Wydział Matematyki i Informatyki
Uniwersytetu im. Adama Mickiewicza w Poznaniu

Środowiskowe Studia Doktoranckie
z Nauk Matematycznych

Galois modules, Iwasawa theory and leading term conjectures

Cornelius Greither

Institut für Theoretische Informatik und Mathematik
Universität der Bundeswehr, München
cornelius.greither@unibw.de

Publikacja współfinansowana ze środków Uni Europejskiej
w ramach Europejskiego Funduszu Społecznego

Po prostu wierzyć się nie chce, że kłamstwo
istniało przed wynalezieniem druku.
S. J. Lec

The underlying theme of these lectures (and of much work in the past and present) is the connection between algebraic structures coming from number theory and geometry on the one side, and arithmetic data coming from zeta and L-functions on the other. A prototypical and classical example is the analytic class number formula. If K is a number field, then its class number (the order of the ideal class group of K) is given by $-w_K/R_K$ times the leading coefficient of the Dedekind zeta function $\zeta_K(s$ at $s = 0$. Since Galois extensions K/F play such an enormous role in algebraic number theory, it is natural to regard actions of the Galois group G of K/F on all kind of objects, for example the class group cl_K. This class group together with the G-action is a much more interesting and subtle object than just the class number. For instance one can sometimes factor the class number into χ-class numbers, one for each irreducible character of G. Such a factorization should also be reflected in a refined class number formula involving L-functions, again one function for each χ. This is indeed possible. In the proofs, Iwasawa theory play a decisive role. Its main idea is to consider not only one field K but a whole (infinite) tower of fields $K = K_0 \subset K_1 \subset K_2 \ldots$ Contrary to appearances, this sometimes has a simplifying effect. (This can be compared to analysis; real numbers are given by infinite series, but they are a most useful abstraction. Working with finite precision is often much more cumbersome from the theoretical point of view.)

This series of lectures will try to tell something about the techniques (local methods, Iwasawa theory, a little homological algebra) as well as the results. The philosophy sketched above extends to many other domains of contemporary mathematics; we only mention K-theory and the theory of elliptic curves.

Introduction

This course is intended as an introduction to two related topical areas of contemporary algebraic number theory. We will begin by giving a solid review of the relevant parts of classical algebraic number theory, with an emphasis on examples. This is not only useful and necessary for what follows but also an end in itself. In a similar vein, we will not aim for maximal generality in the later, more specialised parts, but try to motivate things and to explain what is going on.

The two areas we will then focus on are Iwasawa theory and a certain Leading Term Conjecture. In passing we will also discuss some highlights of additive Galois module structure. In all of these topics, three aspects meet and interact: classical objects of number theory (for example class groups), group actions, and objects of analytic origin (Zeta functions, and a little more generally L-functions). The analytic class number formula is a prototype of a result connecting an L-function (in fact a Dedekind zeta function) to the class number of a number field K. It gives the residue of ζ_K at $s = 1$ as a product of the

class number, the regulator, and a few technical terms. Via the functional equation, it can be reformulated as:

$$\zeta_K^*(0) = -h_K w_K / R_K.$$

Here $f^*(0)$ is the first non-vanishing Taylor coefficient in the development of the analytic function $f(s)$ around $s = 0$; h_K is the class number, w_K is the (finite!) cardinality of the group of roots of unity in K, and R_K is the regulator, defined in terms of certain logarithms of units.

We are interested in refinements of this formula taking into account the action of a Galois group. One such refinement arises in Iwasawa theory, where one considers an infinite tower of Galois extensions of a very special kind. One simple example is the following tower:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\Big(\sqrt{2+\sqrt{2}}\Big) \subset \mathbb{Q}\Big(\sqrt{2+\sqrt{2+\sqrt{2}}}\Big) \dots$$

The n-th field in his tower (starting with $n = 0$) is a cyclic extension of $\mathbb{Q}$ of degree 2^n. This is an example of a so-called cyclotomic Iwasawa extension.

