Classical Iwasawa Theory

B.J.H. Jansen

A detailed proof of a simple version of Iwasawa's theory assuming the structure theory for Λ-modules

This section is almost literally taken from the first three pages of Ralph Greenberg's article Past and Present, only that we give more details and that we restrict to one special case.

Let F be a number field. Let p be a prime number. Suppose that F_∞ is a Galois extension of F such that *there is only one prime in F above p and this prime is totally ramified in F_∞* (the part that is written curved is the special case we consider, this assumption is not necessary, so theorem 0.1 is true without this assumption, although in the proof of theorem 0.1 we will use the assumption) and that $\Gamma = \mathrm{Gal}(F_\infty/F)$ is isomorphic (as topological groups) to $\mathbb{Z}_p$. For example $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$.

The nontrivial closed subgroups of Γ are of the form $\Gamma_n = p^n\Gamma$ for $n \geq 0$. Indeed, suppose H is a closed subgroup of $\mathbb{Z}_p$. Let $x = p^i u$ ($u \in \mathbb{Z}_p^*$) be an element of $H - \{0\}$. Then we have $H \supset \overline{p^i\mathbb{Z}} = p^i\mathbb{Z}_p$, since we can multiply x by an truncation of u^{-1} and get as close to p^i as we wish. Now take i as small as possible then we also have $H \subset p^i\mathbb{Z}_p$, hence we have $H = p^i\mathbb{Z}_p$. Since Γ is isomorphic to $\mathbb{Z}_p$ we have that the nontrivial closed subgroups of Γ are of the form $\Gamma_n = p^n\Gamma$ for $n \geq 0$. These closed subgroups form a descending sequence and Γ/Γ_n is cyclic of order p^n. If we let $F_n = F_\infty^{\Gamma_n}$, then we obtain a tower of number fields

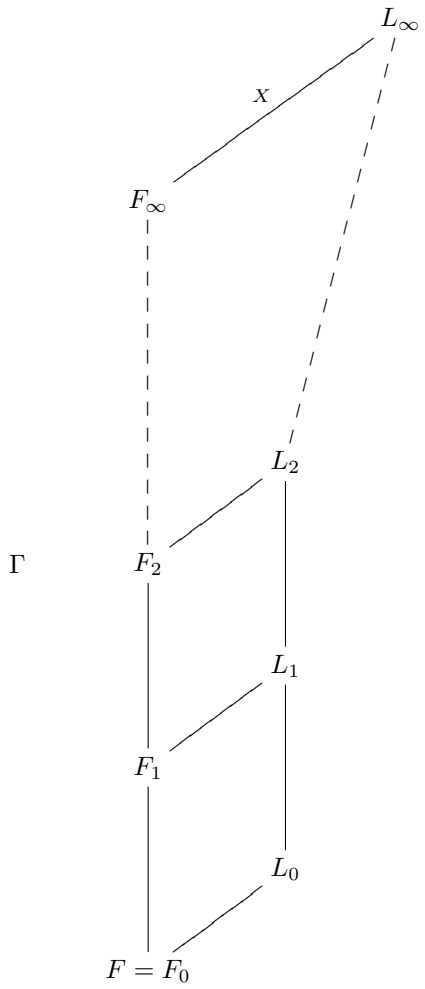
$$F = F_0 \subset F_1 \subset \ldots \subset F_n \subset \ldots$$

such that F_n/F is a cyclic extension of degree p^n and F_∞. We will prove the following theorem of Iwasawa.

Theorem 0.1 *Let p^{e_n} be the highest power of p dividing the class number of F_n. Then there exist integers λ, μ and ν such that $e_n = \lambda n + \mu p^n + \nu$ for all sufficiently large n.*

Iwasawa's proof of his theorem is based on studying the Galois group $X = \mathrm{Gal}(L_\infty/F_\infty)$, where $L_\infty = \bigcup_n L_n$ and L_n is the p-Hilbert class field of F_n. (Note that $L_n \subset L_{n+1}$ since we have that if $K \subset L$ are number fields then $H(K) \subset H(L)$, with $H(K)$ and $H(L)$ the Hilbert class field of K, L respectively.

Also recall that $\mathrm{Gal}(H(K)/K)$ is isomorphic to class group of K.)



