\mathbb{Q}(\zeta_n)}$ is injective. Hence, the quotient $h_{\mathbb{Q}(\zeta_n)}/h_{\mathbb{Q}(\zeta_n)^+}$ is the order of the cokernel of this natural map, and therefore an integer.*

The quotient $h_{\mathbb{Q}(\zeta_n)}/h_{\mathbb{Q}(\zeta_n)^+}$ is written $h^-_{\mathbb{Q}(\zeta_n)}$ and called the *minus part of the class number* or simply the minus class number.

In the statement of Stickelberger's theorem, which goes back to 1890, minus parts do not occur, but in the appreciation of its strength and sharpness they will be vital. Since $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts on $cl_{\mathbb{Q}(\zeta_n)}$, the latter naturally becomes a module over the group ring $\mathbb{Z}[G]$. Since the group structure in the class group is usually seen as multiplication (not addition), it is natural to write "scalars" $\alpha \in \mathbb{Z}[G]$ as exponents, when they affect a class x, not as multipliers from the left, i.e. x^α instead of αx. (Think of the simple case where α is a natural number.) But this convention is not observed always and by everyone. We are finally ready for the statement.

Theorem 1 *Let n and $K = \mathbb{Q}(\zeta_n)$ be as above. Define the so-called Stickelberger element $\theta_n \in \mathbb{Q}[G]$ by*

$$\theta_n = \frac{1}{n} \sum_{(a,n)=1} a \cdot \sigma_a^{-1}.$$

(*The sum runs over integers a between 1 and $n-1$, coprime to n.*) *Then*:

(*a*) *For every b coprime to n, the product $(\sigma_b - b)\theta_n$ lies in $\mathbb{Z}[G]$.*

(*b*) *All these products $(\sigma_b - b)\theta_n$ annihilate the class group of K:*

$$x^{(\sigma_b - b)\theta_n} = 1, \qquad \forall x \in cl_K \quad \forall (b,n) = 1.$$

Part (b) can be stated more explicitly, and indeed this was the attacking point for the proof; for every ideal I of the ring O_K of integers in K, the "power" $I^{(\sigma_b - b)\theta_n}$ is shown to be principal.

It turns out that in the minus part, the elements $(\sigma_b - b)\theta_n$ not only *annihilate* but give a very good idea of the *size* of the class group. To this end we have to explain what the *minus part of a module* is.

For every $\mathbb{Z}[G]$-module M, we define $M^+ = \{x \in M | j \cdot x = x\}$ and $M^- = \{x \in M | j \cdot x = -x\}$. So M^+ (M^-) is the kernel of multiplication by $1 - j$, and $1 + j$ respectively. If M happens to be a module over $\mathbb{Z}[1/2][G]$ (i.e., multiplication by 2 on M is bijective), then $M = M^+ \oplus M^-$, and $M^\pm = e_\pm M$, where the idempotents $e_\pm$ are defined as $(1 \pm j)/2$.

Let $J \subset \mathbb{Z}[G]$ be the ideal generated by all the $(\sigma_b - b)\theta_n$; this is called the *Stickelberger ideal.* We can then look at $J^- \subset \mathbb{Z}[G]^-$. The following nice result is due to Iwasawa. For the proof, see [35, p. 105f].

Theorem 2 *Recall that $K = \mathbb{Q}(\zeta_n)$ and $G = \mathrm{Gal}(K/\mathbb{Q})$; assume that $n = p^m$ is a prime power. Then the two $\mathbb{Z}[G]$-modules $\mathbb{Z}[G]^-/J^-$ and cl_K^- have the same order up to a power-of-two factor. Moreover the order of the minus part cl_K^- is equal to the minus class number h_K^-.*

This gives rise to the idea that perhaps the minus part of the Fitting ideal of cl_K^- over $\mathbb{Z}[1/2][G]$ could be given by J^- (its plus part would be the unit ideal). We want to explore this, and also the link with the Analytic Class Number Formula. This formula gives a precise expression, in terms of values of Dirichlet L-functions, for the order of cl_K^-; and we will see that in many interesting cases Stickelberger's ideal coincides in the minus part with the Fitting ideal of the class group. This suggests that there should be a direct link between the Stickelberger element and Dirichlet L-functions. We will now discuss these two aspects: the Stickelberger ideal as a Fitting ideal, and the connection between the Stickelberger element, which is of an entirely algebraic nature, and L-functions, which are defined by convergent series and hence stem from complex analysis.

We recap very briefly the definition of Dirichlet characters and the attached L-functions. A *character* χ mod f is a character of the abelian group $(\mathbb{Z}/f\mathbb{Z})^*$, that is, a homomorphism from that group into $\mathbb{C}^*$. Of course the values of χ are roots of unity, of order dividing $\varphi(f)$. We say that χ has *conductor* f if χ is not induced from a character of $(\mathbb{Z}/e\mathbb{Z})^*$ for any proper divisor e of f. If n is any multiple of the conductor (if it differs from the conductor it must be specified!), we also consider χ as a map on $\mathbb{Z}$ by putting $\chi(a) = \chi([a])$ if a is coprime to n, and $\chi(a) = 0$ otherwise. The L-series attached to χ is then

$$L_{(n)}(s, \chi) = \sum_{a=1}^{\infty} \chi(a) a^{-s}, \quad \mathrm{Re}\, s > 1.$$

If the conductor of χ is n, one writes $L(s, \chi)$ instead of $L_{(n)}(s, \chi)$. For the trivial character $\chi = 1$ (which has $f = 1$), this reproduces Riemann's zeta function. For nontrivial χ, this function has a holomorphic continuation to all of $\mathbb{C}$. Our general policy is not to give proofs of any statements of this analytic type.

The miracle is now that the values of these functions at $s = 0$, which can only be attained by analytic continuation, are algebraic numbers. Note as a little contrast that $\zeta(2) = \pi^2/6$ is transcendental. And better still, these algebraic numbers are closely linked to θ_n, where again $n > 1$ is an arbitrary natural number. We call a character χ *odd* if $\chi(-1) = -1$, and *even* if $\chi(-1) = +1$; these are the only possibilities. Every character χ of $(\mathbb{Z}/n\mathbb{Z})^*$ (not necessarily of conductor n) gives a character (again denoted χ) of the group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the isomorphism $(\mathbb{Z}/n\mathbb{Z})^* \to G$ explained above. Odd characters are characterized by $\chi(j) = -1$. We then have:

Proposition 3 *For every odd character χ of G, also considered as Dirichlet character mod n (not necessarily of conductor n), we have*

$$\chi(\theta_n) = -\frac{1}{n} \sum_{(a,n)=1} \chi^{-1}(a)\, a = L_{(n)}(0, \chi^{-1}).$$

For the case that χ (seen as a Dirichlet character) has conductor n (not less), this is [35, second display on p. 101] combined with [35, Thm. 4.2]; but it holds in general. If n is a prime power, then it makes no difference whether we take $L_{(n)}(0, \chi^{-1})$ or $L(0, \chi^{-1})$ as long as χ is nontrivial.

It is easily shown that every element α of $\mathbb{C}[G]^-$ is completely determined by the set of values $(\chi(\alpha))_\chi$ with χ ranging over the odd characters of G. As the plus part of θ_n turns out to be easily described and not too interesting, the consequence is that the Stickelberger element is essentially described by L-values at $s = 0$. Indeed, this description will generalize to more general situations while the explicit definition we gave will not.

We now go back to the algebraic side, keeping the assumption that $n = p^m$ is a prime power. To avoid expository difficulties stemming from the prime 2, we will invert 2, that is, we replace $\mathbb{Z}[G]$ with $\mathbb{Z}[1/2][G]$, and every $\mathbb{Z}[G]$-module gets tensored with $\mathbb{Z}[1/2][G]$. In different terminology: Many questions about a $\mathbb{Z}[G]$-module M can be considered locally, that is, replacing M by its p-adic completions, one prime p at a time. And the operation of inverting 2 then simply corresponds to neglecting the case $p = 2$.

We recall that every $\mathbb{Z}[1/2][G]$-module M is the direct sum of its plus part and its minus part. We put $R' = \mathbb{Z}[1/2][G]/(1 + j)$. Note that now we are factoring out by $1 + j$, not taking the kernel of multiplication by $1 + j$. But since we inverted 2, we have a natural isomorphism $R' \cong \mathbb{Z}[1/2][G]^-$, and the point is that now R' is naturally a ring and J^- is an R'-module. We recall that cl_K^- is annihilated by J^-. Let $cl'_K = R' \otimes_R cl_K = R' \otimes_R cl_K^-$. Likewise, let J' be the image of J (equivalently, of J^-) in R'.

Proposition 4 *If the R'-module cl'_K can be generated by one single element, then we have an isomorphism*

$$cl'_K \cong R'/J'.$$

In particular, the (initial) Fitting ideal of cl'_K over R' is J'.

