

Iwasawa Theory and Cohomology

(Notes of a minicourse held at Lille, July 9-13, 2001)

CORNELIUS GREITHER

Preliminary remarks: The reader should not expect a complete account of Iwasawa theory, nor a coherent development leading up to one major result. These notes were written for the benefit of the audience at Lille, as a backup to the lectures, and also for the benefit of the speaker, since they allow to omit a few things (in particular, most material printed in smaller type) from the lectures, by referring to the notes. As the reader will see, the emphasis is rather on providing techniques which were useful in some recent developments; a second objective was to prepare the ground for the three subsequent lectures of D. Benois. I am grateful to several people in the audience for pointing out inaccuracies; these have been corrected, but it is likely that others remain.

I. Standard Iwasawa theory for ideal class groups

§1 — *The setup*

Throughout these notes K is an algebraic number field and p a fixed prime number. A \mathbf{Z}_p -extension of K is a sequence $K = K_0 \subset K_1 \subset K_2 \subset \dots$ 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 \mathbf{Z}_p of the p -adic integers; simply map $1 \in \mathbf{Z}_p$ to a coherent sequence $(\gamma_n)_n$ where each γ_n is a generator of Γ_n . This explains the name “ \mathbf{Z}_p -extension”, but the name “ Γ -extension” has also been used.

A standard example is obtained as follows: Let $p \neq 2$ and $K_{(m)}$ be the maximal subextension with p -power degree in $K(\zeta_{p^{m+1}})/K$, where ζ_s always denoting a primitive s th root of unity. Since $\text{Gal}(K(\zeta_{p^{m+1}})/K)$ 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 $K = \mathbf{Q}$). 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. $m \geq n_0$), and we again get a \mathbf{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 \mathbf{Z}_p -extensions.

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

$$A = \varprojlim A_n.$$

This projective limit is taken with respect to the norm maps $A_{n+1} \rightarrow A_n$. By considering ramification it may be shown that these norm maps are surjective for $n \gg 0$ (cf. [Wa] Thm.10.1 plus Lemma 13.3.), so there is some hope a priori that one can recover A_n from A .

§2 — The Iwasawa algebra

We begin by defining Λ as a projective limit

$$\Lambda = \varprojlim \mathbf{Z}_p[\Gamma_n].$$

Obviously Λ is a commutative ring; it is called the Iwasawa algebra, and the modules over it are of central importance. The ring Λ is compact in the limit topology, where each $\mathbf{Z}_p[\Gamma_n]$ carries the p -adic topology. It will be important to identify Λ with another compact \mathbf{Z}_p -algebra: $\mathbf{Z}_p[[T]]$ with the \mathfrak{m} -adic topology, where $\mathfrak{m} = (p, T)$ is the maximal ideal. It is well-known that $\mathbf{Z}_p[[T]]$ is factorial and of Krull dimension 2. Call $f \in \mathbf{Z}_p[[T]]$ distinguished if f 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 $f = T^2 + pT + p$.

Proposition 1.2.1. (Weierstraß preparation) *Every $f \in \mathbf{Z}_p[[T]]$ whose coefficients are not all of them divisible by p , is associated to a distinguished polynomial, and the prime elements of $\mathbf{Z}_p[[T]]$ are, up to unit factors, precisely the following: p , and all irreducible distinguished polynomials $f(T)$.*

For a proof see e.g. [NSW] Chap.V §3. We are now going to show that Λ and $\mathbf{Z}_p[[T]]$ are canonically isomorphic. Note that the quotient ring $\Lambda/(f)$ is \mathbf{Z}_p -free of rank $\deg(f)$ whenever f is distinguished. We also fix generators γ_n of Γ_n in such a way that γ_{n+1} maps to γ_n for all n . Then $\gamma = (\gamma_n)_n$ is a well-defined element of Λ .

Lemma 1.2.2. *The continuous ring homomorphism $a : \mathbf{Z}_p[[T]] \rightarrow \Lambda$ with $a(T) = \gamma - 1$ is bijective (hence a topological isomorphism).*

We sketch an argument due to Serre: The map $a_n : \mathbf{Z}_p[[T]] \rightarrow \mathbf{Z}_p[\Gamma_n]$ sending T to $\gamma_n - 1$ is onto and well-defined since $\gamma_n - 1$ is topologically nilpotent. The kernel I_n of a_n is generated by the distinguished polynomial (!) $\omega_n = (T+1)^{p^n} - 1$ (this is seen by comparing \mathbf{Z}_p -ranks). Thus a is well-defined as the limit of the a_n , and has dense

image, hence is surjective by compactness of $\mathbf{Z}_p[[T]]$. If a were not injective, then $\ker(a)$ would contain a nonzero f ; since p is a nonzerodivisor on Λ we may suppose f not divisible by p . Thus, f is associated to a distinguished polynomial, and hence $\mathbf{Z}_p[[T]]/(f) \cong \Lambda$ would have finite rank over \mathbf{Z}_p , which is manifestly wrong. \square

We conclude this section by the following remark: If $\pi \in \Lambda$ is a prime element, then $\Lambda_{(\pi)}$ (one inverts all $g \in \Lambda$ *not* in (π)) is local regular of dimension 1, hence a discrete valuation ring; and $\Lambda[1/\pi]$ is regular factorial of dimension 1, hence a PID.

§3 — Iwasawa modules

Suppose until further notice that all modules are over Λ and finitely generated. We will not distinguish any more between Λ and $\mathbf{Z}_p[[T]]$. We call M torsion if there exists $0 \neq f \in \Lambda$ with $fM = 0$, and torsion-free if $fx = 0$ implies $f = 0$ or $x = 0$ ($f \in \Lambda, x \in M$). Furthermore we call $\varphi : M \rightarrow N$ a quasi-isomorphism (q.i.) if both the kernel and the cokernel of φ are finite. One shows easily that M is finite (quasi-null) iff M is annihilated by some power of the maximal ideal $\mathfrak{m} = (p, T)$, and for this it is sufficient that M is annihilated by two coprime nonzero elements.

There is a nice classification of Λ -modules up to quasi-isomorphism which is not very difficult. (We will not go into the equally nice but harder classification modulo isomorphism due to Jannsen; see [NSW].)

Theorem 1.3.1. *Every torsion module M is q.i. to a finite direct sum of cyclic modules:*

$$M \rightarrow \bigoplus_{i=1, \dots, k} \Lambda/(f_i),$$

where one may even assume that the f_i are powers of prime elements; under this assumption the decomposition is essentially unique.

We sketch the existence proof. Suppose $fM = 0$; pick a prime π coprime to f in Λ . Since $\Lambda[1/\pi]$ is a PID, we get:

$$\alpha : M[1/\pi] \xrightarrow{\sim} \bigoplus_i \Lambda[1/\pi]/(f_i)$$

with f_i prime powers in $\Lambda[1/\pi]$; we may assume the f_i are prime powers in Λ prime to π , and we may assume that α is induced by $\beta : M \rightarrow \bigoplus \Lambda/(f_i)$ by standard arguments from localization theory. Then the kernel and the cokernel die after inverting π , hence they are annihilated by some power of π . Since they are annihilated by f ($\prod f_i$ resp.), they are finite. \square

Theorem 1.3.2. *Every (f.g.) Λ -module M admits a quasi-isomorphism $M \rightarrow \text{tors}(M) \oplus F$ with F free. (Here $\text{tors}(M)$ is the submodule of Λ -torsion elements, which contains the \mathbb{Z}_p -torsion, but is in general larger.)*

Proof: One considers the short exact sequence $0 \rightarrow \text{tors}(M) \rightarrow M \rightarrow \overline{M} \rightarrow 0$ with \overline{M} defined by the sequence; obviously \overline{M} is torsion-free. By a method similar to the last proof, one shows that this s.e.s. has a “quasi-splitting”, i.e. one finds a q.i. $M \rightarrow \text{tors}(M) \oplus \overline{M}$. It remains to show that $N = \overline{M}$ is q.i. to a free module. This goes as follows: Let $-^\#$ denote the functor $\text{Hom}_\Lambda(-, \Lambda)$ (Λ -dual). One has a canonical map e from N into its bidual $N^{\#\#}$. On localizing at any prime element π , one obtains an isomorphism since all torsion-free modules over a PID are canonically isomorphic to their biduals (“reflexive”). Hence e is a quasi-isomorphism. Using a little commutative algebra one can check that over any local ring of Krull dimension 2, the dual of any (f.g.) module is already free (cf. [OSS]). Hence $N^{\#\#}$ is free, and we are done.