The extension L_∞/F is Galois. Indeed, if we have a isomorphism σ of L_∞ to an other field (in a same algebraic closure of $\mathbb{Q}$) leaving F fixed, then $\sigma(L_\infty)$ over $\sigma(F_\infty) = F_\infty$ is unramified. Hence $\sigma(L_\infty)$ is equal to L_∞ by maximality of L_∞ (or the L_n's). We have an exact sequence of groups

$$0 \to X \to \mathrm{Gal}(L_\infty/F) \to \Gamma \to 0.$$

Since X is a projective limit of finite abelian p-groups, we can regard X as a topological compact $\mathbb{Z}_p$-module (namely we have $\mathbb{Z}_p \to \mathrm{End}(X) = \mathrm{End}(\lim X_i)$, where $X_i = \mathrm{Gal}(F_{infty}L_i/F_\infty)$ by sending z to $(z : (x_i)_i \mapsto (z \cdot x_i)_i)$). But there is also a natural action of Γ on X. If $\gamma \in \Gamma$ and $x \in X$, one defines $\gamma(x) = \tilde{\gamma} x \tilde{\gamma}^{-1}$, where $\tilde{\gamma}$ is a lift of γ to $\mathrm{Gal}(L_\infty/F)$. This is well-defined since if $\tilde{\gamma}'$ is another lift of γ then $\tilde{\gamma}^{-1}\tilde{\gamma}' = y \in X$ (because $\tilde{\gamma}^{-1}\tilde{\gamma}'|_{F_\infty = \mathrm{id}_{F_\infty}}$). Hence

since X is abelian we have $\tilde{\gamma}' x \tilde{\gamma}'^{-1} = \tilde{\gamma} y x y^{-1} \tilde{\gamma}^{-1} = \tilde{\gamma} x \tilde{\gamma}^{-1}$. And since X is normal in $\mathrm{Gal}(L_\infty/F)$ we have $\gamma(x) \in X$. All of this structure allows Iwasawa to study the growth of $[L_n : F_n] = p^{e_n}$.

Proof of theorem 0.1.

First we will prove that the number of elements of X modulo the commutator subgroup of $\mathrm{Gal}(L_\infty/F_n)$ is equal to e_n. Then we will prove that X is a Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$, and we will apply the structure theory for Λ-modules in order to calculate the number of elements of X modulo the commutator subgroup of $\mathrm{Gal}(L_\infty/F_n)$.

Lemma 0.2 *The only prime of F that is ramified in F_∞ is the prime above p.*

Let q be a prime in F not above p. Then q is tamely ramified and we can use the following theorem.

Theorem 0.3 *Let L/K be a finite abelian extension of number fields. If p is a prime of K tamely ramified in L, then the ramification index of p in the extension L/K divides $N(p) - 1$.*

Proof: Let q be a prime in L above p. By local class field theory we have the following commutative diagram

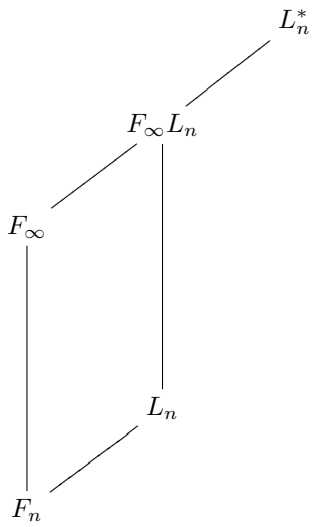
$$\begin{array}{ccc} K_p^*/N(L_q^*) & \longrightarrow & G_p \\ \uparrow & & \uparrow \\ U_0 N(L_q^*)/N(L_q^*) & \longrightarrow & I_p \end{array}$$

where the horizontal arrows are isomorphisms, the vertical arrows are inclusions and we define $U_i = 1 + (p)^i$ and $U_0 = U$ the units of the ring of integers A of K_p. Since $N(U_q^*) \subset U_0$ we have $U_0 N(L_q^*)/N(L_q^*) \simeq U_0 N(U_q^*)/N(U_q^*) = U_0/N(U_q^*)$. The reduction map $A \to A/p$ induces the map $U_0 \to (A/p)^*$ with kernel U_1. Since p is tamely ramified we know that $U_0 \supset N(U_q^*) \supset U_1$. Hence $\#I_p = \#U_0/N(U_q^*)$ divides $\#U_0/U_1 = \#(A/p) = N(p) - 1$.