Proof From our hypothesis we get a surjective R'-homomorphism $f : R' \to cl'_K$. By Stickelberger's annihilation result, this homomorphism factors through R'/J', giving an epimorphism $\bar{f} : R'/J' \to cl'_K$. Now the finite abelian group R'/J' equals $\mathbb{Z}[G]^-/J^-$ with the 2-part thrown away. Similarly, cl'_K equals cl_K^- with the 2-part thrown away. By Iwasawa's result, the abelian groups R'/J' and cl'_K have the same order. Therefore $\bar{f}$ is an isomorphism. □

Remarks (1) The proposition can be extended to also cover the 2-primary parts, avoiding the inversion of 2. See [33].

(2) In the same paper, Schoof showed that the cyclicity hypothesis of the theorem is satisfied if $n = p$ (a prime) and $p \leq 509$. It should be mentioned that the orders of the concerned abelian groups grow very fast with n; for instance in case $n = 491$, this order (including the correct power of 2, which is 64) has 138 decimal digits.

The obvious question is now what happens in general. It can be seen fairly easily, using the quadratic subfield of $\mathbb{Q}(\zeta_p)$, that e.g. for $p = 3299$, the module $cl'_{\mathbb{Q}(\zeta_p)}$ will *not* be cyclic over R'. To understand the general case better we will need a little more algebra.

4 More Recent Results and Techniques

In this section we expand our point of view. We introduce the notion of modules having projective dimension at most one (the best possible substitute for projective modules, which are simply too large if nonzero) and link this to group cohomology. In other words, we characterize the modules with projective dimension at most one over a group ring as being exactly those which have zero cohomology groups (cohomologically trivial modules). In a different direction, we introduce Iwasawa towers, certain infinite-dimensional extensions of number fields. This leads to very powerful new techniques. Then we explain what to do if the modules to be studied are not themselves cohomologically trivial; vaguely one seeks cohomologically trivial "approximations" which can be understood more easily. We illustrate this by two example scenarios.

4.1 Cohomological Triviality

We keep the assumption that R is commutative and Noetherian, and we recall that the (initial) Fitting ideal of a module is by definition generated by a whole slew of determinants. Let us look at situations where one single determinant suffices.

This certainly happens if M is a finite module over $R = \mathbb{Z}$; the relation matrix A can be taken to be square of size n, where n is the number of elements one needs to generate M over $\mathbb{Z}$. Indeed we saw that we can even assume A to be a diagonal matrix.

Whenever $n = m$ in a free presentation of a f.g. R-module, there is only the single minor $\det(A)$ itself which is relevant, so in that case we have

$$\mathrm{Fitt}_{0,R}(M) = R \cdot \det(A).$$

We will say that M admits a *quadratic presentation*. As just said, this works for all finite $\mathbb{Z}$-modules, and more generally it will work for all f.g. torsion modules over a P.I.D.

There is a deeper aspect to this notion. Assume $f : R^n \to R^n$ is left multiplication with the square matrix A, and $\det(A)$ is a nonzero divisor in R. This gives a quadratic presentation of the module $M = \mathrm{coker}(f)$: Of course we have $R^n \to R^n \to M \to 0$, and moreover f is injective (use the adjunct matrix of A and the fact that multiplication by $\det(A)$ is injective on R). This exhibits M as the quotient F/U of the free module $F = R^n$ by the free submodule $U = im(f) \cong R^n$. In other words, the sequence is a short exact sequence

$$0 \to R^n \to R^n \to M \to 0.$$

In the parlance of homological algebra, one says in this case that $pd_R(M) \leq 1$ (read: the projective dimension of M over R is at most one). We will not go into the general setup of projective dimension, to save space. Let us just mention that M has $pd \leq 1$ iff for any epimorphism $g : P \to M$ with P projective over R, the kernel $U = \ker(g)$ is also projective. It is a neat fact (not obvious but a special case of Schanuel's lemma) that it suffices to test this on one single such g, which one may

choose at will. We have already mentioned torsion modules over Dedekind rings. Quite generally, an R-module is called *torsion* if it is annihilated by some nonzero divisor in R. One then has the following result (recall that a ring R is semilocal iff it has only finitely many maximal ideals):

Proposition 5 *Let M be any f.g. torsion R-module.*

(a) If $pd_R(M) \leq 1$, then the ideal $\mathrm{Fitt}_{0,R}(M)$ is locally free. In particular if moreover R is semilocal, then $\mathrm{Fitt}_{0,R}(M)$ is free cyclic over R.

(b) The converse of the first sentence in (a) also holds.

Part (a) is well-known. The proof of both parts can be extracted, using some localization arguments, from the proof of Prop. 4 in [7].

The preceding proposition is useful, but one needs a little more. We first note that if R is Dedekind, then the equivalent conditions of the proposition hold for every f.g. module M. If now $R = \mathcal{O}[G]$ where $\mathcal{O}$ is any Dedekind ring and G any finite abelian group, then there is another equivalence, involving group cohomology. We cannot define this here; let us just say that for any finite abelian group G and any G-module M, one has cohomology groups $\mathrm{H}^q(G, M)$ for all $q \in \mathbb{N}$. Here $\mathrm{H}^0(G, M) = M^G$, the submodule of G-fixed elements. We also need Tate's modification: $\hat{\mathrm{H}}^q(G, M) = \mathrm{H}^q(G, M)$ if $q > 0$, and $\hat{\mathrm{H}}^0(G, M) = M^G/N_G M$, where $N_G = \sum_{g \in G} g$ is the norm element. We then have (for the proof we refer to Prop. 4 in [7] again):

Proposition 6 *Let M be any f.g. torsion R-module, with $R = \mathcal{O}[G]$ as just described. Then $pd_R(M) \leq 1$ if and only if $\hat{\mathrm{H}}^q(U, M) = 0$ for all $q \geq 0$ and all subgroups $U \subset G$.*

The latter vanishing property is also expressed by saying that M is *cohomologically trivial* over G (c.t./G for short). The proposition also remains true for the ring $R' = \mathbb{Z}[1/2][G]/(1 + j)$ considered above: finite R'-modules have $pd \leq 1$ iff they are cohomologically trivial over G.

Typical examples for $\mathcal{O}$ would be $\mathcal{O} = \mathbb{Z}$ or $\mathcal{O} = \mathbb{Z}_p$ (the ring of p-adic integers). Since class groups are finite, they can never be free, or even projective, over $\mathcal{O}[G]$ unless they are zero. The notion of cohomological triviality is the best possible substitute for projectivity. The idea is that c.t./G-modules are much easier to deal with than general ones. This is substantiated by the fact that for finite such modules one can indeed show that the Fitting ideal is invariant under taking duals. Even more importantly, there is the following result, due to Schoof [33]. (There is a sharper version that also captures the 2-part.)

Theorem 7 *Let p^m be a prime power, $K = \mathbb{Q}(\zeta_{p^m})$, $G = \mathrm{Gal}(K/\mathbb{Q})$, and $R' = \mathbb{Z}[1/2][G]/(1 + j)$. Then the module cl'_K is c.t./G; equivalently, it satisfies $pd_{R'}(cl'_K) \leq 1$. In particular, $\mathrm{Fitt}_{0,R'}(cl'_K)$ is a locally free ideal.*

One can actually determine the Fitting ideal. Recall that J' is the image of the Stickelberger ideal in R'. The next theorem comes from [11]. The cohomological triviality of the class group is a crucial point in its proof; we will come back to this.

Theorem 8 *Let p^m be a prime power, K, G and R' as in the last theorem. Then*

$$\mathrm{Fitt}_{0,R'}(cl'_K) = J'.$$

This result generalizes the proposition stated at the end of the last section; we have eliminated the cyclicity hypothesis on cl'_K. The theorem also tells us that J' is locally free over R'. This is not obvious from the definition, which involved many terms $\sigma_b - b$, but the local freeness may be checked directly.

Let us give a numerical example: $n = p = 23$. Then $G \cong (\mathbb{Z}/23\mathbb{Z})^*$ is the direct product of the subgroup S of squares (generated by σ_2) and the subgroup $\{id, j\}$. When we project θ_{23} to $R = \mathbb{Z}[1/2][G]/(1+j)$, then $\sigma_{23-a} = j \cdot \sigma_a$ goes to $-\sigma_a$. Moreover R is canonically isomorphic to $\mathbb{Z}[1/2][S]$. Hence we get, denoting σ_2 by τ, and denoting the smallest nonnegative residue of any $z \in \mathbb{Z}$ modulo 23 by $\{z\}_{23}$:

$$\theta_{23} = \frac{1}{23}\sum_{i=0}^{10}(2 \cdot \{2^i\}_{23} - 23)\tau^{-i} \in \mathbb{Q}[S].$$

We claim that J' has index 3 in the ring R'. This can be checked quite comfortably with the help of PARI. We first note that $\theta_{23} \in \mathbb{Q}[S]$ is integral locally at all p except $p = 23$. Looking at the determinant of multiplication by $23 \cdot \theta_{23}$ in $\mathbb{Z}[S]$ (this can be done by the norm function in PARI), we see that θ_{23} is a unit at all $p \neq 3, 23$ and generates an ideal of index 3 at $p = 3$. One finally checks that at $p = 23$, J' is the unit ideal. Since the 3-adic completion of R' is a product of discrete valuation rings, these calculations imply that any R'-module having Fitting ideal J' must be isomorphic to R'/J'. When we check this against a table of class numbers, we must remember that we have neglected the 2-part, but indeed $h_{\mathbb{Q}(\zeta_{23})} = h^-_{\mathbb{Q}(\zeta_{23})} = 3$.