Example: If $N = \mathfrak{m}$, then $N^{\#\#} = \Lambda$.

The two preceding theorems put together show that every M is quasi-isomorphic to a direct sum of cyclic modules of the shape Λ or $\Lambda/(\pi^e)$ with π prime, $e \in \mathbb{N}$; this decomposition is essentially unique. M is torsion iff there are no factors Λ ; in this case the characteristic power series of M is defined to be the product of all intervening π^e ; so it is only defined up to a unit. The characteristic polynomial $\text{char}(M)$ is then the unique element of Λ having the form “ p -power times distinguished polynomial” and associated to a characteristic power series.

§4 — *The Λ -module A and its relatives*

The module A was defined in §1, starting with an arbitrary \mathbb{Z}_p -extension of a number field K . It is clear that Λ acts on A since for every n , $\mathbb{Z}_p[\Gamma_n]$ acts on A_n . By class field theory A_n is (canonically isomorphic to) the Galois group of the maximal p -abelian unramified extension of K_n . There are the following variants: $A'_n = A_n$ modulo classes of primes above p ; this is the Galois group of the maximal p -abelian unramified extension of K_n in which all divisors of p split. X_n is defined as the Galois group of the maximal p -abelian p -ramified extension of K_n , where p -ramified means: at most divisors of p may ramify. (There is also a description in terms of the idele class group.) We have epimorphisms

$$X_n \rightarrow A_n \rightarrow A'_n.$$

Let A' and X be the corresponding projective limits. (The notation varies: our A is X in [Wa] and X_{nr} in [NSW]. Our X is Y in [Wa] and X in [NWS], and our A' is X' in [Wa] and X_{cs} in [NSW].)

Theorem 1.4.1. *X (and hence A and A' as well) are finitely generated over Λ ; A (and hence A' as well) is even Λ -torsion.*

The main ingredient needed to prove this is a topological version of Nakayama's lemma. For the proof we refer to [Wa] Lemma 13.16 or [NSW] Cor.5.2.18.

Lemma 1.4.2. *If Z is a compact Λ -module, then z_1, \dots, z_n generate Z iff the residues $\bar{z}_1, \dots, \bar{z}_n$ generate $Z/\mathfrak{m}Z$. \square*

Proof sketch for 1.4.1: All three modules X , A , and A' are compact (as limits of compact modules). One can establish a short exact sequence $0 \rightarrow X/TX \rightarrow X_0 \rightarrow \Gamma \rightarrow 0$; since X_0 is finitely generated over \mathbf{Z}_p (this uses some class field theory), this gives at once that X/TX is finitely generated over \mathbf{Z}_p , thus Lemma 1.4.2 yields that X is finitely generated. One also has by [Wa] Lemma 13.15: If all ramified primes in K_∞/K are totally ramified (Assumption T), then $A/TA \cong A_0$, and this is finite. One checks using the classification of §3 that if A were not torsion then A/TA would be infinite, the main reason being that $\Lambda/T\Lambda = \mathbf{Z}_p$ is infinite. Without Assumption T, one replaces the base field K by K_m for suitably high m ; this ensures Assumption T by [Wa] Lemma 13.3, at the price of replacing Γ by its subgroup of index p^m . But then we even obtain that A (which is unchanged) is torsion over a certain subalgebra of Λ , which of course suffices. \square

We now state the main theorem for the A_n . (An analogous statement is true for A'_n , but not for the X_n which are always infinite.)

Theorem 1.4.3. *There exist $\lambda, \mu, \nu \in \mathbb{N}$ such that for $n \gg 0$:*

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

Highlights of proof: Suppose Assumption T holds. Then $A_n \cong A/\omega_n A$. By the classification one “reduces” to the case A a direct sum of cyclic modules (the finite error term goes into ν), and then of course to $A = \Lambda/(f)$ with either $f = p^e$ or f a distinguished polynomial. One calculates, and this is the fun part:

$$\begin{aligned} \left| \frac{\Lambda/(p^e)}{(\omega_n)} \right| &= p^{ep^n}; \\ \left| \frac{\Lambda/(f)}{(\omega_n)} \right| &= p^{n \cdot \deg(f) + n_0}, \end{aligned}$$

the second equality holding for $n \gg 0$ with some $n_0 \in \mathbf{Z}$. \square

There are various conjectures and many calculations concerning these so-called Iwasawa invariants λ, μ, ν in the case of the *cyclotomic* \mathbf{Z}_p -extension. For instance one conjectures that the μ invariant is always zero (equivalently: $\text{char}(A)$ is not

divisible by p). For K abelian over \mathbb{Q} this was proved by Ferrero and Washington in 1979 (cf. [Wa]). “Greenberg’s conjecture”, which might be more prudently called Greenberg’s question, proposes that both μ and λ should be zero if K is a *totally real* field. One knows plenty of fields K with $\lambda > 0$, but none of them is totally real. On the other hand there exist non-cyclotomic \mathbb{Z}_p -extensions that have $\mu > 0$.

§5 — *The main conjecture*

In this subsection we will be very brief and refer to [Wa] or [NSW] for more information. Let K_∞/K be the cyclotomic \mathbb{Z}_p -extension and A the associated Iwasawa module. The characteristic polynomial $\text{char}(A)$ has the form $p^e f$ with f distinguished; we have $e = \mu$ and $\deg(f) = \lambda$. The point is: how can one get information on $\text{char}(A)$? Any result in this direction should be viewed as generalization of the analytic class number formula, with group action and at infinite level.

We take F totally real and $K = F(\zeta_p)$. Then $\Delta = \text{Gal}(K/F)$ has order prime to p , acts on “everything”, and every $\mathbb{Z}_p[\Delta]$ -module M splits up as direct sum of the eigenspaces M_χ with χ running over the characters $\Delta \rightarrow \mathbb{Z}_p^*$. Thus we get Iwasawa modules A_χ for every χ . On the other hand, the theory of p -adic L -functions provides series $f_\chi \in \Lambda$ for *odd* characters $\chi \neq \omega$, such that

$$f_\chi(g^s - 1) = L_p(s, \omega\chi^{-1}) \quad \forall s \in \mathbb{Z}_p,$$

where: γ is a fixed generator of Γ ; g is determined by $\gamma(\zeta_{p^n}) = \zeta_{p^n}^g$ for all n ; and ω is the Teichmüller character of Δ , again given by $\delta(\zeta_p) = \zeta_p^{\omega(\delta)}$. For $\chi = \omega$ there is a somewhat similar formula.

Main Conjecture, First Form:

If $\chi \neq \omega$, then f_χ agrees, up to a unit factor, with $\text{char}(A_\chi)$.

This has been proved for $F = \mathbb{Q}$ by Mazur and Wiles [MW]; actually they allow general abelian extensions K/\mathbb{Q} and general odd Dirichlet characters $\chi \neq \omega$. For this generality the statement has to be modified slightly, since $[K : \mathbb{Q}]$ is not supposed to be prime to p . A much more general result, which replaces \mathbb{Q} by an arbitrary totally real field F , was proved by Wiles [Wi]. Briefly: The main conjecture for $p \neq 2$ is proved in maximum generality, when one takes into account the discussion of the μ -invariants on p.656f. in [NSW].

