Classical Iwasawa theory

Arizona Winter School 2018

L1. Foundational material

The lecture will briefly cover, without proofs, the background in algebra and number theory needed at the beginning of Iwasawa theory. Throughout, p will denote an arbitrary prime number, and Γ a topological group which is isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. Thus, for each $n \geqslant 0$, Γ will have a closed subgroup of index p^n, which we will denote by Γ_n, and Γ/Γ_n will then be a cyclic group of order p^n. The Iwasawa algebra $\Lambda(\Gamma)$ of Γ is defined by

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n],$$

and it is endowed with the natural topology coming from the p-adic topology on the $\mathbb{Z}_p[\Gamma/\Gamma_n]$.

1.1 Some relevant algebra

We recall without proof some of the basic algebra needed in classical Iwasawa theory. Let $R = \mathbb{Z}_p[[T]]$ be the ring of formal power series in an indeterminate T with coefficients in $\mathbb{Z}_p$. Then R is a Noetherian regular local ring of dimension 2 with maximal ideal $\mathfrak{m} = (p, T)$. We say that a monic polynomial $q(T) = \sum_{i=0}^{n} a_i T^i$ in R is <u>distinguished</u> if $a_0, \dots, a_{n-1} \in p\mathbb{Z}_p$. The Weierstrass preparation theorem for R tells us that every non-zero $f(T)$ in R can be written uniquely in the form $f(T) = p^{\mu} q(T) u(T)$, where $\mu \geqslant 0$, $q(T)$ is a distinguished polynomial, and $u(T)$ is a unit in R.

<u>Proposition</u> 1.1. Let γ be a fixed topological generator of Γ. Then there is a unique isomorphism of $\mathbb{Z}_p$-algebras

$$\Lambda(\Gamma) \xrightarrow{\sim} R = \mathbb{Z}_p[[T]]$$

which maps γ to $1+T$.

In the following, we shall often identify $\Lambda(\Gamma)$ and R, bearing in mind that Γ will not usually have a canonical topological generator.

Let X be any profinite abelian p-group, on which Γ acts continuously. Then the Γ-action extends by continuity and linearity to an action of the whole Iwasawa algebra $\Lambda(\Gamma)$. Moreover, X will be finitely generated over $\Lambda(\Gamma)$ if and only if $X/\mathfrak{m}X$ is finite, where $\mathfrak{m} = (p, \gamma - 1)$, with γ a topological generator of Γ, is the maximal ideal of $\Lambda(\Gamma)$. We write $\mathfrak{R}(\Gamma)$ for the category of finitely generated $\Lambda(\Gamma)$-modules. If X is in $\mathfrak{R}(\Gamma)$, we define the $\Lambda(\Gamma)$-rank of X to be $Q(\Gamma)$-dimension of $X \otimes_{\Lambda(\Gamma)} Q(\Gamma)$, where $Q(\Gamma)$ denotes the field of fractions of $\Lambda(\Gamma)$. We say X is $\Lambda(\Gamma)$-torsion if it has $\Lambda(\Gamma)$-rank 0, or equivalently if $\alpha X = 0$ for some non-zero α in $\Lambda(\Gamma)$.

Although $\Lambda(\Gamma)$ is not a principal ideal domain, there is nevertheless a beautiful structure theory for modules in $\mathfrak{R}(\Gamma)$ (see Bourbaki, Commutative Algebra, Chap. 7, §4), which can be summarized by the following result:-

<u>Theorem</u> 1.2. For each X in $\mathfrak{R}(\Gamma)$, we have an exact sequence of $\Lambda(\Gamma)$-modules

$$0 \to D_1 \to X \to \Lambda(\Gamma)^r \oplus \bigoplus_{i=1}^{m} \Lambda(\Gamma)/(f_i) \to D_2 \to 0,$$

where D_1 and D_2 have finite cardinality, and $f_i \neq 0$ for $i = 1, \dots, m$. Moreover, the ideal $c(X) = f_1 \dots f_m \Lambda(\Gamma)$ is uniquely determined by X when $r = 0$.