It is time now to extend the scope again. We will consider certain field extensions which are infinite-dimensional.

4.2 Iwasawa Theory

The theory we are now going to sketch was not primarily invented to serve as a tool for determining the structure of individual class groups, but it is very useful. We try to indicate why, postponing the details. In order to apply the powerful methods of linear algebra and representation theory one prefers to work over a base field or at least a semisimple algebra over a field. But class groups are finite $\mathbb{Z}$-modules, so if we base-change them from $\mathbb{Z}$ to $\mathbb{Q}$, they become zero. Iwasawa theory now brings larger modules over larger rings into play, and there we get a chance of replacing $\mathbb{Z}$ by its quotient field $\mathbb{Q}$ (more precisely $\mathbb{Z}_p$ by $\mathbb{Q}_p$) without ruining everything. Let us turn to the details.

We fix a prime p, assuming $p > 2$ just for the sake of simplicity. Instead of one field K we consider a whole "tower". By Galois theory, for any $n \in \mathbb{N}$ there is exactly one subfield B_n of degree p^n inside the cyclotomic field $\mathbb{Q}(\zeta_{p^{n+1}})$. Its Galois group over $\mathbb{Q}$ is cyclic of order p^n. The infinite extension $B_\infty = \bigcup_n B_n$ is then Galois in the profinite sense; its Galois group Γ is the projective limit of the groups $\mathrm{Gal}(B_n/\mathbb{Q})$, and Γ is (even if multiplicatively written originally) algebraically and topologically isomorphic to the additive group $\mathbb{Z}_p$.

For any number field K one defines $K_\infty = KB_\infty$. This is again an ascending union of extensions K_n which are cyclic of degree p^n over K. Frequently one has $K_n = KB_n$; in general a certain shift of numbering may occur. We call K_∞/K the *cyclotomic $\mathbb{Z}_p$-extension* of K, and we again denote its profinite Galois group by Γ.

For any number field L we denote by A_L the p-primary part of cl_L. For every n, the norm map induces a group homomorphism $A_{K_{n+1}} \to A_{K_n}$. One defines the Iwasawa module X_K as the projective limit

$$X_K = \varprojlim_n A_{K_n}.$$

The Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]]$ is by definition the profinite limit of the group rings $\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$. It is well known that every choice of a pro-generator γ of Γ induces an identification ($\gamma - 1$ corresponding to T)

$$\Lambda = \mathbb{Z}_p[[T]] \quad \text{, a power series ring in one variable.}$$

One point of this construction is that the ring Λ is in many respects nicer than the group rings $\mathbb{Z}[G]$ or $\mathbb{Z}_p[G]$ that have occurred so far. It is a domain, local and regular; in particular it enjoys unique prime factorization of elements. The Iwasawa module X_K becomes naturally a module over Λ.

A key fact of the theory is that X_K is finitely generated and torsion over Λ, so loosely speaking X_K is not too large. A typical nontrivial instance of such a module over Λ might be $M = \Lambda/(T-a)$, where $a \in p\mathbb{Z}_p$ is any noninvertible p-adic integer. For instance if $a = 0$, then M is just a copy of $\mathbb{Z}_p$ with T acting as zero (equivalently, with trivial Γ-action).

Another very important circumstance is that very often it is fairly easy to "descend", that is to transform knowledge on X_K into knowledge on the individual finite groups A_{K_n}. This works best using the concept of totally real fields and CM fields, which is a straightforward generalization of what happens for cyclotomic fields.

A number field K is totally real if all of its embeddings $\varphi : K \to \mathbb{C}$ into the complex numbers have real image, that is, $\varphi(K) \subset \mathbb{R}$. For K to be CM, it is not enough that K is totally imaginary (no embedding has real image). One needs a little more: K is a totally imaginary quadratic extension of a totally real field K^+. The nontrivial automorphism of K over K^+ is then complex conjugation, which will be written j as in an earlier section. Examples abound; one may take K to be any full cyclotomic field and $K^+ = K \cap \mathbb{R}$. Also, if K is CM then so are all the layers K_n in the cyclotomic $\mathbb{Z}_p$-extension.

For all arithmetic objects attached to a CM field K, we can then take minus parts again, e.g. $A_K^- = \ker(1 + j : A_K \to A_K)$. For rings it is more natural to take cokernels and let $R^- = R/(1 + j)$. We recall that as soon as 2 is invertible, the kernel and cokernel of $1 + j$ can be canonically identified.

We now consider an additional group action. Assume L/k is an abelian extension of number fields with group G, k is totally real and L is CM. Then there is also the group ring $\Lambda[G]$ and we can (at least if $p > 2$) consider the minus part X_L^- as a module over $\Lambda[G]/(1 + j)$. We are now in a position to briefly sketch the proof of Theorem 8. This forces us to change notation. Let $n = \ell^m$ be a prime power,

$L = \mathbb{Q}(\zeta_n)$, $k = \mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. We remark that the following argument works for a much wider class of extensions, so-called nice extensions, see [11], but for expository reasons we restrict to the setting just described.

We want to prove for every $p > 2$ that the $\mathbb{Z}_p[G]^-$-Fitting ideal of A_L^- (the p-part of cl_L^-) is given by the Stickelberger ideal. This is done in two steps. First one proves an analog at infinite level, defining a Fitting ideal $J_\infty^- \subset \Lambda[G]^-$ which projects onto J^- under $\Lambda[G]^- \to \mathbb{Z}[G]^-$, $T \mapsto 0$, and showing that

$$\mathrm{Fitt}_{0,\Lambda[G]^-}(X_K^-) = J_\infty^-. \qquad (*)$$

For the second step we recall the notion of coinvariants. If a group Γ acts on a module Y, then $Y_\Gamma = Y/\langle(\gamma - 1)Y : \gamma \in \Gamma\rangle$ is the largest factor module of Y on which Γ acts trivially. In our context Y is a $\Lambda[G]$-module and $Y_\Gamma = Y/TY = \mathbb{Z}_p[G] \otimes_{\Lambda[G]} Y$. The point of the second step is to show that the natural map

$$(X_K^-)_\Gamma \to A_K^-, \quad (x_n)_{n\in\mathbb{N}} \mapsto x_0,$$

is an isomorphism. This, and the compatibility of Fitting ideals with base change gives the desired statement.

Finally let us explain in an equally terse style the main elements of the first step. We consider the statement $(*)$ tensored with $\mathbb{Q}_p$ over $\mathbb{Z}_p$. The algebra $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda[G]$ is now very nice; indeed it is a product of principal ideal rings. This makes the theory of Fitting ideals pretty simple, as we have seen. The module $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} X_K^-$ is a finite-dimensional $\mathbb{Q}_p$-vectorspace with a G-action. The so-called Main Conjecture in Iwasawa theory (one of the many aspects of the theory we have to neglect, unfortunately) gives the $\mathbb{Q}_p$-tensored version of (*) without too much effort. (Of course much effort had gone into proving the Main Conjecture previously.) The way back to the un-tensored version relies among other things on the fact (which must be proved) that X_K^- has projective dimension at most one over $\Lambda[G]^-$, which tells us beforehand that the Fitting ideal will be principal; and on the vanishing of the so-called μ-invariant. In our situation this simply means that X_K^- is finitely generated as a $\mathbb{Z}_p$-module.

Let us pause for a quick intermediary summary. We are interested in class groups as Galois modules, that is, as modules over $\mathbb{Z}[G]$ where G is a Galois group. One central aspect of this study is determining the Fitting ideal. This is closely related to (but a much more precise tool than) Stickelberger's classical annihilation theorem. The theory of Fitting ideals is fairly translucent over PIDs or products of PIDs. However the ring $\mathbb{Z}[G]$ is practically never of this kind. There are situations (prime-power cyclotomic extensions or more generally, "nice" extensions) where some of the nicer features of the Fitting ideal carry over; the important notions are those of "quadratic presentation" and "projective dimension at most one". It stands to reason, however, that this approach will never capture all cases of interest. Therefore we have to extend our scope again. The idea of using Iwasawa theory (going up to an infinite extension and then coming back) will certainly remain useful in the wider context.