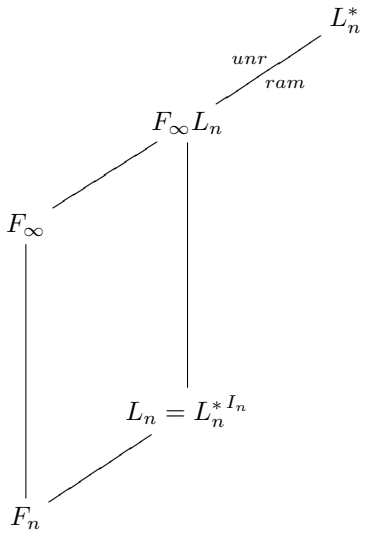
Using the theorem we see that the inertia group of q must be finite, but the only finite subgroup of Γ is 0. Hence q is unramified. This completes the proof of lemma 0.2.

Let L_n^* denote the maximal abelian extension of F_n contained in L_∞. We

want to show that $L_n^* = L_n F_\infty$. One inclusion ($\supset$) is obviously.

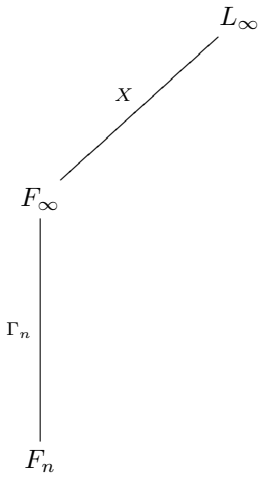


Let π_n be the unique prime above p in F_n (here we use the assumption). Let I_n be the inertia group of π_n in the extension L_n^*/F_n. Since L_n^*/F_n is only ramified at π_n we see that $L_n^{*\,I_n} = L_n$. On the other hand L_n^*/F_∞ is unramified since $L_n/F_\infty \cap L_n$ is unramified for every n. This gives us the following diagram.



Hence we get $L_n^* = F_\infty L_n$. And since $L_n \cap F_\infty = F_n$ we get $\mathrm{Gal}(L_n/F_n) \simeq \mathrm{Gal}(L_n^*/F_\infty)$ (Now we have put the information about the e_n's in X.). Because L_n^* is the maximal abelian extension of F_n in L_∞ we also have that the closure of the commutator subgroup of $G_n = \mathrm{Gal}(L_\infty/F_n)$ is equal to $\mathrm{Gal}(L_\infty/L_n^*)$.

Note that if we divide X out by the closure of this commutator subgroup then we get a group isomorphic to $\mathrm{Gal}(L_n/F_n)$, which is of primary interest.



Now we take a closer look at this commutator subgroup. We want γ_0 to be a topological generator of Γ, i.e. $\overline{\langle\gamma_0\rangle} = \Gamma$. It suffices to take γ_0 such that γ_0 restricted to F_1 is not the identity. Indeed, if we take such a γ_0 then the image, say c, of γ_0 is in $\mathbb{Z}_p^*$ (remember Γ is isomorphic to $\mathbb{Z}_p$). We can multiply c by a truncation of c^{-1} and get as close to 1 as we wish. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ it follows that c is a topological generator of $\mathbb{Z}_p$, hence γ_0 is a topological generator of Γ. Since the map Γ to $p^n\Gamma$ by sending x to $p^n x$ is an isomorphism of topological groups, we see that $\gamma_n = p^n\gamma_0$ is a topological generator of $p^n\Gamma$. Recall that we have an action of Γ_n on X.

Lemma 0.4 *The commutator subgroup of G_n is equal to $X^{\gamma_n - 1} = \{\gamma_n(x)x^{-1} | x \in X\}$.*

Proof (from Washington's cyclotomic fields page 278): First we will specify a lifting of $\gamma_n \in \Gamma_n$ to G_n. Let $\tilde{\pi}_n$ be a prime of L_∞ above π_n. Let $I_{\tilde{\pi}_n}$ be the inertia group of π_n. We have the natural maps $I_{\tilde{\pi}_n} \hookrightarrow G_n \twoheadrightarrow G_n/X$. This give us a natural map $I_{\tilde{\pi}_n} \twoheadrightarrow G_n/X = \Gamma_n$, which is injective since $X \bigcap I_{\tilde{\pi}_n} = \{e\}$ (by looking at ramification). This map is also surjective, since F_∞/F_n is totally ramified. Hence we have a specific isomorphism between $I_{\tilde{\pi}_n}$ and $G_n/X = \Gamma_n$. If we identify those two, then we get $G_n = I_{\tilde{\pi}_n}X = \Gamma_n X$. This gives us a specific lifting for $\gamma_n \in \Gamma_n$ to G_n.