Contrary to first impressions, such infinite towers actually smoothen some algebraic problems, since one is able to work over a ring Λ with good properties. Another approach to studying number-theoretical objects is provided by cohomologically trivial modules. Cohomological triviality is a generalisation of the notion of freeness for modules. This complicates things at first sight, since the standard objects (class groups, unit groups) are usually not cohomologically trivial themselves, so one has to look for "approximations" of them which are cohomologically trivial. In the end however, this leads to very precise conjectures, which are far-reaching generalisations of the Analytic Class Number Formula, and not proven in general yet.

There will be exercises in the Notes and in the Course. The Notes contain a short bibliography. For introductory reading (if desired), the author would like to recommend two books: G. Janusz, *Algebraic Number Fields* (2nd ed.), AMS, Providence 1996; and L. C. Washington, *Introduction to Cyclotomic Fields* (2nd ed.), Graduate Texts in Mathematics 83, Springer, New York 1997. Of course it is not expected that anybody is familiar with the whole content, or even major parts of these two volumes. A reasonable set of prerequisites would be: a good knowledge of general algebra (rings, modules, fields), and some acquaintance with algebraic number theory. To give an idea: it would be good if the notions of Galois extensions and class number have already been encountered by most participants, but both notions will actually be explained.

In the sequel we will sketch the content of the individual sections.

1. Reminders and preparations

1.1. A quick review of Galois theory, with examples

We will always look at an extension L/K of fields such that $[L : K]$, the K-dimension of L (also called the degree of L over K), is finite. Examples are abundant: $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ (here the degree is 2, unless m happens to be a square in $\mathbb{Q}$); $\mathbb{C}/\mathbb{R}$ (degree 2 of course);

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$. In the last example, which we will revisit a lot, the degree is a little trickier to determine: it is $\phi(n)$ (Euler's totient function of n).

The most basic notions in this course are Galois groups and Galois extensions. By definition, a K-automorphism of L is a map $\sigma\colon L \to L$ which is identity on K and satisfies $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in L$. Such a map cannot send a nonzero x to zero (why?) and therefore has to be injective. As it is K-linear by the defining properties, and L is finite-dimensional, it actually has to be bijective, which justifies the word automorphism.

We define $G(L/K)$ to be the set of all K-automorphisms of L. A moment's thought shows that this is a group under composition. For example $G(\mathbb{C}/\mathbb{R})$ consists exactly of the identity and of complex conjugation. (Where can the element i map under an automorphism?)

By definition, L/K is called a *Galois extension* if equality is $G(L/K) = [L : K]$. (It can be shown that $\leqslant$ holds all the time. Thus, Galois extensions are characterised as those extensions that have as many automorphisms as possible.) For example, all examples cited above are Galois, and this is nonobvious only for the third example. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has no automorphisms other than identity, because the two nonreal cubic roots of 2 are not in this field, so it is not a Galois extension. Very often we will just write G for the Galois group $G(L/K)$ in context.

For all subgroups $H < G(L/K)$, the *fixed field* L^H is simply the set of $x \in L$ such that $\tau(x) = x$ for all $\tau \in H$. This is indeed a field, sitting between K and L. One has:

Theorem 1. *Let $G = G(L/K)$. Then L/K is Galois iff $L^G = K$ (in other, more vague terms: L^G is as small as it can be).*

In the course we will discuss one nontrivial example, as a warm-up. Let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt[4]{7}, i)$. Write β for $\sqrt[4]{7}$. We will first calculate $[L : \mathbb{Q}]$ and then show that $L/\mathbb{Q}$ is Galois by finding enough automorphisms. We will find that the Galois group of $L/\mathbb{Q}$ is one of the two non-abelian groups of order eight, to wit, the dihedral group. We will really go into the details here.

Next we will discuss/recall splitting fields. They are important examples of Galois extensions. In particular we will see that $L = \mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois and calculate its Galois group G. The field L is the splitting field of the polynomial $X^p - 1$ over $\mathbb{Q}$, and the Galois group is isomorphic to the group of prime residues modulo p.