Further remarks concerning the Main Conjecture and p -adic L -functions: (1) It is not possible to introduce p -adic L -functions from scratch in the limited space we have. The essential point is that p -adic L -functions interpolate values of standard L -functions, with a little twist: for every even Dirichlet character ψ and every $n > 0$ one has (after fixing an embedding $\mathbb{C}_p \rightarrow \mathbb{C}$)

$$L_p(1 - n, \psi) = L_{\{p\}}(1 - n, \psi\omega^{-n}).$$

The notation $L_{\{p\}}$ is a special case of the notation L_S which means that all factors corresponding to places in S are omitted from the Euler product defining the L -function. Note that one p -adic L -function interpolates a sequence of values obtained by shuffling together $p - 1$ standard L -functions via twisting χ by powers of ω . The functions $L_p(s, \psi)$ are meromorphic in s on a certain ball in \mathbb{C}_p , with at most one pole, and no pole at all when ψ is nontrivial. Of course the hard point is existence since uniqueness follows from what is called “analytic continuation”.

In p -adic L -functions some limited exchange is possible between the variables s and ψ , which is more easily explained on the level of Iwasawa series (see [Wa] Thm. 7.10). More precisely: Suppose ρ is an even character of the second kind, that is: the conductor and the order of ρ are both p -powers. Then $f_{\rho\psi}(T) = f_{\psi}(\rho(g)^{-1}(1 + T) - 1)$.

(2) It is of course very important to get back from the statement of the Main Conjecture to theorems at finite level. Unfortunately, we cannot go into this interesting topic here; the general shape of these theorems is that the order of χ -parts of arithmetic objects (class groups or higher K-groups) is given by special values of (standard, not p -adic) L -values. It is important to have standard L -values here in order to obtain global statements, as in the (equivariant) Tamagawa number conjectures. As a concrete example we mention the formula of Iwasawa and Leopoldt: let $p \neq 2$, K absolutely abelian of degree prime to p . Then for every odd character $\chi \neq \omega$ of $\text{Gal}(K/\mathbb{Q})$ the order of $A(K)_{\chi}$ is in a precise sense the p -part of $L(0, \chi^{-1})$. On taking the product over all odd χ one recaptures the minus part of the analytic class number formula: $\zeta_K(0)/\zeta_{K^+}(0) = h_K^-/w_K$ up to sign and 2-power factors. This has the following analogue for zeta values at negative integers: suppose K is a totally real number field, p odd (for simplicity), and $n > 0$ even. Then the p -part z of the (rational!) number $\zeta_K(1 - n)$ can be expressed as a quotient of orders of cohomology groups: $z = |\mathrm{H}^2(O_K[p^{-1}], \mathbb{Z}_p(n))|/|\mathrm{H}^1(O_K[p^{-1}], \mathbb{Z}_p(n))|$. A similar formula “on the minus side” is true for odd n and K a CM field. These formulas are part of the so-called *cohomological Lichtenbaum conjectures*, representing the “easy part” where no regulator is involved. Under the stated conditions, $\mathrm{H}^i(O_K[p^{-1}], \mathbb{Z}_p(n))$ is isomorphic to $\mathrm{H}^{i-1}(O_K[p^{-1}], \mathbb{Q}_p/\mathbb{Z}_p(n))$ for $i = 1, 2$. The Quillen-Lichtenbaum conjecture identifies $\mathrm{H}^i(O_K[p^{-1}], \mathbb{Z}_p(n))$ with the p -part of the K-group $K_{2n-i}(O_K)$. The Lichtenbaum conjectures are obtained from the cohomological Lichtenbaum conjectures via replacing cohomology groups by the corresponding K-groups; these conjectures, including the version including regulator terms, should be regarded as generalizations of the Analytic Class Formula, expressing zeta values in terms of arithmetic objects.

What happens in the Main Conjecture and all of its variations can be summarized as follows: Arithmetical objects (class groups, K-groups etc.) are linked to special values of complex analytic functions, via the intermediary of p -adic analytic objects, which are, so to speak, a little more algebraic than analytic objects over \mathbb{C} .

II. Projective limits of unit groups, Euler systems

§1 — Semilocal units

For any number field K and any prime number p one has a canonical isomorphism $O_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \prod_{\mathfrak{p}|p} O_{K,\mathfrak{p}}$, and similarly for K instead of O_K . This ring isomorphism gives at once a corresponding isomorphism between the groups of units on both sides. We set

$$U_p(K) = \left(\prod_{\mathfrak{p}|p} O_{K,\mathfrak{p}}^* \right) \{p\}, \quad V_p(K) = \left(\prod_{\mathfrak{p}|p} K_{\mathfrak{p}}^* \right) \{p\}.$$

The symbol $\{p\}$ means p -completion; in the case of $U_p(K)$ this just amounts to factoring out by the non- p torsion. One obtains Iwasawa modules U_{∞} and V_{∞} by taking the limit of $U_p(K_n)$ (resp. $V_p(K_n)$) in a \mathbb{Z}_p -extension; from now on we will assume that this is the cyclotomic \mathbb{Z}_p -extension. We need a little modification: $\bar{U}_p(K_n) = U_p(K_n)/tors$ and $\bar{U}_{\infty} = \lim_{\leftarrow} \bar{U}_p(K_n)$. The following result is not too hard to prove (cf. [Gr1], but it was known long before).

Proposition 2.1.1. *\bar{U}_{∞} and \bar{V}_{∞} are free Λ -modules of rank $[K : \mathbb{Q}]$; one has codescent for V , i.e. the canonical map*

$$(\bar{V}_{\infty})_{\Gamma} \rightarrow V_p(K)$$

is a monomorphism. (Its image consists of the group of so-called universal norms in $V_p(K)$.) \square

Often one would like a more explicit description of U_{∞} ; we turn to this question now. To simplify things, let us try to exhibit elements of U_{∞} . First we claim $z = (1 - \zeta_{p^{n+1}})_n$ is such an element if we take $K = \mathbb{Q}(\zeta_p)$. Indeed,

$$N_{K_n/K_{n-1}}(1 - \zeta_{p^{n+1}}) = \prod_{\substack{a \equiv 1 \pmod{p^n} \\ a=0, \dots, p^{n+1}-1}} (1 - \zeta_{p^{n+1}}^a) = \prod_{b=0}^{p-1} (1 - \zeta_p^b \zeta_{p^{n+1}}) = 1 - \zeta_{p^{n+1}}^p = 1 - \zeta_{p^n}.$$

If we now try $K = \mathbb{Q}(\zeta_p, \zeta_r)$ with $(r, p) = 1$ and take $(1 - \zeta_r \zeta_{p^{n+1}})_n$, then the above calculation quickly adapts to show

$$N_{K_n/K_{n-1}}(1 - \zeta_r \zeta_{p^{n+1}}) = 1 - \zeta_r^p \zeta_{p^n},$$

(note the exponent p on ζ_r), so an adjustment is necessary: Let $F = F_p$ be the Frobenius automorphism attached to p on any field E in which p does not ramify; one has $F\zeta_r = \zeta_r^p$. Then the sequence $(1 - F^{-n}\zeta_r \cdot \zeta_{p^{n+1}})_n$ is indeed norm-coherent and gives an element of U_{∞} . The idea of Coleman's theory is now to write the entries

of any $(b_n) \in U_\infty$ as values of a power series f_b in X at the points $X = 1 - \zeta_{p^{n+1}}$; note that $f = X$ does the job in our first example!

In order to state the central technical result, let us change notation: we only look at local units, writing K for $K_{\mathfrak{p}}$. We actually assume that $K = E(\zeta_p)$ with E an unramified extension of \mathbb{Q}_p , and write O for O_E . Consequently U_∞ now has the meaning $\varprojlim O_{K_n}^*$. We make F act on K_n by letting it act trivially on p -power roots of unity (so it “only acts on E ”).

Theorem 2.1.2. (COLEMAN [Co1]) *For any norm-coherent sequence $(b_n) \in U_\infty$ there is a series $f_b \in O[[X]]^*$ with:*

$$f_b(1 - \zeta_{p^{n+1}}) = F^n b_n \quad \text{for all } n \geq 0.$$

□

We can find f_b for b as in the last example: the identity $F^n b_n = 1 - \zeta_r \zeta_{p^{n+1}} = 1 - \zeta_r + \zeta_r(1 - \zeta_{p^{n+1}})$ shows that we can take $f_b(X) = 1 - \zeta_r + \zeta_r X$. Note that this is indeed a unit since the constant coefficient is a unit. Another important example (with $E = \mathbb{Q}_p$) is the following norm-coherent family of cyclotomic units: $c_n = (1 - \zeta_{p^{n+1}}^a)/(1 - \zeta_{p^{n+1}})$ for some fixed $a \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Here one finds $f_c = [a]X/X$, where the operation $[a]$ is defined by the formula $1 - [a]X = (1 - X)^a$. Again f_c is a unit. (Exercise: what is its constant term?)