4.3 Relating General Modules to c.t. Modules

Let us begin with the algebra; arithmetic context will follow as soon as possible. We saw that for instance over a group ring $R = \mathbb{Z}[G]$, it is equivalent for a finite

module M to say either $pd_R(M) \leq 1$ or $\mathrm{Fitt}_{0,R}(M)$ is rank one projective. We look at modules which do not satisfy $pd \leq 1$ and resolutions of them by modules which do satisfy $pd \leq 1$. More precisely we will look at exact 4-term sequences

$$0 \to N \to P \to Q \to M \to 0$$

of f.g. torsion modules over a fixed commutative ring R, where $pd_R(P) \leq 1$ and $pd_R(Q) \leq 1$. Take one typical example: G is cyclic of prime order p with generator σ, $R = \mathbb{Z}[G]$, $P = Q = R/pR, M = \mathbb{F}_p = R/(p, \sigma - 1)$. To construct the 4-term sequence, the map $P \to Q$ must be multiplication by $\sigma - 1$. The kernel of this map is $\mathbb{F}_p \cdot N_G$, where $N_G = 1 + \sigma + \cdots + \sigma^{p-1}$ is the norm element. Hence we must take $N = \mathbb{F}_p$ (trivial G-action), and the map $N \to P$ sends 1 to N_G. In this situation we actually have $N \cong M$; in particular the Fitting ideals of M and N agree.

Let us look at a more involved example. For G we take the direct product of two cyclic groups of order p, with generators σ and τ respectively, and $R = \mathbb{Z}[G]$. Take $M = \mathbb{F}_p$ (trivial action), $Q = \mathbb{F}_p[G]$, $P = \mathbb{F}_p[G] \oplus \mathbb{F}_p[G]$; the map $Q \to M$ is the only possible map, with kernel generated by $s := \sigma - 1$ and $t := \tau - 1$. We also need the "norm elements" $\nu_\sigma = 1 + \sigma + \cdots + \sigma^{p-1}$ and $\nu_\tau = 1 + \tau + \cdots + \tau^{p-1}$. Note that $\nu_\sigma R$ is the exact annihilator of sR and vice versa; similarly for $\nu_\tau R$ and tR. The map $f : P \to Q$ sends the first (second) basis element of P as a $\mathbb{F}_p[G]$-module to s and t respectively. For N we take the kernel of f. It has $\mathbb{F}_p$-dimension $p^2 + 1$ and is generated by the three 2-vectors

$$a = (\nu_\sigma, 0);$$
$$b = (0, \nu_\tau);$$
$$c = (t, -s).$$

We cannot expect N to be isomorphic to M because N is too large, and the relation between the Fitting ideals of M and N is far from evident.

Now duality enters into play. In the next result, we suppose for simplicity that R is a commutative reduced algebra over one of the base rings $\mathbb{Z}$, $\mathbb{Z}[1/2]$ or $\mathbb{Z}_p$, and finitely generated free over the base ring. (Standard example: $R = \mathbb{Z}[G]$ a group ring.) Then an R-module M is f.g. and torsion iff it is finite. We abbreviate $\mathrm{Fitt}_{0,R}$ to Fitt.

Proposition 9 *Let $0 \to N \to P \to Q \to M \to 0$ be an exact sequence of f.g. torsion R-modules, and assume that both P and Q have projective dimension at most 1 over R. Then we have the equality*

$$\mathrm{Fitt}(N^\vee)\,\mathrm{Fitt}(Q) = \mathrm{Fitt}(P)\,\mathrm{Fitt}(M).$$

We will not give the proof, but of course a reader may wonder just where the dual comes from. Vaguely speaking, N is the kernel and M is the cokernel of the same map; and in a way, kernel and cokernel are dual notions.

Let us look at the two examples again. In the first one, P and Q are isomorphic; N and M are isomorphic and N is self-dual, so the formula of the lemma obviously

holds. In the second example, $\mathrm{Fitt}(Q) = (p)$; $\mathrm{Fitt}(P) = (p^2)$; and $\mathrm{Fitt}(M) = (p, s, t)$. Proposition 9 tells us

$$\mathrm{Fitt}(N^\vee) = p \cdot (p, s, t).$$

It does not tell us what $\mathrm{Fitt}(N)$ is. By a direct computation one can show that $\mathrm{Fitt}(N)$ is properly smaller than $\mathrm{Fitt}(N^\vee)$. A list of generators is as follows. If J denotes the ideal generated by s and t, then

$$\mathrm{Fitt}(N) = p(J^2 + pJ + p^2R).$$

Before explaining the arithmetic relevance of this result, we also state its Iwasawa theoretic variant. Recall $\Lambda = \mathbb{Z}_p[[T]]$ (with p a fixed prime). Assume that R is a commutative reduced Λ-algebra, f.g. free as a Λ-module. (Standard example: $R = \Lambda[G]$.) One can show that every f.g. torsion R-module which has no p-torsion is finitely generated over $\mathbb{Z}_p$. We then have:

Proposition 10 *Let $0 \to N \to P \to Q \to M \to 0$ be an exact sequence, in which all modules are f.g. torsion over R but without $\mathbb{Z}_p$-torsion, and assume that both P and Q have projective dimension at most 1 over R. Then there is the equality*

$$\mathrm{Fitt}(\alpha(N))\,\mathrm{Fitt}(Q) = \mathrm{Fitt}(P)\,\mathrm{Fitt}(M),$$

where $\alpha(N)$ denotes the contravariant Iwasawa adjoint.

We cannot explain the notion of Iwasawa adjoint here; it is again a kind of dual. Proposition 9 is [7, Prop. 6]; this was reproved (with a slight necessary amendment) in [3, Lemma 5]. Proposition 10 is [12, Prop. 1].

We now try to explain in a grossly over-simplified way how these two propositions are used in order to determine the Fitting ideals of objects like class groups or projective limits of such (Iwasawa modules). The general pattern for a useful sequence $0 \to N \to P \to Q \to M \to 0$ is:

- Either N or M is the module whose Fitting ideal we want to determine.
- The other "outside" module (M, or N) does not have too good algebraic properties, but it should be "explicit" in some sense.
- The modules P and Q have projective dimension at most 1, and we should be able to determine their Fitting ideals.

In the next subsection we will present two example scenarios, skipping all proofs. Subsequently we will try to explain the underlying principle that allows to obtain such 4-term sequences in a systematic way.

4.4 Example Scenarios

First Scenario [7] Here the goal was to describe the $\mathbb{Z}[G]$-Fitting ideal of cl_K, where K is any subfield of the totally real field $\mathbb{Q}(\zeta_{\ell^n})^+$, with ℓ^n an arbitrary prime power and $G = \mathrm{Gal}(K/\mathbb{Q})$. The description is "relative" in the sense that it involves another

algebraically defined module, and no quantities of analytical origin. Let us state the result as clearly as possible without giving too much detail.

The analysis goes "prime by prime", so all modules are completed at a prime p, which in the end varies over all primes. The p-part of a finite module B will be written $B\{p\}$ consistently. We take $R = \mathbb{Z}_p[G]$ and $M = A_K$, which was defined before by $A_K = cl_K\{p\}$. To construct N and P, we need the so-called group of cyclotomic units Cyc_K and the so-called group of semilocal units at p: $\mathcal{U}_p = \prod_{v|p} \mathcal{O}_{K_v}^*$. We put

$$N = (\mathcal{O}_K^*/\mathrm{Cyc}_K)\{p\}; \quad P = (\mathcal{U}_p/\mathrm{Cyc}_K)\{p\}.$$

Finally, let Y_p denote the Galois group of the maximal abelian p-ramified p-extension M/K. Global class field theory then gives the desired sequence

$$0 \to N \to P \to Y_p \to M = cl_K\{p\} \to 0.$$

One can show that P and Y_p have pd ≤ 1 over R. Thus their Fitting ideals are principal. The crucial fact is now that one can prove that they are equal. We simplify the notation $\mathrm{Fitt}_{0,R}$ to Fitt_R. Then Proposition 9 gives the simple result

$$\mathrm{Fitt}_R(N^\vee) = \mathrm{Fitt}_R(M).$$

As a finishing touch, one then shows that $\mathrm{Fitt}_R(N^\vee) = \mathrm{Fitt}_R(N)$. This is nontrivial and uses that G is cyclic; see Prop. 1 in the appendix of [27].

For real abelian fields K whose conductor is not a prime power, it is sometimes possible to find an explicit enlargement $\bar{C}_K$ of the group Cyc_K. Then there is a relation between the Fitting ideal of the quotient $\mathcal{O}_K^*/\bar{C}_K$ and the Fitting ideal of *a subgroup of* $cl_K\{p\}$. See [14, p. 179] and follow-up work by the same authors.

Second Scenario [12, 17] We adapt and simplify some notation from these papers for the present purpose.

Let K/k be a G-abelian extension of totally real number fields, and let S be a set of places of k which includes all places that ramify in K. We fix a prime p and consider the p-cyclotomic extension K_∞. With this comes an Iwasawa module X_S, the Galois group of the maximal S-ramified p-abelian extension M/K_∞. (This is a projective limit of so-called ray class groups.) We assume k_∞ to be linear disjoint from K, so the Galois group of $K_\infty = Kk_\infty/k$ is $\Gamma \times G$. We put $R = \Lambda[G] = \mathbb{Z}_p[[\Gamma \times G]]$.