Let us now recapitulate the main arithmetic objects associated to any number field L (of course there are others):

$$\begin{aligned} \mathcal{O}_L &: \text{ the ring of integers in } L. \\ cl(\mathcal{O}_L) &: \text{ the class group of } L \text{ (ideals modulo principal ideals)} \\ E_L = \mathcal{O}_L^\times &: \text{ the units of } L. \end{aligned}$$

Whenever L/K is G-Galois, all these objects carry an action of G; in other words, they are modules over the group ring $\mathbb{Z}[G]$. One is interested in the structure of these modules.

1.2. Some algebra

Some of the rings one frequently encounters in our theory are not quite as nice as the ring $\mathbb{Z}$ of integers. We discuss the differences, and what can be done in more generality. In particular, not every ring of integers has unique factorisation into prime elements.

The ring $\mathbb{Z}$ is what we call a PID (principal ideal domain): it has no zerodivisors, and every ideal is principal (generated by one element). Every finitely generated $\mathbb{Z}$-module M without torsion, that is without nonzero elements of finite order, is free:

$$M \cong \mathbb{Z}^k$$

for exactly one integer k, the rank of M. In other words: M has a $\mathbb{Z}$-basis $m_1, \ldots, m_k$. That is, every $m \in M$ has a unique representation $m = \sum_{i=1}^{k} z_i m_i$ with coefficients $z_i \in \mathbb{Z}$. A standard example is $M = \mathcal{O}_K$, with K a number field of degree k. A concrete instance is $K = \mathbb{Q}(i)$: here $\mathcal{O}_K = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ (this is not completely trivial), and $\{1, i\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

The frequently used rings $\mathcal{O}_K$ and $\mathbb{Z}[G]$ fail to be PIDs in general, but the group ring fails in a worse way, so to speak. Much of the theory of PIDs can be salvaged for rings of integers, albeit at a certain price. If all rings of integers were PIDs, Fermat's Last Theorem would have been proved 150 years ago.

In the course we will need to do some module theory in greater generality. Let R be any ring; as we do not suppose R commutative, we have to watch sides, and we declare: modules are left R-modules. We know what free modules are: isomorphic copies of R^k. The description of free modules via R-bases carries over literally.

Definition 1. *An R-module P is projective, if for every R-linear surjection $f\colon M \to N$ and every R-linear map $h\colon P \to N$, there is a "lift" $\tilde{h}\colon P \to M$ such that $f\tilde{h} = h$.*

This looks very abstract, but it is useful. First of all, free modules are easily seen to be projective. (One may define the "lift" $\tilde{h}$ by its values on a basis.) Projective modules have nice permanence properties, and over a PID they are all free.

We recall that R is called a domain if it is commutative and does not have zerodivisors (equivalently: if R is a subring of a field). A very central notion in algebraic number theory is defined as follows.

Definition 2. *A domain R is a* Dedekind ring*, if all its ideals are finitely generated and projective as R-modules.*

This looks very abstract. But at least it is clear that every PID is Dedekind: in fact, every ideal is either zero, or free of rank one. The main motivation for studying Dedekind rings is the following theorem. Its proof is interesting but so long that we will not be able to cover it in the course.

Theorem 2. *For every number field K, the ring of integers $\mathcal{O}_K$ is a Dedekind ring.*

In the course we will at least discuss one fairly simple example at length. Let $K = \mathbb{Q}(\sqrt{-5})$. We shall see that $R = \mathcal{O}_K$ is not a PID. Indeed if it were, one would have unique factorization into prime elements, similarly as for the ring $\mathbb{Z}$. Look at the factorizations

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \qquad (*)$$

None of the four elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ can be factored further in R. So we get two essentially different factorizations of $6 \in R$. From this one can deduce that the ideal $I = (2, 1 + \sqrt{-5}) = 2R + (1 + \sqrt{-5})R$ cannot be principal.

But in Dedekind rings, every nonzero ideal can be uniquely factored into a product of prime ideals. We will illustrate this for the above example.