It remains to discuss why this machinery leads to an almost completely explicit description of U_∞ . In order to understand just which f are eligible as f_b (not all f are), one has to come to grips with Coleman’s Norm Operator N . This is a group endomorphism of $O[[X]]^*$ defined by the strange-looking formula

$$Nf(1 - (1 - X)^p) = \prod_{i=0}^{p-1} f(1 - \zeta_p^i(1 - X)).$$

If one were permitted to substitute $Y = 1 - X$, so $f(X) = g(Y)$, then the formula would get much neater: $Ng(Y^p) = \prod g(\zeta_p^i Y)$, so one sort of takes the norm from $\mathbb{Z}_p[Y]$ to $\mathbb{Z}_p[Y^p]$ and in the result one replaces Y^p again by Y . One easy example, for which this last argument is actually valid, is $NX = X$.

Theorem 2.1.2. (COLEMAN) *f_b is unique, and the image of the resulting map $b \mapsto f_b$ on U_∞ is*

$$\mathfrak{M}^0 = \{f \in O[[X]] : f(0) \equiv 1(p) \ \& \ F(f) = Nf\},$$

where the Frobenius acts just on coefficients. (This is just a particular case of a more general result on formal groups [Co1]; we are looking at the formal group G_m only.)

□

Through various other maps one then tries to describe \mathfrak{M}^0 ; we skip this and only explain the outcome in case $E = \mathbb{Q}_p$, $K = \mathbb{Q}_p(\zeta_p)$. We have $\Gamma' = \text{Gal}(K_\infty/\mathbb{Q}_p) = \Gamma \times \Delta$ with $\Delta = \text{Gal}(K/\mathbb{Q}_p)$; Γ' is canonically isomorphic to \mathbb{Z}_p^* (call the isomorphism κ) and acts on $O[[X]]$ via $\gamma'(X) = 1 - (1 - X)^{\kappa(\gamma')}$ for all $\gamma' \in \Gamma'$. Thus $O[[X]]$ and likewise U_∞ are modules over $R := O[[\Gamma']] = \Lambda[\Delta]$, and the result is that U_∞ is almost free cyclic over R : there is a four term exact sequence

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow U_\infty \xrightarrow{\beta} R \cdot (1 - X) \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0.$$

The very important term $\mathbb{Z}_p(1)$ needs to be explained: it is $\varprojlim \mu_{p^n}$, or in other words: \mathbb{Z}_p with Γ' acting through κ . The map β is $b \mapsto f_b$ followed by a cleverly modified logarithm (note the usual logarithm would introduce denominators). More precisely: $\beta(b) = (1 - p^{-1}\varphi) \log f_b$ with $\varphi(X) = 1 - (1 - X)^p$.

§2 — Projective limits of global units

Let again K be a number field and K_∞/K be the cyclotomic extension. We let $E(K_n) = O_{K_n}^*$. If one defines E_∞ as the projective limit of the $E(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ (note this coincides with the p -completion of $E(K_n)$ since $E(K_n)$ is finitely generated), then one can show the following result which is deeper than its semilocal analogue:

Theorem 2.2.1. ([KU]; [GR1]) *E_∞ is Λ -free of rank $r_1(K) + r_2(K)$.* \square

There is an obvious map $E_\infty \rightarrow U_\infty$ from global to semilocal units in the limit. For the injectivity of the analogous map at finite level one needs Leopoldt's conjecture to hold, but fortunately in the limit the weak Leopoldt conjecture suffices to make $E_\infty \rightarrow U_\infty$ injective, and this latter conjecture is a comparatively easy theorem (see [Wa] Lemma 13.30).

One is, in this case, interested in the quotient U_∞/E_∞ . Coleman theory can be applied when E_∞ is replaced by a more explicit subgroup, the cyclotomic units $C(K_n)$. The definition of $C(K_n)$ is a bit awkward in general, so we suppose $K = \mathbb{Q}(\zeta_p)$. There $C(K_n)$ is obtained by taking the multiplicative group generated by ± 1 and all $1 - \zeta_p^{a_{n+1}}$ with $(a, p) = 1$, and intersecting it with $E(K_n)$. Actually the norm maps $C(K_{n+1}) \rightarrow C(K_n)$ are onto, and one puts $C_\infty = \varprojlim C(K_n) \otimes \mathbb{Z}_p$. Hence one has

$$C_\infty \subset E_\infty \subset U_\infty.$$

The group Δ (see §1) acts on these modules, and since Δ has order $p - 1$, everything can be decomposed in eigenspaces corresponding to the characters of Δ . Using the results of the last subsection one then can prove a remarkable result; for its statement we need the involutory automorphism of Λ defined by $T \mapsto \dot{T} = \kappa(\gamma)(1 + T)^{-1} - 1$.

We recall that κ is the canonical injection $\Gamma \rightarrow \mathbf{Z}_p^*$, γ a fixed generator of Γ , and $\gamma = 1 + T$.

Theorem 2.2.2. (IWASAWA 1973, COLEMAN 1983 [CO2]) *For any even nontrivial character ψ of the group Δ , there is an isomorphism of Λ -modules*

$$(U_\infty/C_\infty)_\psi \cong \Lambda/(f_{\omega\psi^{-1}}(\dot{T})).$$

□

The power series $f_{\omega\psi^{-1}}$ comes from a p -adic L-function, see I.5 above; but one has to note the dot on the variable T . Let us put $\chi = \omega\psi^{-1}$. So there is a close link between the Iwasawa modules $(U_\infty/C_\infty)_\psi$ and A_χ : their characteristic polynomials are given by $f_\chi(\dot{T})$ (for the former) and $f_\chi(T)$ (for the latter).

However, the former module is cyclic and the latter need not be so. In a way that can be made precise, A_χ and X_ψ (see I.4) are duals, and their characteristic polynomials are again linked by the involution $T \mapsto \dot{T}$. Therefore $\text{char}(X_\psi) = \text{char}((U_\infty/C_\infty)_\psi)$. On the other hand, local class field theory produces an exact sequence

$$0 \rightarrow (U_\infty/E_\infty)_\psi \rightarrow X_\psi \rightarrow A_\psi \rightarrow 0.$$

We obtain by multiplicativity of char :

$$\text{If } \psi \text{ is even and nontrivial, then } \text{char}((E_\infty/C_\infty)_\psi) = \text{char}(A_\psi).$$

Let us call this the **Second Form of the Main Conjecture**. (This disagrees with the terminology in [Wa].)

§3 — Euler systems

This topic is slightly less close to Iwasawa theory, but we have already seen certain norm relations for cyclotomic elements; the theory of Euler systems systematizes these relations and draws great profit from them.