Let $a = \alpha x$, $b = \beta y$, with $\alpha, \beta \in \Gamma_n$, $x, y \in X$ be arbitrary elements of $G_n = \Gamma_n X$. Then

$aba^{-1}b^{-1} =$
$ax\beta yx^{-1}\alpha^{-1}y^{-1}\beta^{-1} =$
$x^\alpha\alpha\beta yx^{-1}\alpha^{-1}y^{-1}\beta^{-1} =$
$x^\alpha(yx^{-1})^{\alpha\beta}(\alpha\beta)\alpha^{-1}y^{-1}\beta^{-1} =$

$x^\alpha(yx^{-1})^{\alpha\beta}(y^{-1})^\beta =$
$(x^\alpha)^{1-\beta}(y^\beta)^{\alpha-1}$.

Let $\beta = 1$ and $\alpha = \gamma_n$, then we find $y^{\gamma_n - 1} \in [G_n, G_n]$. Hence $X^{\gamma_n - 1} \subset [G_n, G_n]$.

To show that the other inclusion also holds, we will prove that $1-\beta$ and $\alpha - 1$ contain a factor $\gamma_n - 1$. We need a very important lemma, which we will also use later.

Lemma 0.5 *X is a $\mathbb{Z}_p[[\gamma_n - 1]]$-module.*

Proof: First we prove that each X_i is a $\mathbb{Z}_p[[\gamma_n - 1]]$-module. Clearly X_i is a $\mathbb{Z}_p[\gamma_n - 1]$-module. From the inclusion $(\gamma_n - 1)^{p^i} \subset (\gamma_n^{p^i} - 1, p)$ and the facts that the action of $\gamma_n^{p^i}$ is trivial on X_i and the action of (p) is nilpotent, it follows that the action of $(\gamma_n - 1)$ on X_i is nilpotent. Hench X_i is a $\mathbb{Z}_p[[\gamma_n - 1]]$-module. Now since the restriction maps from X_{i+1} to X_i are $\mathbb{Z}_p[[\gamma_n - 1]]$-lineair, it follows that X is a $\mathbb{Z}_p[[\gamma_n - 1]]$-module. This completes the proof.

Since γ_n is a topological generator we can find for every $\beta \in \Gamma_n$ an $c \in \mathbb{Z}_p$ such that $\beta = \gamma_n^c$. Hence

$$1 - \beta = 1 - \gamma_n^c = 1 - (1 + \gamma_n - 1)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} (\gamma_n - 1)^n \in (\gamma_n - 1)\mathbb{Z}_p[[\gamma_n - 1]].$$

(Note that the third equality holds, since it holds for the dense subset $\mathbb{N}$ of $\mathbb{Z}_p$ and both functions are continuous in c.) Let $a \in \mathbb{Z}_p[[\gamma_n - 1]]$ be such that $1 - \beta = (1 - \gamma_n)a$ and let $x' = x^\alpha$, then $(x^\alpha)^{(1-\beta)} = (x')^{(1-\gamma_n)a} = ((x')^a)^{\gamma_n - 1} \in X^{\gamma_n - 1}$, since $(x')^a \in X$. Similarly for $(y^\beta)^{\alpha - 1}$. Hence $[G_n, G_n] = X^{\gamma_n - 1}$. This completes the proof of lemma 0.4.

Now since $X^{\gamma_n - 1}$ is the image of the compact set X under the continues map $x \mapsto \gamma_n(x)x^{-1}$, it follows that $X^{\gamma_n - 1}$ is closed hence

$$\mathrm{Gal}(L_n/F_n) \simeq \mathrm{Gal}(F_\infty L_n/F_\infty) \simeq X/X^{\gamma_n - 1}.$$

By lemma 0.5 and setting $T = \omega_0$, where $\omega_n = \gamma_n - 1$, we can view X as an Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$. Then we can derive, after showing that X is a finitely generated and torsion as Λ-module, the number of elements of $X/\omega_n X$ from the following classification theorem for such Λ-modules.