Next we explain/review the notions of class group and class number. "Ideal" will always mean "nonzero ideal" in this context. Two ideals I and J are called equivalent if they are R-isomorphic. Equivalently, if there are $x, y \in R \setminus 0$ such that $xI = yJ$. One class under this equivalence relation is the class of all principal ideals. It is fairly easy to see that multiplication of ideals is compatible with equivalence, so the factor set

$$cl(R) = \text{ ideals of } R \text{ modulo equivalence}$$

becomes a commutative monoid. (The neutral element is given by the class of principal ideals.) It is not too hard to show that this is even a group. In elementary terms, this amounts to showing that for every ideal I there is another ideal J such that IJ is principal. (Generally, such ideals I are called invertible ideals.) A fundamental result, which does require a considerable effort to prove, states that the class group $cl(\mathcal{O}_K)$ is always finite. (This would be wrong for general Dedekind rings R.) Its order h_K is called the class number of K. In the above example, the class number is exactly 2 in this example. It cannot be 1, since this would mean that O_K is a PID, so would have unique factorization into prime elements, and this is not the case.

We need two basic algebraic techniques: localisation, and completion.

Localisation can be described as "fractional calculus for rings", From now onward, R is supposed to be a domain (no divisors of zero).

Definition 3. (1) *A subset $S \subset R$ is called multiplicative if $1 \in S$, $0 \notin S$, and $s, s' \in S$ implies $ss' \in S$.*

(2) *If $S \subset R$ is multiplicative, we define an equivalence relation $\sim$ on $R \times S$ by decreeing*

$$(r, s) \sim (r', s') \longleftrightarrow rs' = r's.$$

The set of classes under $\sim$ is written R_S, and the class of (r, s) is written r/s or $\frac{r}{s}$.

(3) *One defines addition and multiplication on R_S by the (hopefully obvious) formulas*

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}; \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

By unenlightening routine verifications, one can show that R_S again is a ring, and actually a domain.

A standard example arises taking the maximal possible choice $S = R \setminus 0$ (if you like, take $R = \mathbb{Z}$); then the result ring R_S is actually a field, the so-called quotient field of R (for $R = \mathbb{Z}$ we of course get $\mathbb{Q}$). The really interesting applications concern rings that sit somewhere between R and its quotient field.

A very important class of such "localisations" is obtained as follows. For any prime ideal, the complement $S = R \setminus \mathfrak{p}$ is multiplicative. Almost everywhere in the literature the notation R_S in this particular case is replaced by $R_{\mathfrak{p}}$. This should not lead to any confusion, because $\mathfrak{p}$ itself never is a multiplicative set, as it contains 0.

In this context we will discuss local rings, that is, rings having exactly one maximal ideal. For example, the ring $\mathbb{C}[[X]]$ of formal power series is local: here the maximal ideal consists of all power series divisible by X (i.e. without constant term). Localisation and completion techniques produce many more examples. Localisations of Dedekind rings are again Dedeking, and even PIDs if one localises at a maximal ideal.

At the end of this section we discuss the behaviour of prime ideals of the bottom field K in a finite extension L. The important thing to note is that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ will no longer be prime when pushed up to L, that is, $\mathcal{O}_L\mathfrak{p}$ will have nontrivial factors. The shape of this factorization is quite important. In particular $\mathfrak{p}$ is called ramified, if the pushed-up ideal has repeated factors. We will discuss many examples.

In another subsection we will discuss completions. This is another process on rings and fields, closely analogoues to the process of obtaining the real numbers from the rationals by adjoining all limits of Cauchy sequences. When applied to $\mathbb{Z}$ for instance, this is more radical than localisation; the result is a local ring, but in a certain way even simpler than the localised ring. In this context we will also treat (or review) discriminants. To each extension L/K one can associate a discriminant, and the primes of K that ramify in L are exactly those that divide the discriminant. Discriminants "commute" in a certain way with completions, so it is enough to be able to calculate discriminants of completed fields.