One now needs a fairly restrictive new hypothesis, forced on us by the ascent to the p-cyclotomic power: we must assume that S contains all the places above p. Then the theory of canonical classes (for details see [11] p. 739f. and the references given there) produces a 4-term sequence of f.g. R-modules

$$0 \to X_S \to \bar{Y}_S \to R \to \mathbb{Z}_p \to 0.$$

The term $\mathbb{Z}_p$ has trivial action by G and T acts as zero, so it is as simple and explicit as one could wish. The term R has projective dimension zero, and is again gratifyingly simple; one also has $pd_R(\bar{Y}_S) \leq 1$. But we have overshot the goal since R is not torsion, and hence neither is $\bar{Y}_S$. A repair job is needed to trim the two middle modules down, but this is fairly simple. One takes any free cyclic submodule $fR \subset R$

in the kernel of the map $R \to \mathbb{Z}_p$, which is simply the augmentation map; one lifts f back to $\bar{f} \in \bar{Y}_S$; and one lets $P = \bar{Y}_S/\bar{f}R$, $Q = R/fR$. This does give the desired sequence

$$0 \to X_S \to P \to Q \to \mathbb{Z}_p \to 0,$$

with the only little wrinkle that f is far from unique; but this is not a problem in the end.

In [12] this was used to determine the Fitting ideal of the Iwasawa adjoint $\alpha(X_S)$ over the ring $R = \Lambda[G]$. We have

$$\mathrm{Fitt}_R(\alpha(X_S)) = \mathrm{Fitt}_R(\mathbb{Z}_p) \cdot \Phi_S \cdot R,$$

where Φ_S generates the principal ideal $\mathrm{Fitt}_R(P)\,\mathrm{Fitt}_R(Q)^{-1}$, and is again defined in terms of generalized Stickelberger elements. Here are the details. Pick a CM extension L abelian over k with $K = L^+$. For every n, define $\theta_{L_n/k}$ by the property

$$\chi(\theta_{L_n/k}) = L_S(0, \chi^{-1})$$

for all characters χ of $\mathrm{Gal}(L_n/k)$. (We skip the general definition of L-series attached to characters; it is a generalization of the construction given in Sect. 3.) One can show that the projective limit of these $\theta_{L_n/k}$ defines an element Θ in the full quotient ring of $\Lambda[\mathrm{Gal}(L/k)]$; we take the minus part of this, and by a so-called Tate twist that exchanges "minus" and "plus", Θ turns into $\Phi \in Quot(R)$.

This result is still not what one would like in general, in two respects. Firstly, one really wants the Fitting ideal of the Iwasawa module X_{S_p}, with S_p denoting the set of places above p on k, instead of X_S, in the (frequent) cases where some non-p-adic places ramify in K/k. The module X_{S_p} is the more canonical object, because it is related by duality to the minus part of $X_\emptyset(L)$, if L is a CM field, abelian over k, with $K = L^+$; and the module $X_\emptyset(L)$ is the most natural and most studied Iwasawa module.

The switch from X_S to X_{S_p} may be achieved by a major cheat, as follows. One multiplies all modules by a certain idempotent $e \in \mathbb{Z}_p[G]$. (To be precise, this eliminates the χ_0-component where χ_0 is the trivial character of the non-p-part of G. Therefore one loses everything if G is a p-group!) The effect is that $e\mathbb{Z}_p$ vanishes, eX_S has projective dimension ≤ 1 over eR, and one can find another 4-term sequence of the desired kind:

$$0 \to Z \to V \to eX_S \to eX_{S_p} \to 0,$$

where both V and X_S have projective dimension at most 1 over eR, both Z and V are quite well known, and the Fitting ideal of Z agrees with that of $\alpha(Z)$, so one may continue; but we repeat that the results obtained this way are completely void if G is a p-group.

Secondly, one would like to know the Fitting ideal of X_S itself, not its Iwasawa adjoint (which, we recall, is a kind of dual). A naive example we gave above, showing what may happen to Fitting ideals when taking duals of modules over the group ring

$\mathbb{Z}[G]$ of a bicyclic group, suggests that X_S might have a more complicated Fitting ideal than $\alpha(X_S)$.

The second issue is treated in [17] completed by [19]; the issue of eliminating the major cheat is dealt with in [20]. We will discuss all this briefly in the final section.

5 Further Developments

In this final section we try to highlight some important and more-or-less recent results. Since we try to cover diverse directions, the reader should not expect a clear-cut storyline. The crowning glory will be the discussion of a very recent breakthrough concerning Brumer's conjecture.

5.1 Field Extensions of Non-prime Power Conductor

So far we have seen two main methods. Either one shows that the module in question is amenable in a precise algebraic sense (cohomologically trivial) and makes the most of this, or if the module is less amenable one tries to link it up to other modules which are somehow easier to treat.

We will now discuss a third approach, mainly due to Kurihara. For this we remain in the cyclotomic scenario but we allow more general fields, allowing K to be any imaginary abelian extension of $\mathbb{Q}$. By the theorem of Kronecker-Weber, it is equivalent to say that K is contained in *some* cyclotomic field $\mathbb{Q}(\zeta_n)$; the minimal such n is called the conductor of the field K. Let $G = \mathrm{Gal}(K/\mathbb{Q})$.

When the conductor is composite, having at least 3 different prime factors say, then there is an obstacle that prevents a simple result. The analog J^- of the Stickelberger ideal has infinite index in $\mathbb{Z}[G]$, and therefore it cannot be the Fitting ideal of the finite module cl_K^-. A way out of this impasse was found by Sinnott [34], who gave the correct general definition of the Stickelberger ideal in the cyclotomic situation. In general, it requires quite a lot of generators (exponential in the number of primes dividing the conductor), and it is a challenge to fully understand its $\mathbb{Z}[G]$-structure. The relations between the generators are given by so-called Euler relations, generalizations of which have played a very prominent role in the last decades.

In a remarkable paper [23], Kurihara managed to prove under fairly mild assumptions on K that after inverting 2 (just as in earlier sections of this survey), the initial Fitting ideal of cl_K^- is again given by the Stickelberger ideal, whose definition is however, in general, not exactly the same as Sinnott's. Here are some details on this.

(1) If K is the direct compositum of all its inertia subfields (this happens always if $K = \mathbb{Q}(\zeta_n)$ is a full cyclotomic field), then Kurihara's construction agrees with Sinnott's.

(2) Concerning the "mild assumptions", it suffices for example that $K/\mathbb{Q}$ is only tamely ramified; but many wild (= non-tame) fields K are also covered.

(3) The approach is local, considering the completions at each prime $p > 2$, and proceeds by going up to an Iwasawa-theoretic situation, that is, passing to projective limits in a cyclotomic $\mathbb{Z}_p$-extension. Of course one then has to descend again, and this is a nontrivial task.

(4) Kurihara's approach completely avoids cohomologically trivial modules. He bites the bullet and works directly with modules which (presumably) have very complicated cohomology. A main technical tool is an ingenious comparison lemma for two ideals of $\mathbb{Z}[G]$. Actually this involves whole families of ideals, attached to various subfields of K, and compatibilities between them. The comparison lemma works at infinite level, before descent.

There is no reason to expect that the annihilator of the minus class group equals the Fitting ideal. Indeed there is a systematic way of finding annihilators outside the Stickelberger ideal for special classes of abelian imaginary extensions of $\mathbb{Q}$, see [15].

5.2 On Higher Fitting Ideals in a Simple Case

It was mentioned that over a PID (or Dedekind ring) R, any f.g. torsion module M is determined by the sequence of its (higher) Fitting ideals. This can be made more precise. Abbreviating $\mathrm{Fitt}_{i,R}$ to F_i for a moment, one has

$$M \cong \bigoplus_{i \geq 0} F_{i+1}(M)/F_i(M).$$

Of course this direct sum is only formally infinite, since for $i \gg 0$, $F_i(M)$ stabilizes at $F_i(M) = R$. In [24] a result on the higher Fitting ideals of cl_K is proved for general abelian CM-extensions K of totally real fields k with group G, generalizing work of Kolyvagin and Rubin. The statement is a little involved. It is again local, and supposes for the p-local version that $[K : k]$ is prime to p. Then the group ring $\mathbb{Z}_p[G]$ is a direct product of DVRs. Under some more hypotheses which we do not make explicit (see Theorem 0.1 in loc. cit.; note that the indices of the two Θ terms should be exchanged), the higher Fitting ideals $\mathrm{Fitt}_{i,\mathbb{Z}_p[G]}(cl_K^-)$ are determined in terms of higher Stickelberger ideals.