Theorem 0.6 *If X is any finitely generated, torsion Λ-module, then there exists a Λ-module pseudo-isomorphism (i.e. finite kernel and cokernel)*

$$X \to \bigoplus_{i=1}^{t} \Lambda/(f_i(T)^{a_i}),$$

where each $f_i(T)$ is an irreducible element of Λ and each a_i is a positive integer for $1 \leq i \leq t$. The value of t, the prime ideals $(f_i(T))$, and the corresponding a_i's are uniquely determined by X, up to their order.

First we will show that we can apply theorem 0.6. We will use a version of Nakayama's lemma.

Lemma 0.7 *Let X be a compact Λ-module. Then X is finitely generated over Λ if and only if $X/(p,T)X$ is finite.*

Proof: See Washington's cyclotomic fields page 279.

Since X is closed in the compact product topology, we have that X is compact. Further we have $\#X/(p,T)X \leq \#X/TX \leq h_{F_0} < \infty$. Hence by lemma 0.7 X is finitely generated. Now we only have to show that X is a torsion Λ-module in order to apply theorem 0.6.

Lemma 0.8 *The Λ-module X is torsion.*

Proof: We know by lemma 0.7 that X is finitely generated, say X is generated by a_1, $a_2....a_n$. We also know that X/TX is finite, since $\#X/TX \leq h_{F_0} < \infty$. This two things imply that $p^m a_i = T(\sum_{j=1}^{n} \lambda_{ij} a_i)$. Doing this for all a_i together we get the following equation $M(a_i)_i = 0$, where M is the matrix $T(\lambda_{ij}) - p^m I$. Multiplying on both side by the adjoint matrix of M, we get that $\det(M)a_i = 0$. Since the constant term of the polynomial $\det(M)$ in T is non-zero, namely $(-p^m)^n$, and X is generated by the a_i's it follows that X is torsion. This completes the proof of the lemma.

So now we can apply theorem 0.6. This gives us

$$X \to \bigoplus_{i=1}^{t} \Lambda/(f_i(T)^{a_i}) = \bigoplus_{i=1}^{t} Y_i,$$

where $Y_i = \Lambda/(g_i(T)$, with $g_i(T) = f_i(T)^{a_i}$. The number of elements of $Y_i/\omega_n Y_i$ will give us the number of elements of $X/\omega_n X$.

Lemma 0.9 *The number of elements of $Y_i/\omega_n Y_i$ times $\prod_{\zeta^{p^n}=1} g_i(\zeta - 1)^{-1}$ is in $\mathbb{Z}_p^*$.*

Proof: The surjective map $\Lambda \to \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$ given by $T = \omega_0 - 1 \mapsto \omega_0 \mid_{F_n} -1$ has a kernel generated by ω_n. Hence $\Lambda/\omega_n\Lambda \simeq \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$. So $\Lambda/\omega_n\Lambda$ is a free $\mathbb{Z}_p$-module of rank $\#\mathrm{Gal}(F_n/F) = \#\mathbb{Z}/p^n\mathbb{Z} = p^n$. Multiplication by T on $\Lambda/\omega_n\Lambda$ is $\mathbb{Z}_p$-linear and has characteristic polynomial $\omega_n = (T+1)^{p^n} - 1$ with eigenvalues $\zeta - 1$, where $\zeta^{p^n} = 1$. Now $Y/\omega_n Y$ is the cokernel of multiplication by $g_i(T)$ on $\Lambda/\omega_n\Lambda$. This map is $\mathbb{Z}_p$-linear and his determinant is the product of the eigenvalues which is $\prod_{\zeta^{p^n}=1} g_i(\zeta - 1)$. This completes the proof of the lemma

Recall that Λ is a unique factorization domain. The irreducible elements of Λ are p and the irreducible polynomials of the form $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_0$, where $p|a_i$ for all $0 \leq i \leq n-1$ (polynomials of this form are called distinguished polynomials).