2. Galois modules and Iwasawa theory

Here we begin with out subject matter proper. We are interested in some canonical objects (rings of integers, class groups), and their structure as Galois modules, that is, as modules over the relevant group ring. This accurately describes the first subsection; in the second (Iwasawa theory) a passage to the limit is involved as well.

2.1. Tame extensions, additive Galois modules

We keep looking at a G-Galois extension L/K of number fields. Recall that $\mathbb{Z}[G]$ acts on several objects attached to L (ring of integers, units, class group). Of course $\mathbb{Z}[G]$ also acts on the additive module L; but obviously the larger group ring $K[G]$ acts on L as well: K via multiplication, G via automorphisms. There is a classical result in this context, the Normal Basis Theorem:

Theorem 3. *The $K[G]$-module L is free on one generator. In explicit terms, there exists $x \in L$ (a so-called normal element for L/K) such that the set of all conjugates $\{\sigma x | \sigma \in G\}$ is a K-basis of L (a so-called normal basis).*

Example 4. *If L/K is a quadratic extension, say $L = K(\alpha)$ with $\alpha^2 = a \in K$, then $x = 1 + \alpha$ is a normal element; together with its conjugate $1 - \alpha$ it visibly spans L over K.*

The start of "tame additive Galois module theory" is the observation that it makes sense to look at the integral version of normal bases. One may ask whether $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module. Let us look at two examples ($K = \mathbb{Q}$).

$L = \mathbb{Q}(\sqrt{-3})$: Here $\mathcal{O}_L$ has the $\mathbb{Z}$-basis $1, (1 + \sqrt{-3})/2$. (Note the latter is a primitve 6th root of unity). And in fact $x = (1 + \sqrt{-3})/2$ is a $\mathbb{Z}[G]$-generator of $\mathcal{O}_L$: the conjugate is $x' = (1 - \sqrt{-3})/2$, so $x + x' = 1$, and x, x' generate $\mathcal{O}_L$ over $\mathbb{Z}$. So the answer to the question is yes.

$L = \mathbb{Q}(i)$, so $\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z}i$: Assume that $x = a + bi$ is a $\mathbb{Z}[G]$-generator, that is, $a + bi$ together with $a - bi$ is a $\mathbb{Z}$-basis of $\mathbb{Z} \oplus \mathbb{Z}i$. This is tantamount to

$$\det \left(\begin{smallmatrix} a & b \\ a & -b \end{smallmatrix} \right) = \pm 1.$$

But the determinant is $-2ab$, so it cannot be ± 1, and the answer to the question is no.

It turns out that much more reasonably one should ask two related questions.

– Is $\mathcal{O}_L$ projective over $\mathcal{O}_K[G]$?
– If yes, what is its structure? Under what conditions is it free?

A classical result, going back to E. Noether (1931), answers the first question: $\mathcal{O}_L$ is projective over $\mathcal{O}_K[G]$ iff L/K is at most tamely ramified. (Of course the notion "tamely ramified" will be explained. For the moment, let us just say that if there is no ramified prime at all, then the extension is certainly tame.)

Noether's theorem is just the starting point of a whole theory, founded by Fröhlich and brought to perfection by M. Taylor. We will give a few highlights, without any proofs, and then we will move on to Iwasawa theory.

2.2. Classical Iwasawa theory

In general it is very hard to determine the structure of $cl(\mathcal{O}_L)$ as a Galois module, that is, over $\mathbb{Z}[G(L/K)]$, assuming that L/K is Galois. When one looks at particular extensions which somehow permit a passage to a limit (a certain infinite extension), then surprisingly precise descriptions become possible, both in an abstract algebraic setting, and using L-functions.

For this, one fixes a prime p and a number field K.