Changing notation somewhat, we let, for $0 \neq n \in \mathbf{N}$, $z_n = 1 - \zeta_n$ with $\zeta_n = \exp(2\pi i/n)$. (The main thing is to have the compatibility $\zeta_{nm}^m = \zeta_n$ always.) Let $\mathbf{Q}(n)$ denote the field $\mathbf{Q}(\zeta_n)$. The Frobenius F at p has already been defined; we now write F_p for clarity. There is an important variation on the elements z_n : fix n_0 and let n be squarefree and coprime to n_0 . Then one defines

$$y_n = 1 - \left(\prod_{l|n} \zeta_l \right) \zeta_{n_0}. \quad (l \text{ running over prime divisors of } n)$$

One then can prove the following proposition by calculations as in II.1:

Proposition 2.3.1. *Suppose $n = pm$ and $(p, m) = 1$. Then*

$$N_{\mathbb{Q}(n)/\mathbb{Q}(m)}(z_n) = z_m^{1-F_p^{-1}}; \quad (1)$$

$$N_{\mathbb{Q}(nn_0)/\mathbb{Q}(mn_0)}(y_n) = y_m^{F_p-1}. \quad (2)$$

□

Now one replaces $\mathbb{Q}(nn_0)$ by $K\mathbb{Q}(n)$ throughout, where K is any number field, and defines an Euler system over K to be a family (y_n) with $y_n \in K\mathbb{Q}(n)$ such that the norm relation (2) holds and a certain congruence condition (which we do not spell out) holds as well. For details we refer to the literature, e.g. [Ru]. In any case, definitions of Euler systems, even in this explicit form, vary slightly. In many applications, the range of n is restricted; e.g. one asks that all prime divisors $l|n$ are congruent to 1 modulo a large M that was previously fixed. Historically and didactically the foremost application is the following (cf. [Th]):

Theorem 2.3.2. (THAINE) *Let $K = \mathbb{Q}(\zeta_{n_0})^+$ and \tilde{C}_K the set of units y in K that “start an Euler system”, that is, for which an E.S. (y_n) exists with $y_1 = y$. Then for any $a \in \mathbb{Z}[\text{Gal}(K/\mathbb{Q})]$ that annihilates the quotient $E(K)/\tilde{C}_K$, the element $2a$ annihilates the class group Cl_K . □*

In practice, one knows that every cyclotomic unit starts an Euler system, and one surmises that no other unit does. A class group that is known to be annihilated by something might still be large if it requires a lot of generators. Therefore the following theorem ([Ko], [Ru]) is much stronger and also a lot harder to prove; but is it precisely here that Euler systems show their full strength, and the main point is the construction of so-called Kolyvagin elements out of the Euler system.

Theorem 2.3.3. (KOLYVAGIN, RUBIN) *Let K be as above, $G = \text{Gal}(K/\mathbb{Q})$ and p a prime not dividing $[K : \mathbb{Q}]$. Then for all p -adic characters χ of G , the order of $Cl_K\{p\}_\chi$ divides the order of $(E(K)/\tilde{C}_K)\{p\}_\chi$. □*

By a suitable passage to the limit, this actually yields a proof of the second form of the Main Conjecture for K and the primes p that do not divide the degree of K . It is interesting to note that the proof of Mazur and Wiles (which came first) works by showing that A_χ is not too small, and the proof via Euler systems does just the opposite, providing an upper bound. In both proofs, one passes from an inequality to an equality with the help of the analytic class number formula.

Nowadays the definition given above is just a special case of a broader scenario which we will sketch (cf. [Ru1], [PR]). Let K be a number field, T a finitely generated free \mathbb{Z}_p -module with a continuous action of $\text{Gal}(\bar{K}/K)$ (a “ p -adic Galois representation”). One defines a submodule $\text{III}(T)$ of $H^1(K, T \otimes (\mathbb{Q}/\mathbb{Z}))$ by “local conditions”. A family of elements

$y_n \in H^1(K(n), T^\vee(1))$ which satisfies analogs of condition (2) and (3) will be called an Euler system. (Here $T^\vee(1) = \text{Hom}(T, \lim \mu_{p^n})$ is a kind of dual to T .) As in the ‘‘classical’’ case, the Euler system produces so-called Kolyvagin elements $\kappa_n \in H^1(K, T \otimes \mu_{p^N})$ (for some previously fixed N), and these give annihilators for $\text{III}(T)$. We will just indicate how this specializes back to the above cyclotomic setting, upon making the appropriate choice for T : take $T = \mathbf{Z}_p$ with trivial action of $\text{Gal}(\bar{K}/K)$. Then

$$\text{III}(T) = H^1(\text{Gal}(K_{unr}/K), \mathbf{Q}_p/\mathbf{Z}_p) = \text{Hom}(\text{Gal}(K_{unr}/K), \mathbf{Q}_p/\mathbf{Z}_p),$$

with K_{unr} the maximal unramified extension of K . Thus $\text{III}(T)$ is, by global class field theory, dual to $Cl_K\{p\}$. The Euler system then lives in

$$H^1(K(n), T^\vee(1)) = H^1(K(n), \mathbf{Z}_p(1)) \cong K(n)^* \otimes_{\mathbf{Z}} \mathbf{Z}_p,$$

the isomorphism coming from Kummer theory. The Kolyvagin elements live in

$$H^1(K, T \otimes \mu_{p^N}) = H^1(K, \mu_{p^N}) = K^*/K^{*p^N},$$

and they provide principal ideals, that is, annihilators for the class group, by looking at their factorization into prime ideals.

Another very important case is where T is the Tate module $T_p(E)$ of an elliptic curve. Here it is worth remarking that $T^\vee(1) \cong T$ via the Weil pairing.

We present a variant at infinite level of the Euler system of cyclotomic units (including a certain twist), because this gives a nice link to Iwasawa theory, and will be needed later in the conference. The reader unfamiliar with Tate twists should take $r = 1$ in the following and be reminded that $H^1(K, \mathbf{Z}/p^n\mathbf{Z}(1)) = H^1(K, \mu_{p^n})$ is canonically isomorphic to K^*/K^{*p^n} . We fix m prime to p . For every $n \in \mathbb{N}$ and arbitrary r in \mathbf{Z} one then has an element

$$\begin{aligned} z_{m,n}^{(r)} &:= (1 - \zeta_{mp^n}) \otimes (\zeta_{p^n})^{\otimes(r-1)} \in H^1(\mathbf{Q}(mp^n), \mathbf{Z}/p^n\mathbf{Z}(1)) \otimes (\mathbf{Z}/p^n\mathbf{Z})^{\otimes(r-1)} \\ &\cong H^1(\mathbf{Q}(mp^n), \mathbf{Z}/p^n\mathbf{Z}(r)) \end{aligned}$$

(one may pull in the term $(\mathbf{Z}/p^n\mathbf{Z})^{\otimes(r-1)}$ since the absolute Galois group of $\mathbf{Q}(mp^n)$ acts trivially on it). One moreover has a corestriction map

$$\text{cor} : H^1(\mathbf{Q}(mp^n), \mathbf{Z}/p^n\mathbf{Z}(r)) \rightarrow H^1(\mathbf{Q}(m), \mathbf{Z}/p^n\mathbf{Z}(r)).$$

For $r = 1$ this corresponds to the norm map. The elements $\text{cor}_n(z_{m,n}^{(r)})$ are compatible under the obvious transition maps induced by $\mathbf{Z}/p^n\mathbf{Z} \rightarrow \mathbf{Z}/p^{n-1}\mathbf{Z}$, and they define an element

$$C_r(m) = \lim_n \text{cor}_n(z_{m,n}^{(r)}) \in H^1(\mathbf{Q}(m), \mathbf{Z}_p(r)).$$

For varying m (and constant r), these elements satisfy the following Euler relation: Let l be prime to p and m . Then (in additive notation)

$$\text{cor}_{\mathbb{Q}(lm)/\mathbb{Q}(m)}(C_r(ml)) = (1 - l^{r-1}F_l^{-1})C_r(m).$$

Note that this is very similar to an earlier formula in case $r = 1$.

III. Cohomology of Iwasawa modules

§1 — *Fitting ideals and cohomological triviality*

The main purpose of this section is to consider Λ -modules which have an extra action by a group G (usually a group of automorphisms of the base field K) that commutes with the Λ -structure, so we are simply dealing with $\Lambda[G]$ -modules. Since G is finite one may identify $\Lambda[G]$ also with the profinite group ring $\mathbb{Z}_p[[\Gamma \times G]]$ (we have not covered this construction; see [NSW]).