We will not go into the definition of higher Stickelberger ideals; they arise via a certain derivation process (Kolyvagin systems) from the "usual" Stickelberger ideals. But it is important to realize that these latter ideals only have a quick and explicit definition in the cyclotomic setting. Kurihara's neat idea is to take the existing link from L-values to Stickelberger elements in the cyclotomic case, and to turn it around in the general situation, making it into a *definition* of Stickelberger elements in greater generality.

This research has been taken further in two directions. Kurihara strengthened his results (relaxing the rather sharp condition that p may not divide the degree of the field extension) in [25], and Ohshita [32] proved analogous results on the plus side, that is, for the case that K is totally real and abelian over $\mathbb{Q}$.

5.3 About 4-Sequences and Cohomology

We have seen a few 4-sequences and their applications, but we have not seen a conceptual way to obtain them. It seems worthwhile and useful to provide some information in this direction as well. Unfortunately the prerequisites for a complete and systematic discussion are so complex that we will have to cut quite a few corners.

Let us begin by outlining the basic idea concerning complexes. Assume that we have a complex $C^\bullet$ of R-modules with two properties: it has nonzero cohomology only in two successive dimensions i and $i+1$, and it is "perfect". Perfectness is a technical condition, saying that in the derived category $C^\bullet$ is isomorphic to a bounded complex all of whose terms are f.g. projective over R. The miracle is that the complexes occurring from cohomology, hard of access as they look, are all perfect in practice. One can show that any such complex leads to a 4-term exact sequence $0 \to N \to P \to Q \to M \to 0$, where N and M are the ith (and $i+1$st respectively) cohomology of $C^\bullet$, and P, Q have projective dimension at most 1. One can say more: the class of this 4-sequence in $\mathrm{Ext}^2_R(M,N)$ determines the isomorphism class of the complex in the derived category.

After these preliminaries we will now sketch in which way the 4-term-sequence of the second scenario (see above) stems from étale cohomology. (Only after this will we turn to the 4-term sequence of the first scenario, since there things are even less plain.) Let us quickly review this sequence. One takes a G-abelian extension K/k of totally real fields and a finite set of places S containing all primes that ramify in K_∞/k. Then the leftmost term of the 4-sequence is X_S, the Galois group of the maximal p-abelian S-ramified extension M/K_∞, and the rightmost term is simply $\mathbb{Z}_p$. Note that all this happens at infinite level, at the top of the cyclotomic tower.

Let us now consider any abelian G-Galois extension K/k, with ramifying set S, and the étale site over $\mathcal{O}_{K,S}$, the set of S-integers in K (elements of K that can be written with a denominator coprime to all primes in S). Let $R = \mathbb{Z}[G]$. Sheafs $\mathcal{F}$ in that topology lead to complexes (rather: objects in the derived category of R-modules), whose cohomology is the étale cohomology $\mathrm{H}^\bullet(\mathcal{O}_S, \mathcal{F})$. We explain how a version of the second 4-term sequence at level K can be obtained. It would be beautiful if we could simply take $\mathcal{F} = \mathbb{G}_m$ (the "multiplicative group"). While this is the correct start, modifications are necessary. For the rather difficult details we refer to [2], in particular p. 1376. First, one has to replace "étale cohomology" by "compactly supported étale cohomology". This produces the right object in degree 1:

$$\mathrm{H}^1_c(\mathcal{O}_{K,S}, \mathbb{G}_m) = C_K(S),$$

where $C_K(S)$ is the exact analog of X_S at finite level, namely the Galois group of the maximal abelian S-ramified p-extension $M_S(K)/K$. But degree 2 and 3 still make trouble, as $\mathrm{H}^2_c(\mathcal{O}_{K,S}, \mathbb{G}_m) = 0$ and $\mathrm{H}^3_c(\mathcal{O}_{K,S}, \mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}$. So this does not lead to a 4-sequence as above but to a 5-sequence with rightmost term $\mathbb{Q}/\mathbb{Z}$; that is, an element of $\mathrm{Ext}^3(\mathbb{Q}/\mathbb{Z}, C_K(S))$. Using the tautological sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$, this can be changed into an element of $\mathrm{Ext}^2(\mathbb{Z}, C_K(S))$, which gives the analog of the desired 4-sequence at finite level. The 4-sequence we are actually interested in, the one starting with X_S and living at infinite level, is then attained, very roughly speaking, by passing to the projective limit.

The author is not aware of a direct construction of the 4-term sequence for the first scenario (the one for real abelian fields) by these principles, but there is a recent development that comes close and opens up new horizons, the work [5] of Burns, Kurihara, and Sano. The relevant sequence ran as follows:

$$0 \to \mathcal{O}_K^*/\mathrm{Cyc}_K\{p\} \to \mathcal{U}_p/\mathrm{Cyc}_K\{p\} \to Y_p \to cl_K\{p\} \to 0,$$

where Y_p denotes the Galois group of the maximal abelian p-ramified p-extension $M_p(K)/K$.

To approach this sequence, one would like to use the sheaf $\mathbb{G}_m$ again. Perhaps some readers will remember from geometry that the Zariski cohomology $\mathrm{H}^1(X, \mathbb{G}_m)$ is isomorphic to the Picard group of the variety X, and class groups are Picard groups. The zeroth cohomology (whatever version) of $\mathbb{G}_m$ is easily determined, e.g. $\mathrm{H}^0(\mathcal{O}_{K,S}, \mathbb{G}_m) = \mathcal{O}_{K,S}^*$. But the second cohomology is not zero as one would like, so something must be changed. We report on the paper [5].

We again consider a G-Galois extension K/k of number fields, G abelian, and we fix a set S of places of K containing the archimedean primes and those ramified in K. We define $Y_{K,S}$ to be the free $\mathbb{Z}$-module with basis $S(K)$ (the set of places of K lying over places in S) and $\Xi_{K,S} \subset Y_{K,S}$ the kernel of augmentation, i.e. the map to $\mathbb{Z}$ sending each basis element to 1. (Let us remark that many authors use $X_{K,S}$ instead of $\Xi_{K,S}$, but we have already used X_S for something entirely different.) We now need an auxiliary finite set T of places of k, disjoint with S, and the subring $\mathcal{O}_{K,S,T}$ of $\mathcal{O}_{K,S}$ formed by all elements which are congruent to 1 at all places in K over T. Then after several modifications and embellishments (étale to compactly supported étale to compactly supported Weil-étale to T-modified compactly supported Weil-étale; no explanations are possible here), one finds

$$\mathrm{H}^0_{c,T}((\mathcal{O}_{K,S,T})_{\mathcal{W}}, \mathbb{G}_m) = \mathcal{O}^*_{K,S,T},$$

and one defines $\mathcal{S}^{tr}(K, S, T)$ as $\mathrm{H}^1_{c,T}((\mathcal{O}_{K,S,T})_{\mathcal{W}}, \mathbb{G}_m)$. Under mild assumptions, these are the only non-vanishing cohomology groups, and the underlying complex is perfect.

We cannot go into details, but let us at least explain the hypothesis one needs to make on T (in particular it cannot be taken empty). We need that the unit group $\mathcal{O}^*_{K,S,T}$ is torsion free; in other words, the main role of T is eliminating roots of unity. Such auxiliary sets T always exist and are easily controlled. The T-modified group $cl_{K,S,T}$ is a sort of ray class group, and it surjects onto $cl_{K,S}$.

This gives a handle on the module $\mathcal{S}^{tr}(K, S, T)$. This module turns out to be an extension of the desired object $cl_{K,S,T}$ by the explicit module $\Xi_{K,S}$, unaffected by T:

$$0 \to cl_{K,S,T} \to \mathcal{S}^{tr}(K, S, T) \to \Xi_{K,S} \to 0. \qquad (**)$$

While this may look complicated, it is in a sense a natural analog to Selmer groups attached to elliptic curves. These Selmer groups, very roughly speaking, are also "hybrids", one part coming from points on the curve and the other part coming from the famous Sha group, which is an analog of the class group.

We cannot formulate the deep results of [5], which give results on Fitting ideals (including higher ones) of the "hybrid" object $\mathcal{S}^{tr}(K, S, T)$, also involving analogs of cyclotomic units (Rubin-Stark elements) which are still conjectural in general. We prefer just to illustrate one of the results, Theorem 1.5 (ii) for $r = 1$ (the important parameter r is defined in loc. cit.), by one fairly simple example based and elaborating on Remark 1.13 in loc. cit. Indeed, let us go back to $K = \mathbb{Q}(\zeta_{p^m})^+$, $G = \mathrm{Gal}(K/\mathbb{Q})$,

the setting of [7]. Then $\varepsilon = 1 - \zeta_{p^m}$ is a $\mathbb{Z}[G]$-generator of the cyclotomic p-units of K mod torsion, and the theorem (plus a little algebra) yields with $S = \{\infty, p\}$:

$$\begin{aligned}\mathrm{Fitt}_{1,\mathbb{Z}[G]}(\mathcal{S}^{tr}(K,S)) &= \{\varphi(\varepsilon) : \varphi \in \mathrm{Hom}(\mathcal{O}_K[1/p]^*, \mathbb{Z}[G])\} \\ &= \mathrm{Fitt}_{0,G}(\mathcal{O}_K^*/\mathrm{Cyc}_K).\end{aligned}$$

In this case it is easy to get back to the class group, since $\Xi_{K,S}$ happens to be free of rank one over $\mathbb{Z}[G]$ (a generator being $v - \mathfrak{p}$ where v is any of the infinite places of K and $\mathfrak{p}$ the unique place above p in K); this "obvious" fact is not even mentioned in loc. cit. Then the exact sequence $(**)$ splits, and by the "pretty exercise" near the end of Sect. 2, $\mathrm{Fitt}_{1,\mathbb{Z}[G]}(\mathcal{S}^{tr}(K,S))$ coincides with $\mathrm{Fitt}_{0,\mathbb{Z}[G]}(cl_{K,S})$. As a final touch one has to check that in the present case $cl_{K,S}$ happens to agree with cl_K.