Definition 4. *A $\mathbb{Z}_p$-extension K_∞ of K is a sequence $K = K_0 \subset K_1 \subset K_2 \subset \ldots$ such that for every n, the field K_n is Galois over K with cyclic Galois group Γ_n of order p^n. Then Γ_n is canonically isomorphic to the unique factor group of Γ_{n+1} of order p^n, and the Galois group of the field $K_\infty = \bigcup_{n=1}^{\infty} K_n$ over K is the projective limit of the system $(\Gamma_n)_n$. This limit Γ is isomorphic to the additive group $\mathbb{Z}_p$ of the p-adic integers. Indeed,*

$\mathbb{Z}_p$ also arises as the projective limit of the finite cyclic groups $\mathbb{Z}/p^n$; it suffices to pick a coherent sequence of generators γ_n for Γ_n, and to identify $\mathbb{Z}/p^n$ with Γ_n via $1 \mapsto \gamma_n$.

This identification explains the name "$\mathbb{Z}_p$-extension", but the name "Γ-extension" has also been used, for example by Iwasawa, the founder of the theory.

A standard example is obtained as follows: Assume $p \neq 2$, and let $K_{(m)}$ be the maximal subextension with p-power degree in $K(\zeta_{p^{m+1}})/K$, where ζ_s always denotes a primitive sth root of unity. Since $\mathrm{Gal}(K(\zeta_{p^{m+1}})/K)$ is cyclic, $K_{(m)}$ exists and has cyclic Galois group over K. Frequently $K_{(m)}/K$ has degree exactly p^m for all m, for instance if $K = \mathbb{Q}$. In general, one may show that there is an n_0 such that $K_{(m)}/K$ has degree 1 resp. p^{m-n_0} for $m < n_0$ (resp. $m \geqslant n_0$), and we again get a $\mathbb{Z}_p$-extension by letting $K_n = K_{(n+n_0)}$. For $p = 2$ a slight modification of this construction also works. The extensions obtained in this way are called *cyclotomic $\mathbb{Z}_p$-extensions.*

Now if a $\mathbb{Z}_p$-extension K_∞/K is given, we may consider, for every n, the p-primary part A_n of the class group of K_n as a module over the group ring $\mathbb{Z}_p[\Gamma_n]$. The module $X = X(K_\infty/K)$ is defined by

$$X = \lim_{\leftarrow n} A_n.$$

This projective limit is taken with respect to the norm maps $A_{n+1} \to A_n$. By considering ramification it may be shown that these norm maps are surjective for n sufficiently large. (cf. [Wa] Thm.10.1 plus Lemma 13.3.), so there is some hope a priori that one can recover A_n from X.

So X is some class-group-like object at infinite level. What is the correct "group ring" that acts on it?

We define Λ as a projective limit

$$\Lambda = \lim_{\leftarrow n} \mathbb{Z}_p[\Gamma_n].$$

Obviously Λ is a commutative ring. It is called the *Iwasawa algebra,* and the modules over it are of central importance. It will be important to identify Λ with another compact $\mathbb{Z}_p$-algebra: $\mathbb{Z}_p[[T]]$ with the $\mathfrak{m}$-adic topology, where $\mathfrak{m} = (p, T)$ is the maximal ideal. It is well-known that $\mathbb{Z}_p[[T]]$ is factorial and of Krull dimension 2. It can be seen as a completion of $\mathbb{Z}[T]$, and it is important to appreciate that $\mathbb{Z}_p[[T]]$ is somehow simpler than $\mathbb{Z}[T]$: one can give a nice description of its prime elements. Call $f(T) \in \mathbb{Z}_p[[T]]$ distinguished if $f(T)$ is a monic polynomial and all coefficients of f but the leading one are divisible by p. Examples: $f = T$ or $f = T^2$ or $f = T^2 + pT + p$. One then can show: Every $f \in \mathbb{Z}_p[[T]]$ whose coefficients are not all divisible by p is associated to a distinguished polynomial, and the prime elements of $\mathbb{Z}_p[[T]]$ are, up to unit factors, precisely the following: p, and all irreducible distinguished polynomials $f(T)$.