For the moment let R be any noetherian commutative ring. Let us agree that all R -modules are supposed to be finitely generated. The (first) Fitting ideal of an R -module M is defined as follows: take a free resolution $R^m \xrightarrow{\alpha} R^n \rightarrow M \rightarrow 0$, and let $\text{Fit}_R(M)$ be the R -ideal generated by all the $n \times n$ minors of the $n \times m$ -matrix that represents α . Obviously one must prove something:

Proposition 3.1.1. *The definition of Fit_R is independent of the choice of resolution.*

Sketch proof: It suffices to show that Fit_R is unchanged when one throws in one more generator (n goes up by one) and correspondingly one more relation (the new generator expressed in terms of the old ones, and m also increases by one). The matrix thus grows by one row and one column; the new column at the right is zero, except the corner element which is 1. From here it is an easy matter to compare the minors. \square

It is obvious that for $m < n$ there are no minors of the required format and thus the Fitting ideal is zero. Another very important example is $M = R/I$; here one chooses the obvious generator $\bar{1}$ of M , the matrix degenerates to one row, containing a list of generators of I , so $\text{Fit}_R(R/I) = I$. It is also easy to check that $\text{Fit}_R(M \oplus N) = \text{Fit}_R(M)\text{Fit}_R(N)$, but unfortunately Fit_R does not behave well on non-split short exact sequences.

Now suppose R is local and reduced (so its localization at the set of all nonzerodivisors is a finite product of fields), and M is an R -torsion module of projective dimension ≤ 1 . (We recall: $pd_R(M)$ is the least integer d , if it exists, such that in

any projective resolution of length d , $0 \rightarrow C \rightarrow P_d \rightarrow \cdots \rightarrow P_1 \rightarrow M \rightarrow 0$, the module C is projective. This is well-defined; $pd_R(M) = 0$ iff M is itself projective; and over a Dedekind ring R always $pd_R(M) \leq 1$. A good reference on projective dimension of modules is Chapter VII of [Kz].) If we now look at a resolution $0 \rightarrow C \rightarrow R^n \rightarrow M \rightarrow 0$, then C is again free, and for reasons of rank $C \cong R^n$. In other words, M is the cokernel of the multiplication by an $n \times n$ matrix A on R^n , and $\text{Fit}(R)$ is simply the principal ideal generated by $\det(A)$. Often, knowledge of this principal ideal is already quite satisfactory.

We recall the following definition (a good reference on this is Serre's classic [Se]). Let G be a finite group, and M be a G -module (equivalently: a $\mathbb{Z}[G]$ -module). Then M is cohomologically trivial (c.t.) if for all subgroups $U \subset G$ and for all $q \in \mathbb{Z}$, the Tate cohomology $\hat{H}^q(U, M)$ is zero. It suffices to have this nullity for two consecutive indices $q, q+1$ and all U . Projective $\mathbb{Z}[G]$ -modules are c.t.; in fact if $R = S[G]$ with S a Dedekind ring and G a finite group, then an R -module is c.t. (as G -module) if and only if it has finite projective dimension over R ; and if that is so, the projective dimension is at most 1. One gets the following analog in dimension 2, cf. [Gr3]:

Proposition 3.1.2. *Let $R = \Lambda[G]$ and M an R -module.*

- (1) *M is G -c.t. iff M has finite projective dimension over R .*
- (2) *If $pd_R(M) < \infty$ then $pd_R(M) \leq 2$.*
- (3) *If G is abelian, M is G -c.t. and has no nonzero finite Λ -submodules, then $pd_R(M) \leq 1$.*

Proof: (1) "If" is easy. Suppose M is c.t. over G ; pick a resolution of length 2 of M and let C be the kernel on the left. Since the ring Λ is regular of dimension 2, C is projective (actually free) over Λ . Of course C is again G -c.t. By Cor.5.2.20 in [NWS], C is projective over R as desired.

(2) This can be extracted from the proof of 1. For abelian G one may also reason as follows: it is a general fact that as soon the projective dimension of M is finite, it never exceeds the Krull dimension of R , and the difference $\dim(R) - pd_R(M)$ is the so-called depth of M , by the theorem of Auslander-Buchsbaum. This will be needed in the next argument.

(3) To simplify we assume G is a p -group. Then R is local. We know that $pd_R(M)$ is finite. If it were 2, then by Auslander-Buchsbaum, the depth of M would be zero. By definition, the depth is the maximal length of a sequence $x_1, x_2, \dots \in \text{rad}(R)$ such that x_1 acts injectively on M , x_2 acts injectively on M/x_1M , etc. Now if M has no nonzero finite submodule over Λ , the structure theorem shows that M embeds into a direct sum of modules $\Lambda/(\pi_i^{e_i})$. It is easy to see that some $0 \neq f \in \Lambda$ acts injectively

on that direct sum, so the depth of M is at least one, and we are done. \square

§2 — Calculating Fitting ideals of cohomologically trivial Iwasawa modules

We retain the notation $R = \Lambda[G]$ from above. The usefulness of having a module M over R of finite projective dimension is twofold. First, the Fitting ideal of M carries a lot of information (more than in the general case); more precisely, it determines the class of M in a suitable K -group. Second, the Fitting ideal is easier to calculate than in the general case. This is explained by the following result whose idea can be traced back to Wiles. (For the short proof we refer to [Gr2] p.118. Actually a more general statement holds.)

Proposition 3.2.1. *Suppose G is an abelian group, and $R = \Lambda[G]$ as before. Suppose moreover we are given two principal ideals I and J of R . Then $I = J$ iff this equality holds in codimension 1, that is, iff $I_{\mathfrak{p}} = J_{\mathfrak{p}}$ for all height one prime ideals of R . (Note that for $G = 1$, that is $R = \Lambda$, the height one primes are just the principal primes. Note also that the result would be totally false for nonprincipal I and J .) \square*

We now explain the principal application of this in Iwasawa theory. The setup is the following: K/F is a Galois extension with abelian Galois group G , and K_{∞} is the cyclotomic \mathbf{Z}_p -extension. We assume for simplicity that K_{∞} is the disjoint compositum of K and F_{∞} , so $G_{\infty} = \text{Gal}(K_{\infty})$ is identified with $\Gamma \times G$. All standard Iwasawa modules M are then even modules over $R = \Lambda[G]$. A slight extra hypothesis is needed: Assume that F is totally real and K is CM, that is, imaginary and quadratic over a totally real subfield. Then G contains a uniquely defined complex conjugation, written j .

We have to discuss characters of G now: we consider characters $\chi : G \rightarrow \overline{\mathbf{Q}}_p$, and contrary to an earlier situation, we do allow that p divides $|G|$. Thus one has to be careful when defining eigenspaces, and we choose the “coinvariant” way: let

$$M_{\chi} = \mathbf{Z}_p[\chi] \otimes_{\mathbf{Z}_p[G]} M.$$

The functor $M \mapsto M_{\chi}$ is right exact, and exact if χ has order prime to p . Let us now call a height one prime \mathfrak{p} of R singular if it contains p . One can show: the nonsingular primes \mathfrak{p} correspond to pairs (χ, f) with f a prime element of $\Lambda(\chi)$ not associated to p , and $M_{\mathfrak{p}}$ is canonically isomorphic to M_{χ} localized at f . The Main Conjecture, as proved by Wiles for p odd and F totally real, shows that for odd characters χ the characteristic polynomial of A_{χ} equals f_{χ} time a unit, where again $f_{\chi} \in \Lambda(\chi)$ is given in terms of L-functions and A is the standard Iwasawa module attached to K . Let us therefore assume p odd in the sequel.

Remarks:(1) One thing we have not said is important here: the whole theory of Λ -modules goes through without a hitch for $\Lambda(\chi)$ -modules. The only change is that \mathbb{Z}_p is replaced by $\mathbb{Z}_p(\chi)$ which is a DVR just as well.

(2) In [Wi] the p -power dividing the characteristic polynomial (the so-called μ -invariant, that is) is only partly determined. This is not a problem since the general case follows; see the discussion on p. 657 of [NSW].

The Main Conjecture thus tells us that the Fitting ideal of $A_{\mathfrak{p}}$ is known for all nonsingular \mathfrak{p} of height one. As the Main Conjecture (first form) is totally concentrated in the minus part, we replace A by A_- which is by definition $A/(1+j)A$. Many authors prefer $A^- = \ker(1+j : A \rightarrow A)$ but it really does not matter since $p \neq 2$.

Suppose now that A_- has projective dimension at most one over R (let us worry later just when this happens, and what to do if not!) and call this: Assumption (1). Then $\text{Fit}_R(M)$ is a principal ideal, generated by $F \in R$, say. Make now the following assumption (2):

There exists $\Phi \in R$ such that the image of Φ under χ equals f_χ times a unit, for every odd character χ of G .