If $g_i(T) = p^m$ then we get $\#Y_i/\omega_n Y_i = (p^m)^{p^n} = p^{mp^n}$. If $g_i(T)$ is a distinguished polynomial $T^l + a_{l-1}T^{l-1} + ... + a_0$, then the valuation of $g_i(\zeta - 1)$ is the same as that of $(\zeta - 1)^l$ when ζ has sufficiently large order (the number of times p is divisible by $\zeta - 1$ increases if the order of ζ increases). Further we have $\langle \zeta_{p^{n+1}} \rangle = \langle \zeta_{p^n} \rangle \cup \{\zeta_{p^{n+1}}^i : i \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*\}$ as sets. And since $(\prod_{i \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*} (\zeta_{p^n}^i - 1)) = (p)$ we find that $\prod_{\zeta^{p^{n+}}} = 1(1-\zeta)^l = p^l \prod_{\zeta^{p^n}} = 1(1-\zeta)^l$, so we get $\#Y_i/\omega_n Y_i = p^{ln + constant}$ when $n \gg 0$. Hence the number of elements of $\bigoplus_{i=1}^t Y_i/\omega_n$ is equal to $\prod_{i=1}^t p^{k_i}$, where k_i is equal to $m_i p^n$ or $l_i n + constant_i$, when $n \gg 0$. This is equal to $p^{\lambda n + \mu p^n + constant}$.

Lemma 0.10 *Let X and Y be pseudo isomorphic Λ-modules. Let $w_n \in \Lambda$ be such that $w_n \mid w_{n+1}$ for all $n \in \mathbb{Z}_{\geq 0}$. If $X/w_n X$ is finite for all $n \in \mathbb{Z}_{\geq 0}$, then $\#X/w_n X = p^c \#Y/w_n Y$ for n big enough and some constant c.*

Proof: See Washington's Cyclotomic fields page 282.

Now since $\omega_n \mid \omega_{n+1}$ and X and $Y = \bigoplus_{i=1}^t Y_i$ are pseudo-isomorphic it follows from lemma 0.10 that $\#X/\omega_n X = p^{\lambda n + \mu p^n + \nu}$, where ν is a constant independent of n, for $n \gg 0$. Hence e_n is equal to $\lambda n + \mu p^n + \mu$ if $n \gg 0$. This completes the proof of theorem 0.1.

Remark 0.11 *If we define $f_X(T) = \prod_{i=1}^t f_i(T)^{a_i}$, then $\lambda = deg(f_X(T))$ and μ is the largest integer such that p^μ divides $f_X(T)$ in Λ.*

0.1 What about the constants

Is this section we will discus some of the results which are know about the constants in theorem 0.1. Again this is taken from Greenberg's Past and Present.

Theorem 0.12 *Assume that the class number of F is not divisible by p and that F has only one prime lying over p. Let F_∞/F be any $\mathbb{Z}_p$-extension. Then $\lambda = \mu = \nu = 0$.*

Proof: The assumption $p \nmid h_{F_0}$ implies that π_0 will ramify in F_1. Hence π_0 will totally ramify in F_∞. Now we are in the situation of or proof of theorem 0.1. So we know that $X/TX = 0$. Hence we get that $TX = X$. Using the fact that T is topological nilpotent we get $X = 0$, so $\lambda = \mu = \nu = 0$.

Result 0.13 *Assume that p splits completely in $F/\mathbb{Q}$. Let F_∞/F be a $\mathbb{Z}_p$-extension in which every prime of F lying over p is ramified. Then $\lambda(F_\infty/F) \geq r_2$, where r_2 denotes the number of complex primes of F*

We will now restrict to the special case where $F = \mathbb{Q}(\zeta_p)$ and $F_{infty} = \mathbb{Q}(\zeta_{p^\infty})$. If p is a regular prime then we know by by result 0.12 that $\lambda = \mu = \nu = 0$. For the irregular case we have the following. First we denote by h_p the class number of $F = \mathbb{Q}(\zeta_p)$ and by h_p^+ we denote the class number of $F^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Further we define $h_p^- = h_p/h_p^+$, i.e. $h_p = h_p^+ h_p^-$. A theorem

of Kummer says that $p \mid h_p^+$ implies $p \mid h_p^-$. Vandiver conjectured that $p \nmid h_p^+$. Iwasawa wrote in a paper of 1958 criteria for the non-vanishing of μ_p. He showed that for $p = 37$, 59, 67 we have $\mu_p = 0$ and $\lambda_p = 1$. Now it is known that $p \| h_p$ for these p.