The main feat of Iwasawa theory is a classification of Λ-modules, not up to isomorphism, but up to a slightly weaker equivalence relation. This is strong enough to prove the following main result, due to Iwasawa himself. Let $K_\infty = \bigcup K_n$ be a $\mathbb{Z}_p$-extension, and let A_n be the p-part of the class group of $\mathcal{O}_{K_n}$ for all n. Then the orders of the A_n (in other words, the p-parts of the class numbers h_{K_n} grow in a remarkably regular fashion:

Theorem 5. *There exist $\lambda, \mu, \nu \in \mathbb{N}$ such that for sufficiently large n we have*

$$|A_n| = p^{\lambda n + \mu p^n + \nu}.$$

There are various conjectures and many calculations concerning these Iwasawa invariants λ, μ, ν in the case of the *cyclotomic* $\mathbb{Z}_p$-extension. For instance one conjectures that the μ-invariant is always zero for cylcotomic $\mathbb{Z}_p$-extensions.

2.3. The Main Conjecture

Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension and X the associated Iwasawa module. To any finitely generated Iwasawa module Y one can associate a characteristic polynomial $chr(Y)$ which knows a lot about its structure. The characteristic polynomial $chr(X)$ has the form $p^e f$ with f a distinguished polynomial; we have $e = \mu$ and $deg(f) = \lambda$. This polynomial should be considered as a far-reaching refinement of a class number. Since class numbers are linked to L-functions by the so-called analytic class number formula (ACNF), it is reasonable to look for a similar interpretation of $\mathrm{char}(X)$. This is the goal of so-called main conjectures: construct a certain element f of Λ (which will usually be a power series, not a polynomial), and then prove it coincides with $\mathrm{char}(X)$ up to a unit factor.

Since this is somewhat difficult, we will motivate this by reviewing a special case of ACNF, and then sketch the construction of certain power series in terms of L-functions. The precise formulation of the Main Conjecture is relegated to the course; it postulates an equality (up to unit factor) between characteristic polynomials of Iwasawa modules (which are genuinely algebraic objects) and these power series (which are ultimately of analytic origin). In the special case of ACNF, and in the construction of the power series, Stickelberger elements will play a big role; they are very classical objects, dating back to 1870.

3. Leading Term Conjectures

In this third and final section, we will try to explain some very general conjectures which avoid the detour via infinite level, in comparison with Iwasawa theory. There is a certain price to pay; the general statements are very abstract, and it takes an effort to unwind all the definitions, even in fairly simple cases. But the effort in formulating these conjectures is well spent, because it is known that they are very "influential", that is: if they are true, then many other things can be proved.

A part of the price to be paid is that we again have to invest some time into abstract algebra. This is the content of the first subsection.

3.1. A rapid introduction to cohomology

In the sequel, let G be a group, R a commutative coefficient ring, and all occurring modules are $\mathbb{Z}[G]$-modules. Group cohomology arises from one particular left exact functor, the functor $A \mapsto A^G$ (the $\mathbb{Z}$-submodule of G-fixed elements). Actually this is the same

as the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, where $\mathbb{Z}$ carries the trivial action of G. This functor is not exact, that is, it fails to preserve epimorphisms. It is best to introduce cohomology in all degrees at once. We do not have time for the details, and just state the outcome.

There is a family of functors $\mathrm{H}^q(G, -)$ from $\mathbb{Z}[G]$-modules to $\mathbb{Z}$-modules such that:

(1) $\mathrm{H}^0(G, A) = A^G$;

(2) for any s.e.s. $0 \to A \to B \to C \to 0$ there is a long exact sequence

$$0 \to A^G \to B^G \to C^G \to \mathrm{H}^1(G, A) \to \mathrm{H}^1(G, B) \to \mathrm{H}^1(G, C) \to \mathrm{H}^2(G, A) \dots$$

The maps $\mathrm{H}^q(G, C) \to \mathrm{H}^{q+1}(G, A)$ are called *connecting homomorphisms*.

(3) H^q commutes with direct sums, and if A is $\mathbb{Z}[G]$-free (or more generally $R[G]$-free where R is any commutative ring), then $\mathrm{H}^q(G, A)$ vanishes for all $q > 0$.

In low degrees one can calculate these groups explicitly.