Under these hypotheses, the localizations of the principal ideals (F) and (Φ) at every nonsingular prime coincide. Of course one would like to infer that $(F) = (\Phi)$ in the minus part; this would be an equivariant version of the Main Conjecture. One situation where this is possible is the following:

Theorem 3.2.2. *Assume (1) and (2). If $\mu(A_-) = 0$ (this means A_-/pA_- is finite), then $(F) = (\Phi)$ in $R_- = R/(1+j)$.*

The proof is fairly short: it suffices to show that $(F)_{\mathfrak{p}} = (\Phi)_{\mathfrak{p}}$ for the singular primes \mathfrak{p} as well, and one just goes ahead and proves that both sides are the unit ideal. For (F) this is almost obvious since \mathfrak{p} contains p . For (Φ) one needs the Main Conjecture again; see the proof of Lemma 3.7 in [Gr3].

If K is absolutely abelian, then indeed $\mu(A) = 0$ (even without the minus) as said in I.4. In general this is not known and one needs more in order to prove $(F) = (G)$. It is not hard to show [Gr3] that under the same assumptions as in 3.2.3, without $\mu(A) = 0$, the inclusion $(F) \subset (G)$ implies equality.

We now proceed in the most obvious fashion: first (§3) we discuss when the standard Iwasawa modules A and X (see I.4) are, by good luck, of f.p.d., and then (§4) let us worry what can be done in the other case, which is the prevailing one.

§3 — *Cases where the standard Iwasawa module is already c.t.*

We build on Prop. 3.1.2 and resume the setup K/F and G from the last subsection, assuming that F is totally real and K is CM, that is, imaginary and quadratic over a totally real subfield. Then G contains a uniquely defined complex conjugation, written j ; and we are interested in the Iwasawa module A_- which is the projective limit of the $(A_n)_-$. The following lemma can be considered as obvious since passing to the limit is an exact functor on systems consisting of finite modules:

Lemma 3.3.1. *If all $(A_n)_-$ are G -c.t. then so is A_- . \square*

So it suffices to worry about $(A_n)_-$ for all n . We give a slightly adapted version of [Gr3] here; essentially all this goes back to Schoof [Sch].

Theorem 3.3.2. *Suppose that for every prime \mathfrak{p} that ramifies in K/F the decomposition group $G_{\mathfrak{p}}$ contains j (the complex conjugation) and that the module $\mu(K)\{p\}$ is G -c.t. Then $Cl(K)\{p\}_-$ is cohomologically trivial over G . \square*

Since one can show that the stated hypotheses are inherited by all K_n/F_n , one gets that A_- is c.t. by invoking Lemma 3.3.1. It is now a well-known result (Prop.13.28 in [Wa]) that A_- has no finite Λ -submodules, so 3.1.2 (3) shows that $pd_R(A_-)$ is at most 1 as soon as A_- is G -cohomologically trivial. We sum up:

Corollary 3.3.3. *Under the same hypotheses as in Thm. 3.3.2 we have $pd_R(A_-) \leq 1$. \square*

Recall that this conclusion was dubbed Assumption 1 in the last subsection. It is now rather satisfactory that the same hypotheses also imply hypothesis 2, and the proof of this is routine. We thus get:

Corollary 3.3.4. *Assume the hypotheses of 3.3.2, and that $\mu(A_-) = 0$. Then $\text{Fit}_R(A_-) = (\Phi)$. \square*

A simple class of examples to which 3.3.2 applies is given by extensions K/F in which only one prime ramifies, and it ramifies totally, with the extra condition that $\zeta_p \notin K$. If one assumes e.g. K absolutely abelian on top of this, one also gets the statement 3.3.4.

It is equally possible to look at the Iwasawa module X . Here it can be shown that X is c.t. (“outside the trivial character”) if K is for example totally real of prime power conductor over $F = \mathbb{Q}$. (For the precise statement see [Gr2] p.126.) A generalization of this to the case of two primes dividing the conductor, with additional hypotheses on split ramified primes, can be found in [Bl-Bu].

One main application of this kind of Iwasawa theory is to prove the Brumer conjecture for suitable abelian Galois extension K/F . For details we again refer to [Gr3].

§4 — *How to produce replacements that are cohomologically trivial*

Here we discuss the general case where one should not expect the Iwasawa modules A or X to be cohomologically trivial. Such a situation already comes up at bottom level: for instance, the p -part of the class group $A(K)$ is usually not of finite p.d. over $\mathbb{Z}[G]$. The point is now, very roughly speaking, to associate c.t. modules to non c.t. modules in as canonically a fashion as possible. The first such construction (which is still extremely important) is due to Chinburg. Given K/F G -Galois and using an approach of Tate one sets up a four-term exact sequence

$$0 \rightarrow C_S(K) \rightarrow A \rightarrow B \rightarrow \mathbb{Z} \rightarrow 0,$$

where A and B are c.t. over G (actually one may take B to be torsion-free, hence $\mathbb{Z}[G]$ -projective), and the so-called S -idele class C_S is a close relative of X at bottom level, more precisely: via class field theory C_S is isomorphic to the Galois group of the maximal p -abelian S -ramified extension of K , with S a finite set of places of K which is “large enough” in a technical sense. Among other things S must contain all ramified primes. (We are cheating here a little: actually $C_S(K)$ has to be replaced by a module of finite type in such a way that the cohomology does not change.)

The link between C_S (the “natural” module) and the c.t. modules A and B may appear tenuous — the first thing that hits the eye that one has two, and of course one wants just one module. The way out is that one takes the difference $[A] - [B]$ in the K-group of (f.g.) projective $\mathbb{Z}[G]$ -modules later on. The truly crucial point is well-definedness of A and B , or much more reasonably, of their “difference” $[A] - [B]$. This happens, miraculously, if one imposes the extra condition that the class of the 2-extension above agrees with a class coming from global class field theory (the canonical class). The so-called 3rd Chinburg conjecture for abelian G states that if one adds just this requirement then $[A] - [B]$ is zero; note that via projective resolutions, the classes $[A]$ and $[B]$ make sense even if A and B are just of finite p.d., not themselves projective. It is now reasonable to pass to the limit in the Iwasawa tower with the above 2-extension, after p -adic completion; let X_S stand for the p -completion of $C_S(K)$. This has been done by Ritter and Weiss [R-W], after making the extension more concrete. We now explain this: fix an abelian G -Galois extension K/F . Later K will be replaced by K_n and G by $\text{Gal}(K_n/F)$.

In [R-W] one puts $B = \mathbb{Z}_p[G]$ and the map $B \rightarrow \mathbb{Z}_p$ equal to the augmentation map. It remains therefore to exhibit an extension

$$0 \rightarrow X_S \rightarrow A \rightarrow I_G \rightarrow 0,$$

where $I_G = \langle \sigma - 1 : \sigma \in G \rangle$ is the kernel of the augmentation (written ΔG in loc.cit.). Now there is a canonical construction which translates extensions of $\mathbb{Z}_p[G]$ -modules

as above into group extensions $X_S \subset E \twoheadrightarrow G$, and the point is that a canonical such extension is available, given by the canonical class, provided S is large enough. Still better, one can write down E : just take the Galois group of the maximal S -ramified l -extension of K over F . (If we take it over K , we get back X_S , and usually E is not abelian, contrary to X_S .) The fact that this E does give the canonical class $c_{K/F}$ is a theorem of Shafarevich (cf. [Sh] and [We] p.306f.). One gets then that the above 1-extension, when prolonged to a 2-extension via $0 \rightarrow I_G \rightarrow \mathbb{Z}_p[G] \rightarrow \mathbb{Z}_p \rightarrow 0$, gives indeed the correct class required by Chinburg's theory. Another benefit is that A if constructed from E via the translation functor has finite p.d. over $\mathbb{Z}_p[G]$. (In another parlance, A is called the splitting module of $c_{K/F}$; see [NSW] p.115.)