This discussion of a very special case already indicates that in general it is not obvious how to extract information on $cl_{K,S}$ from Theorem 1.5(ii) in loc. cit.

A situation similar to this arose in work [17], completed in [19], of Kurihara, Tokio (the name has nothing to do with the city Tokyo) and the author. We considered an abelian extension K/k of totally real fields with group G and the Iwasawa module X_S discussed before, which is the Galois group of the maximal abelian S-ramified p-extension of K_∞. In terms of class field theory, this is a projective limit not of class groups but of ray class groups; in the totally real case it is the right object to study, except for the fact that the set of places needs to contain not only the p-adic places (forced by Iwasawa theory) but all places ramified in K/k. In [17] the technique of exact 4-sequences is used to determine the Fitting ideal of X_S over the appropriate Iwasawa algebra $\Lambda[G]$ in general, avoiding the "cheat" discussed at the end of Sect. 4.4.

We try to explain the result of [17] in a nontrivial example, G being elementary abelian of order p^2. Its main advantage over [12] is that it avoids taking the Iwasawa dual $\alpha(X_S)$ and addresses X_S itself. We fix the setup as above. In the discussion of [12] we sketched the construction of a "Stickelberger element at infinite level, on the plus side", which was denoted Φ_S. Unfortunately it is denoted Θ in [17].

Prior experience leads to the idea that $\mathrm{Fitt}_{\Lambda[G]}(X_S)$ should be, roughly speaking, "generated by $\Phi_S = \Theta$ at all nontrivial characters χ of G, and generated by $T \cdot \Theta$ at the trivial character of G" (whatever that means). In fact Θ itself need not be integral (this might ring a bell, since already the cyclotomic θ_n is almost never integral); but the factor T makes it integral, and so do various other factors. Pick two generators σ and σ' of the elementary abelian group G of order p^2. Let $t = \sigma - 1$ and $t' = \sigma' - 1$. A more precise version of the idea just formulated would then be:

$$\mathrm{Fitt}_{\Lambda[G]}(X_S) = (t, t', T) \cdot \Theta.$$

The main results of [17] show that this is not true. The Fitting ideal is more complicated, but it has finite index in the right-hand ideal of the preceding formula (this was expected beforehand). To be precise, from loc. cit. p. 122 item (I) one can extract that

$$\mathrm{Fitt}_{\Lambda[G]}(X_S) = \Big((t,t')(t,t',p), T(t,t',p), T^2\Big) \cdot \Theta.$$

Admittedly this is not too illuminating without much more context, and the formulas get a lot worse when the structure of G gets more complicated. It took a second paper [19] to obtain a final and complete result. Interested readers are referred to both papers; presumably it is better to start with [17].

To close this subsection, we briefly mention a further development [20] in this direction. In the previous results, one is forced to admit all ramified places of K/k into S, besides the p-adic places. However, as said before, the natural object is X_{S_p}, where S_p is just the set of places above p.

Again, X_{S_p} is related by a short exact sequence to X_S. But again this does *not* mean that the step from X_S to X_{S_p} is at all easy, the core of the problem being concentrated in the case where G is a p-group. The paper just quoted determines the Fitting ideal of X_{S_p}, but this requires a lot of technique. Loosely speaking, a complete rebooting of the cohomological machinery that led to the 4-term exact sequences from the outset is needed. For precise statements and proofs we must refer to [20].

5.4 ETNC and Brumer-Stark

For about 15 years now, results on Fitting ideals of class groups have been proved via the so-called equivariant Tamagawa number conjecture (ETNC for short). We cannot explain this conjecture, which is very general; actually it can be stated for many motives, for example coming from elliptic curves, and only one motive is really relevant in the present context. ETNC has a lot to do with cohomology again, and there are 4-sequences involved that are very similar to the ones we saw before. But this is not enough to describe ETNC; one also needs regulators, and when one really works on ETNC one has to grapple with very complicated big diagrams. Our knowledge on the relevant incarnation of ETNC depends very strongly on the base field; it is known if k is abelian over $\mathbb{Q}$ [4, 10], and for many fields k that are abelian over an imaginary quadratic field [1].

We deal with the standard setup: L is an abelian CM extension of a totally real field k, $G = \mathrm{Gal}(L/k)$, and we invert 2; that is, we put $R = \mathbb{Z}[1/2][G]/(1+j)$ and study the R-Fitting ideal of *the dual of* $\mathbb{Z}[1/2] \otimes_{\mathbb{Z}} cl_L^-$. In [13], this ideal is determined and identified with a suitable generalization of Kurihara's Stickelberger ideal (which in turn is a variant of Sinnott's ideal in the cyclotomic case), under the following assumptions: the relevant case of ETNC holds true, and the module of roots of unity in L is c.t./G outside the 2-part. We recall that the Stickelberger ideal needs in general many generators; and in the case $L = \mathbb{Q}(\zeta_n)$ the element θ_n we considered is not itself in this ideal, it has to be multiplied by a simple and explicit factor.

Taking the dual is necessary. Indeed the result would be wrong for the un-dualized class group, as shown in Theorem 3.1 of [16]. This actually produces an example where locally at a prime p, the so-called top-level Stickelberger element $\theta_{L/k}$ (the exact analog of θ_n, defined by L-values at $s = 0$) is already in the Stickelberger ideal (no auxiliary factor needed to achieve integrality, because there are no non-trivial p-power roots of unity in L), and fails to be in the Fitting ideal of the p-part of the un-dualized minus class group.

The result of [13] was improved a great deal in [26]. To understand this we need to discuss a different way of making the Stickelberger elements integral; this is the

so-called T-modification. This might be the better way, because it has a canonical counterpart on the side of class groups. This was already briefly explained in Sect. 5.3. Recall our assumption that T is a finite set of places of k, disjoint with the set S, and large enough so that there are no nontrivial roots of unity in K which are congruent to 1 at every place above T. Moreover we have a variant of the class group, the ray class group cl_L^T of conductor T, which maps onto cl_L. Its p-part is denoted by A_L^T. The variant $\theta_{S,L}^T$ now arises by inserting certain factors, one for each place in T, in the infinite products which define the generalized Dirichlet series attached to k and characters χ of G. The last condition on T ensures integrality of θ_L^T. The main result of [26] now eliminates the c.t. hypothesis on roots of unity (still keeping the hypothesis on the validity of ETNC). It shows that the Fitting ideal of the non-2-minus-part of $(cl_L^T)^\vee$ is given by a T-version of the Kurihara-Sinnott Stickelberger ideal.

Stop press: In March 2021, Atsuta and Kataoka sent a new preprint to the author. It seems that they succeed to treat the *un-dualized* non-2-minus part of cl_L^T by ingenious arguments. However at the time of this survey going to press, this is not yet available on the arXiv or the like.

As a kind of crowning glory of the theory, we now discuss a quite recent breakthrough concerning Brumer's conjecture, which is a far-reaching generalization of Stickelberger's annihilation theorem. We follow closely the nice presentation at the beginning of the recent preprint [21]. We keep our assumptions and notation concerning the CM extension L of a totally real field k. We recall that the finite set S of places of k must contain the places at infinity and those ramifying in L.

The so-called Brumer-Stark conjecture generalizes Brumer's original conjecture and reads as follows.

With the above assumptions on the data, the T-modified generalized Stickelberger element $\theta_{S,L}^T$ annihilates cl_L^T.

The following conjecture, called Strong Brumer Stark, implies Brumer's conjecture outside the 2-primary part. This implication is not obvious but not very hard to show either; one has to look at the plus parts and make sure that "nothing happens there". The Strong Brumer Stark conjecture goes as follows.

With the above data it holds for every odd prime p that

$$\theta_{S,L}^T \in \mathrm{Fitt}_{0,\mathbb{Z}_p[G]^-}\left((A_L^{T,-})^\vee\right).$$

(Note the presence of the dual!)

As $\theta_{S,L}^T$ lies in the T-modified Kurihara-Sinnott ideal, the paper [26] can be said to have made great progress towards this conjecture.