Going back to the more general case where F is a number field. We make the following $\mathbb{Z}_p$-extension. We have $\mathrm{Gal}(\mathbb{Q}(\mu_p^\infty)/\mathbb{Q}) \simeq \mathbb{Z}_p^* = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. We define $\mathbb{Q}_\infty \subset \mathbb{Q}(\mu_p^\infty)$ to be the unique extension such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is $(1 + p\mathbb{Z}_p) \simeq \mathbb{Z}_p$. We set $F_\infty = F\mathbb{Q}_\infty$. We have the following conjectures and result about this so called cyclotomic $\mathbb{Z}_p$-extension.

Conjecture 0.14 *The μ of F_∞/F is equal to 0.*

We have the following result of Ferrero and Washington.

Result 0.15 *If $F/\mathbb{Q}$ is abelian then conjecture 0.14 holds.*

Greenberg came with the following conjecture.

Conjecture 0.16 *Suppose F is a totally real number field then $\lambda = 0$ and $\mu = 0$, i.e. the p-part of the class number of F_n is bounded as n goes to infinity.*

Inspired by the special case where F is Galois over $\mathbb{Q}$ and the special case where F is totally complex field and $\mathrm{Gal}(F/\mathbb{Q})$ is dihedral of order 2 times an odd number, the following was conjectured.

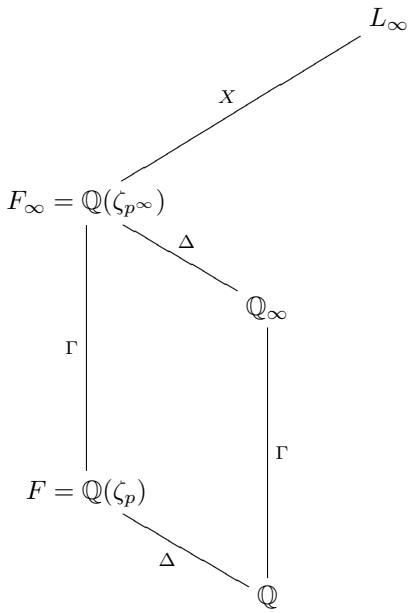
Conjecture 0.17 *Suppose F is a number field. Let $\tilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of F. Let $\tilde{L}$ denote the pro-p Hilbert class field of $\tilde{F}$ and let $\tilde{X} = Gal(\tilde{L}/\tilde{F})$, regarded as a module over the ring $\tilde{\Lambda} = \mathbb{Z}_p[[Gal(\tilde{F}/F)]]$. Then $\tilde{X}$ is a pseudo-null $\tilde{\Lambda}$-module.*

Where pseudo-null means that there are two relatively prime annihilators in Λ.

0.2 Iwasawa's main conjecture

In this section we will explain the main conjecture. Again this is taken from Greenberg's Past and Present.

We have the following setting.



We get an isomorphism of $G = \mathrm{Gal}(F_\infty/\mathbb{Q})$ with $\mathbb{Z}_p^*$ induced by the action of G on ζ_{p^∞}. Furthermore $G = \Gamma \times \Delta$ and maps to $\mathbb{Z}_p^* \simeq \mu_{p-1} \times \mathbb{Z}_p$ via coordinates. The field $\mathbb{Q}_\infty$ is the fix field of the closed subgroup Δ, i.e. the unique $\mathbb{Z}_p$ extension of $\mathbb{Q}$.

In the main conjecture two elements of Λ appear. Now we will describe the first one. Note that X is a $\mathbb{Z}_p[\Delta]$-module via lifting of an element of Δ. Also we have a character $\omega : \Delta \to \mu_{p-1} \subset \mathbb{Z}_p^*$, sending $(\sigma_a : \zeta_p \mapsto \zeta_p^a)$ to $\omega(a)$, where $\omega(a) = a$ modulo p in $\mathbb{Z}_p^*$. Hence we have an isomorphism $\mathbb{Z}_p[\Delta] \to \prod_{i=0}^{p-2} \mathbb{Z}_p$ by sending $\delta \in \Delta$ to $(\omega^i(\delta))_i$. This gives rise to a decomposition of X namely $X = \bigoplus_{i=0}^{p-2} X^{\omega^i}$, where $X^{\omega^i} = \{x \in X : \delta(x) = \omega^i(\delta)x \forall \delta \in \Delta\}$. We define $f_i(T)$ to be $f_{X^{\omega^i}}$ (see remark 0.11).