Since we do not want to anticipate the talks of Ritter and Weiss, let us just briefly indicate what happens next: one considers the above sequence with K replaced by K_n , for every n , and in the limit one obtains

$$0 \rightarrow X_{S,\infty} \rightarrow A_\infty \rightarrow I_{G_\infty} \rightarrow 0$$

where $G_\infty = \text{Gal}(K_\infty/F)$. One proves that A_∞ has p.d. at most 1 over $R = \mathbb{Z}_p[[G_\infty]]$. Unfortunately A_∞ is not torsion over R ; in [R-W] the next step is to mod out a free cyclic R -submodule $\text{Im}(\Psi)$, which leads to a torsion module $A_\infty/\text{Im}(\Psi)$. An Equivariant Main Conjecture is then, quite roughly speaking, the following statement

$$\text{Fit}_R(A_\infty/\text{Im}(\Psi)) = (\Theta_S) \cdot \delta_\Psi,$$

where Θ_S , an element of the full ring of quotients of R , is constructed via L -values (this is closely related to the element whose existence is stated in Assumption 2, but much more general), and δ_Ψ is a correction term, depending on Ψ in a straightforward manner. For more on this we refer to the preprint [R-W] and the relevant talks at this conference.

We now briefly discuss a second approach which is actually much more encompassing than the first one (which evolved independently but can be seen as closely related to the second approach, cf. [Bu3]). This second method uses complexes and cohomology (the latter being involved in an even more crucial way than in methods discussed previously). It is mainly due to Burns and Flach ([Bu-F1], [Bu-F2], [Bu1], [Bu2]) and was applied in an Iwasawa theoretic context in [Bu-Gr]. We will try to indicate the technique that was used there, with the objective of proving the so-called equivariant Tamagawa number conjecture (ETNC) for Tate motives $h^0(\text{Spec}K)(r)$ at an odd prime p for an absolutely abelian base field K . Let us note in passing that ETNC for the "simplest" case $r = 0$ is equivalent to the Lifted Root number conjecture of Gruenberg, Ritter and Weiss; this is a theorem of Burns ([Bu1]). For simplicity let us assume that K is real.

A free rank one R -module Δ is constructed which is essentially the determinant of a perfect complex C . This is a bounded complex which consists of finitely generated cohomologically trivial R -modules, with no condition on the differentials. More honestly though, one has to work in the derived category, so a complex is perfect iff it is quasi-isomorphic to a bounded complex of f.g.c.t. modules. This notion of quasi-isomorphism is unrelated to that of Part I; a morphism between two complexes is a q.i. iff it induces isomorphisms from the cohomology groups of the first complex to the ones of the second complex.

The cohomology groups of this complex are arithmetical entities, more precisely, Iwasawa modules of the types seen in Part I. One then constructs an isomorphism λ from $Q \otimes_R \Delta$ to Q , where Q is the full quotient ring of R . This isomorphism comes from knowledge of the cohomology of C , and over Q splitting is possible, that is, the determinant of a complex is equal to the determinant of its cohomology (considered as complex with zero differential). The main result is then ([B-G] Thm. 6.1):

The image of Δ under λ is exactly R .

This is proved by localization arguments similarly as in §2. For regular primes \mathfrak{p} of R , $R_{\mathfrak{p}}$ is a PID, and again splitting arguments are possible so we may apply results of standard Iwasawa theory, bearing on the cohomology modules. For the singular primes \mathfrak{p} , one shows that the localized complex $C_{\mathfrak{p}}$ is acyclic (i.e., all its cohomology groups vanish). This proof involves showing that various μ -invariants are zero; and the acyclicity is again enough to show that $\lambda(\Delta_{\mathfrak{p}})$ equals $R_{\mathfrak{p}}$. The final touch of the argument is then to invoke Prop. 3.2.1. The talk of D. Burns at this conference presented generalizations of this approach, yielding some results over number fields which are not abelian over \mathbb{Q} .

The approach just discussed is closely related to the Bloch-Kato conjectures. Actually there is a recent preprint [H-K] of A. Huber and G. Kings which states and proves a Main conjecture for arbitrary Dirichlet characters, along with the Bloch-Kato conjecture for these characters. The precise relation of this work to [Bu-Gr] and also to the Equivariant Main Conjecture of [R-W] is not yet clear, but presumably there does exist a fairly close connection.

References

- [Bl-Bu] W. BLEY, D. BURNS, Equivariant Tamagawa Numbers, Fitting Ideals and Iwasawa Theory, *Compositio Math.* **126** (2001) 213-247
- [Bu1] D. BURNS, Equivariant Tamagawa numbers and Galois module theory I, to appear in *Comp. Math.*

- [Bu2] D. BURNS, Equivariant Tamagawa numbers and Galois module theory II, preprint 1998
- [Bu3] D. BURNS, On Tamagawa numbers, p -adic zeta functions and Galois groups, preprint 2001
- [Bu-F1] D. BURNS, M. FLACH, Motivic L-functions and Galois module structures, *Math. Ann.* **305** (1996), 65-102
- [Bu-F2] D. BURNS, M. FLACH, Equivariant Tamagawa numbers for motives, preprint 1999
- [Bu-Gr] D. BURNS, C. GREITHER, On the equivariant Tamagawa number conjecture for Tate motives, preprint 2000
- [Co1] R. COLEMAN, Division values in local fields, *Invent. Math.* **53** (1979), 91-116
- [Co2] R. COLEMAN, Local units modulo circular units, *Proc. AMS* **89** (1983), 1-7
- [Gr1] C. GREITHER, Normes universelles dans les \mathbf{Z}_p -extensions, *J. Th. Nombres Bordeaux* **6** (1994), 205-220
- [Gr2] C. GREITHER, The structure of some minus class groups, and Chinburg's third conjecture for abelian fields, *Math. Zeitschrift* **229** (1998), 107-136
- [Gr3] C. GREITHER, Some cases of Brumer's conjecture for abelian CM extensions of totally real fields, *Math. Zeitschrift* **233** (2000), 515-534
- [H-K] A. HUBER, G. KINGS, Bloch-Kato conjecture and main conjecture of Iwasawa theory for Dirichlet characters, preprint 2000
- [Ko] V. A. KOLYVAGIN, in: *The Grothendieck Festschrift (Vol. II)*, P. Cartier et al. eds., Progress in Math. 87, Birkhäuser, Boston 1990
- [Ku] L. V. KUZ'MIN, The Tate module for algebraic number fields, *Math. USSR Izvestiya* **6** (1972), 263-321
- [Kz] E. KUNZ, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, Boston 1989
- [M-W] B. MAZUR and A. WILES, Class fields of abelian extensions of \mathbf{Q} , *Invent. Math.* **76** (1984), 179-330
- [NSW] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG, *Cohomology of number fields*, Grundlehren 323, Springer 2000
- [OSS] C. OKONEK, M. SCHNEIDER, H. SPINDLER, *Vector bundles on complex projective spaces*, Progress in Math. **3**, Birkhäuser 1980
- [R-W] J. RITTER and A. WEISS, The lifted root number conjecture and Iwasawa theory, preprint 2000
- [Ru] K. RUBIN, The main conjecture, appendix to: *Cyclotomic fields I and II (combined second edition)*, by S. Lang, GTM 121, Springer, New York 1990
- [Ru1] K. RUBIN, *Euler systems*, Princeton University Press, Princeton 2000
- [Sch] R. SCHOOF, Minus class groups of the fields of the l -th roots of unity, *Math. Comp.* **67** (1998), 1225-1245
- [Se] J-P. SERRE, *Cohomologie galoisienne*, Springer Lecture Notes in Math. **5**, Springer

1964 (5th edition)

- [Sh] I. R. SHAFAREVICH, On Galois groups of y -adic fields, *Doklady Ak. Nauk USSR* **53** (1946), 15-16
- [Th] F. THAINE, On the ideal class groups of real abelian number fields, *Ann. of Math.* **128** (1988), 1-18
- [Wa] L. WASHINGTON, *Introduction to cyclotomic fields*, GTM 83, Springer 1982 (second edition 1996)
- [We] A. WEIL, *Basic number theory*, reprint of the 1973 edition, Springer 1995
- [W] A. WILES, The Iwasawa conjecture for totally real fields, *Ann. Math.* **131** (1990), 493-540