The conjecture was recently proven in complete generality (outside the 2 part) by Dasgupta and Kakde [8]. The proof does not proceed by establishing the relevant case of ETNC; in fact ETNC plays no direct role, and the proof uses very intricate modular theory; we cannot say anything more here. But this development shows clearly that the concept of the Fitting ideal is an important one. This recent breakthrough does *not* determine the Fitting ideal; it just shows that it contains a natural element of arithmetic nature. It remains to be seen whether a complete and unconditional determination of all Fitting ideals of class groups is possible and will happen in the next years.

5.5 Developments Not Covered in This Article; Conclusion

What follows is a terse and certainly not exhaustive enumeration of things that we consider relevant in the context of this survey article and that have not been mentioned. The subject is so rich and moving so quickly that we do not think more can be done in the present framework.

1. The methods we discussed can also very well be applied to so-called "higher class groups", that is, even-numbered K-groups of rings of integers. We only mention one very recent paper in this respect, [21], which was already cited a few paragraphs before.

2. We have consistently focussed on abelian Galois extensions; that is, all class groups were considered as modules over *commutative* rings. For some years now, non-commutative Fitting ideals have been studied very successfully. We owe this new lead to Andreas Nickel; presumably this started with the paper [29]. The reader is referred to this, and many subsequent papers of Nickel, partly co-authored by Johnston. Moreover we recommend the recent survey [30].

3. The behaviour of Fitting ideals in resolutions of modules (higher syzygies) was systematically studied by Kataoka [22]. This technique was actually needed in the statements and proofs of the results of [20].

4. In the most recent preprint [6] of Burns, Sakamoto and Sano we find very strong results on Fitting ideals of class groups. But both the statements and the list of hypotheses (partly, unproved conjectures) are so complex that we refrain from discussing them. One hypothesis (2.8(iii)) is still reminiscent of the "niceness" condition discussed much earlier.

5. The so-called function field case, see the corresponding paragraph in the introduction. We repeat that several recent papers include the function field case, for example [5]. For results that are tailored to function fields, we refer to [18].

Conclusion: Even if the question of determining Fitting ideals of class groups, taken in isolation, is perhaps not the most central problem of modern number theory, we hope to have made clear three things: the question is of inherent historical and mathematical interest; it has stimulated the development of new methods and techniques; and it is an excellent testing ground for the most recent and powerful machineries in arithmetic.

Funding Note Open Access funding enabled and organized by Projekt DEAL.

Declarations

Conflict of Interest The author declares that he has no conflict of interest.

References

1. Bley, W.: Wild Euler systems of elliptic units and the equivariant Tamagawa number conjecture. J. Reine Angew. Math. **577**, 117–146 (2004)
2. Burns, D., Flach, M.: On Galois structure invariants associated to Tate motives. Am. J. Math. **120**, 1343–1397 (1998)
3. Burns, D., Greither, C.: Equivariant Weierstrass preparation and values of L-functions at negative integers. Kazuya Kato's fiftieth birthday. Doc. Math. **Extra Vol.**, 157–185 (2003)
4. Burns, D., Greither, C.: On the equivariant Tamagawa number conjecture for Tate motives. Invent. Math. **153**, 303–359 (2003)
5. Burns, D., Kurihara, M., Sano, T.: On zeta elements for $\mathbb{G}_m$. Doc. Math. **21**, 555–626 (2016)
6. Burns, D., Sakamoto, T., Sano, T.: On the theory of higher rank Euler, Kolyvagin and Stark systems IV: the multiplicative group. Preprint (2020)
7. Cornacchia, P., Greither, C.: Fitting ideals of class groups of real fields with prime power conductor. J. Number Theory **73**, 459–471 (1998)
8. Dasgupta, S., Kakde, M.: On the Brumer-Stark conjecture. Preprint (2020). arXiv:2010.00657
9. Fitting, H.: Die Determinantenideale eines Moduls. Jahresber. Dtsch. Math.-Ver. **46**, 195–228 (1936)
10. Flach, M.: On the cyclotomic main conjecture for the prime 2. J. Reine Angew. Math. **661**, 1–36 (2011)
11. Greither, C.: Some cases of Brumer's conjecture for abelian CM extensions of totally real fields. Math. Z. **233**, 515–534 (2000)
12. Greither, C.: Computing Fitting ideals of Iwasawa modules. Math. Z. **246**, 733–767 (2004)
13. Greither, C.: Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture. Compos. Math. **143**, 1399–1426 (2007)
14. Greither, C., Kučera, R.: Annihilators for the class group of a cyclic field of prime power degree. Acta Arith. **112**, 177–198 (2004)
15. Greither, C., Kučera, R.: Annihilators of minus class groups of imaginary abelian fields. Ann. Inst. Fourier **57**, 1623–1653 (2007)
16. Greither, C., Kurihara, M.: Stickelberger elements, Fitting ideals of class groups of CM-fields, and dualization. Math. Z. **260**, 905–930 (2008)
17. Greither, C., Kurihara, M.: Tate sequences and Fitting ideals of Iwasawa modules. Algebra Anal. **27**, 117–149 (2015). Reprinted in St. Petersburg Math. J. **27**, 941–965 (2016)
18. Greither, C., Popescu, C.: Fitting ideals of ℓ-adic realizations of Picard 1-motives and class groups of global function fields. J. Reine Angew. Math. **675**, 223–247 (2013)
19. Greither, C., Kurihara, M., Tokio, H.: The second syzygy of the trivial G-module, and an equivariant main conjecture. In: Development of Iwasawa Theory - the Centennial of K. Iwasawa's Birth. Advances Studies in Pure Math., vol. 86, pp. 317–349. Math. Soc. of Japan, Tokyo (2020)
20. Greither, C., Kataoka, T., Kurihara, M.: Fitting ideals of p-ramified Iwasawa modules over totally real fields. Preprint (2020, submitted)
21. Johnston, H., Nickel, A.: An unconditional proof of the abelian Iwasawa main conjecture and applications. Preprint (2020). arXiv:2010.03186
22. Kataoka, T.: Fitting invariants in equivariant Iwasawa theory. In: Development of Iwasawa Theory - the Centennial of K. Iwasawa's Birth. Advanced Studies in Pure Math., vol. 86, pp. 413–465. Math. Soc. of Japan, Tokyo (2020)
23. Kurihara, M.: Iwasawa theory and Fitting ideals. J. Reine Angew. Math. **561**, 39–86 (2003)
24. Kurihara, M.: On the structure of ideal class groups of CM fields. Doc. Math. **Extra Volume Kato**, 539–563 (2003)
25. Kurihara, M.: Refined Iwasawa theory and Kolyvagin systems of Gauss sum type. Proc. Lond. Math. Soc. **104**, 728–769 (2012)
26. Kurihara, M.: Notes on the dual of the ideal class group of CM fields. J. Théor. Nr. Bordx., Special Issue Iwasawa (2019, to appear)
27. Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$. Invent. Math. **76**, 179–330 (1984)
28. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, 2nd edn. Grundlehren der Mathematischen Wissenschaften, vol. 323. Springer, Berlin (2008)
29. Nickel, A.: Non-commutative Fitting invariants and annihilation of class groups. J. Algebra **323**, 2756–2778 (2010)
30. Nickel, A.: Notes on non-commutative Fitting invariants (with an appendix by H. Johnston and A. Nickel). In: Development of Iwasawa Theory - the Centennial of K. Iwasawa's Birth. Advanced Studies in Pure Math., vol. 86, pp. 27–60. Math. Soc. of Japan, Tokyo (2020)

31. Northcott, D.G.: Finite Free Resolutions. Cambridge Tracts in Mathematics, vol. 71. Cambridge University Press, Cambridge (1976)
32. Ohshita, T.: On the higher Fitting ideals of Iwasawa modules of ideal class groups over real abelian fields. J. Number Theory **135**, 67–138 (2014)
33. Schoof, R.: Minus class groups of the fields of the ℓ-th roots of unity. Math. Comput. **67**, 1225–1245 (1998)
34. Sinnott, W.: On the Stickelberger ideal and the circular units of a cyclotomic field. Ann. Math. **108**, 107–134 (1978)
35. Washington, L.: Introduction to Cyclotomic Fields, 2nd edn. Graduate Texts in Mathematics, vol. 83. Springer, New York (1997)

Cornelius Greither after studying mathematics and computer science in Munich and (one year) at the University of Chicago, got his PhD and his habilitation at LMU Munich. After various research stays and "Professurvertretungen" in Bonn, Karlsruhe, Bordeaux, Ulm and other places, he took up a tenure-track professorship at Université Laval (Québec, Canada) in 1995. Since 1999 he has been full professor at Universität der Bundeswehr, München. His main interests are algebraic number theory, Iwasawa theory, and Hopf algebras acting on field extensions. From 2004 to 2017 he was on the scientific committee for the biannual international Iwasawa conferences.