Now we will define the second element that appears in the main conjecture via a result. Let $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$ by sending $\lim_{\leftarrow}(\sigma_n : \zeta_{p^n} \mapsto \zeta_{p^n}^{i_n})$ to $\lim_{\to} i_n$.

Result 0.18 *Let i, j be integers such that $i + j \equiv 1(p-1)$. For every j even and $2 \leq j \leq p-3$ there exists a unique $g_i(T) \in \Lambda$ such that $g_i(\kappa(\gamma_0)^{1-m} - 1) = -(1 - p^{m-1})B_m/m$ for all $m \geq 1$ with $m + i \equiv 1(p-1)$. Furthermore we have $g_i(\kappa(\gamma_0)^s - 1) = L_p(s, \omega^j)$ for all $s \in \mathbb{Z}_p$, where L_p is the p-adic L-series.*

Now we state the main conjecture.

Conjecture 0.19 *For each odd i, $3 \leq i \leq p-3$, we have $(f_i(T))$ and $(g_i(T))$ are equal in Λ.*

Discussion

The main conjecture has been proved in a more general setting by Mazur and Wiles. Instead we take F to be a finite abelian extension of $\mathbb{Q}$. Further we define $\chi\psi = \omega$ with χ and ψ irreducible characters. Now we can attach to X^χ an element of Λ namely $f_\chi(T)$. Also there is a p-adic L-function $L_p(s,\psi)$ which corresponds to an element of Λ namely $g_\chi(T)$. The main conjecture has been proved in this general setting.

Kummer studied the divisibility of the class number of $\mathbb{Q}(\zeta_p)$ by p (since he was studying Fermat's Last Theorem). And he discovered that $p \mid h_{\mathbb{Q}(\zeta_p)}$ if and only if p divides numerator of at least one of the $S(-1)$, ... , $S(4-p)$, where $S(-n) = \prod_p (1-p^n)^{-1} = -\frac{B_{n+1}}{n+1}$ with n an odd integer. So kummer already related the Riemann zeta function with the p-part of the class group of $\mathbb{Q}(\zeta_p)$. If we know what the algebraic objects $f_i(T)$ are then we can easily derive the constants λ and μ (see remark 0.11). Now the main conjecture tells us that these algebraic objects are related to these analytical objects $g_i(T)$, which are analytical because they come from p-adic L-functions. So we can see the Main conjecture as an extension of Kummer's observation.

What we have done so far for say p-torsion on the circle, can also be done for p-torsion on elliptic curves. In the case where the elliptic curve has complex multiplication we have a analogical proof. The case where the elliptic curve doesn't have complex multiplication is open. But it is believed that there is also an analog for this case. (For more see the notes written by Coates for the Cambridge course of spring 2004 on cyclotomic fields.)

0.3 Appendix infinite number theory

In the text above we used some less common theory about infinite number theory. In this section we will summarize the definitions given in the appendix of Washington's cyclotomic fields. Proofs can be found there.

Let $k/\mathbb{Q}$ and K/k be an algebraic extensions, possibly infinite. The ring of integers for k, denoted by $\mathcal{O}_k$, is defined in the same way as in the finite case (see Lang's algebraic number theory page 6). We also have prime ideals in $\mathcal{O}_k$ which we call just as in the finite case primes of k. If $\mathcal{P}$ is a prime of K, then $\pi = \mathcal{P} \cap k$ is a prime of k. And we also have the reverse, for every prime π in k there is a prime $\mathcal{P}$ in K above $\mathcal{P}$, i.e. $\mathcal{P} \cap k = \pi$ (see Lang's algebraic number theory page 9).

Assume now that K/k is Galois. Let $\mathcal{P}$ and $\mathcal{P}'$ be two primes of K above a prime π in k, then there exist, just as in the finite case, an element σ of the galois group of K/k such that $\sigma(\mathcal{P}) = \mathcal{P}'$ (see Washington page 334). We define the decomposition group D of $\mathcal{P}$ by $D_\mathcal{P} = \{\sigma \in \mathrm{Gal}(K/k) : \sigma(\mathcal{P}) = \mathcal{P}\}$. The inertia group I of $\mathcal{P}$ we define by $I_\mathcal{P} = \{\sigma \in D_\mathcal{P} : \sigma(\alpha) \equiv \alpha \bmod \mathcal{P} \text{ for all } \alpha \in \mathcal{O}_K\}$. Both D and I are closed and we define ramification and splitting behaviour via these groups.