A big role is played by cohomologically trivial (c.t.) modules. A G-module A is *cohomologically trivial* iff $\hat{\mathrm{H}}^q(U, A) = 0$ for all q and all subgroups U of G. Then if A is $R[G]$-free for some base ring R, then one can easily see it is also free over $R[U]$ for all $U < G$ (of which rank?), and hence c.t.; moreover, since cohomology commutes with direct sums, it even suffices that A is $R[G]$-projective, to make it c.t.

We will look at several concrete examples of modules, c.t. or otherwise, from number theory.

Finally we also need to know something about the functor Ext. It is actually closely related to cohomology.

3.2. Ingredients for LTC (Leading Term Conjecture)

The rest of this Extended Abstract will be brief, just dropping some names and notions. The course will (hopefully) provide enough detail to at least give a good first impression of everything.

We will have to discuss three ingredients: Regulators, L-functions, and metrised 2--extensions. At least between the former two, there is an intimate connection. The principal example of metrised 2-extension is afforded by the so-called Tate sequences.

3.3. Putting everything together

We first sketch the program. We keep our assumptions concerning L/K and S. In the extended abstract, some of the following notions are undefined; all necessary definitions are contained in the course and the Course Notes.

– First we introduce the "Euler characteristic" $\chi(E, \phi)$ attached to any metrised sequence (E, ϕ) of $\mathbb{Z}[G]$-modules. This Euler characteristic lives in a certain relative K-group $\mathrm{K}_0(\mathbb{Z}[G], \mathbb{R})$.

– Then we define an invariant $T\Omega = T\Omega_{L/K,S}$ as the difference $\chi(E_{Tate}, reg_S) - \partial(\Theta_S^*(0))$.

Then the statement is simply

$$T\Omega_{L/K,S} = 0.$$

To conclude the course, we will say something about the status of the conjecture, and verify its validity in a fairly simple but nontrivial situation.

Cornelius Greither

Profesor Cornelius Greither jest wybitnym specjalistą algebraicznej teorii liczb, teorii modułów Galois i teorii Iwasawy. Jego najważniejsze wyniki dotyczą opisu struktury algebraicznej grup klas ideałów, p-adycznej interpolacji wartości specjalnych funkcji L oraz funkcji dzeta Dedekinda ciał liczbowych. Opublikował około sześćdziesiąt prac naukowych w tak prestiżowych czasopismach matematycznych jak: *Inventiones mathematicae*, *Journal für die reine und angewandte Mathematik*, *Compositio Mathematica*, *Mathematische Zietschrift*, *Transactions of the AMS*, *Journal of Algebra*, *Acta Arithmetica* i *Journal of Number Theory*. Jego rozprawa habilitacyjna została wydana w prestiżowej serii *Lecture Notes in Mathematics* wydawnictwa Springer.

Cornelius Greither doktoryzował się na podstawie pracy z algebry przemiennej na Uniwersytecie Ludwika Maksymiliana w Monachium w 1983 roku, a w 1988 roku habilitował się na tej samej uczelni. Pracował na Uniwersytetach w Monachium, Karlsruhe, Ulm, na Uniwersytecie Lavala w Kanadzie i w Instytucie Maxa Plancka w Bonn. Od 1999 jest profesorem zwyczajnym na Uniwersytecie Bundeswehry w Monachium-Neubiberg. Wypromował sześciu doktorów matematyki. Jest edytorem czterech czasopism matematycznych o zasięgu międzynarodowym. Ponad 250 razy recenzował prace z matematyki dla *Mathematical Reviews* i dla *Zentralblatt der Mathematik*.

Poza matematyką profesor Greither aktywnie interesuje się muzyką i lingwistyką. Gra na fortepianie w tercecie *Triphonia* wykonującym utwory muzyki klasycznej i kameralnej. Potrafi komunikować się w ponad dziesięciu językach, w tym perfekcyjnie po angielsku i po francusku. Po zaledwie trzech kilkudniowych wizytach w naszym kraju opanował w zadowalającym stopniu język polski.