We list some of the main consequences of the structure theory used in Iwasawa theory. Fist, X will be $\Lambda(\Gamma)$-torsion if and only if $r = 0$. Suppose now that X is $\Lambda(\Gamma)$-torsion. The principal ideal $c(X)$ is called the characteristic ideal of X. A characteristic element of X is any generator $f_X(T)$ of $c(X)$. By the Weierstrass preparation theorem, we can write

$$f_X(T) = p^{\mu(X)} q_X(T) u(T),$$

where $\mu(X)$ is an integer $\geqslant 0$, $q_X(T)$ is a distinguished polynomial, and $u(T)$ is a unit in $\Lambda(\Gamma)$. Clearly $\mu(X)$ and $q_X(T)$ are uniquely determined by X. We define $\mu(X)$ to be the μ-invariant of X, and we define the degree $\lambda(X)$ of $q_X(T)$ to be λ-invariant of X.

Exc 1. Assume X in $\mathcal{R}(\Gamma)$ is $\Lambda(\Gamma)$-torsion. Prove that X is finitely generated as a $\mathbb{Z}_p$-module if and only if $\mu(X) = 0$.

Recall that Γ_n denotes the unique subgroup of Γ of index p^n. Thus, if Γ has a topological generator γ, then Γ_n is topologicall generated by γ^{p^n}. If X is in $\mathcal{R}(\Gamma)$, we define X^{Γ_n} and X_{Γ_n} to be the largest submodule and quotient module of X, respectively, on which Γ_n acts trivially. Thus

$$(X)_{\Gamma_n} = X/(\gamma^{p^n}-1)X.$$

Exc 2. Assume X is in $\mathcal{R}(\Gamma)$, and that, for all $n \geqslant 0$, we have

$\mathbb{Q}_p$-dimension of $\left((X)_{\Gamma_n} \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p\right) = m\, p^n + \delta_n$,
where m is independent of n, and δ_n is bounded as $n \to \infty$. Prove that X has $\Lambda(\Gamma)$-rank equal to m, and that δ_n is constant for n sufficiently large.

Ex. 3. Assume X in $\mathfrak{R}(\Gamma)$ is $\Lambda(\Gamma)$-torsion, and let $f_X(T)$ be any characteristic element. Prove that the following are equivalent:- (i) $f_X(0) \neq 0$, (ii) X_Γ is finite, and (iii) X^Γ is finite. When all three are valid, prove the Euler characteristic formula

$$|f_X(0)|_p^{-1} = \#(X_\Gamma)/\#(X^\Gamma).$$

1.2. <u>Some basic class field theory</u>. We recall basic facts from abelian class field theory which will be used repeatedly later. As always, p is any prime number. Let F be a finite extension of $\mathbb{Q}$, and K an extension of F. We recall that an infinite place v of F is said to ramify in K if v is real and if there is at least one complex prime of K above v. In these lectures, we will mainly be concerned with the maximal abelian p-extension L of F, which is unramified at all finite and infinite places of F (i.e. L is the p-Hilbert class field of F), and with the maximal abelian p-extension M of F, which is unramified at all infinite places of F and all finite places of F which do not lie above p. Artin's global reciprocity law gives the following explicit descriptions of $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(M/F)$, in which we simply write isomorphisms for the relevant Artin maps. Firstly, we have

$$A_F \xrightarrow{\sim} \mathrm{Gal}(L/F),$$

where A_F denotes the p-primary subgroup of the ideal class group of F. Secondly, for each place v of F lying above p, write U_v for the group of local units in the completion of F at v which are $\equiv 1 \bmod v$. Put

$$U_F = \prod_{v|p} U_v.$$

If W is any $\mathbb{Z}_p$-module, we define the $\mathbb{Z}_p$-rank of W to be $\dim_{\mathbb{Q}_p}(W \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p)$. Then U_F is a $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $[F : \mathbb{Q}]$. Let E_F be the group of all global units of F which are $\equiv 1 \bmod v$ for all primes v of F above p. By Dirichlet's theorem, E_F has $\mathbb{Z}$-rank equal to $r_1 + r_2 - 1$, where r_1 is the number of real and r_2 the number of complex places of F. Now we have the obvious embedding of E_F in U_F, and we define $\overline{E}_F$ to be the closure in the $\underline{p}$-adic topology of the image of E_F (equivalently, $\overline{E}_F$ is the $\mathbb{Z}_p$-submodule of U_F which is generated by the image of E_F). Secondly, the Artin map then induces an isomorphism

$$U_F / \overline{E}_F \xrightarrow{\sim} \mathrm{Gal}(M/L),$$

where, as above, L is the p-Hilbert class field of F. Clearly, the $\mathbb{Z}_p$-module $\overline{E}_F$ must have $\mathbb{Z}_p$-rank equal to $r_1 + r_2 - 1 - \delta_{F,p}$ for some integer $\delta_{F,p} \geq 0$, and so we immediately obtain :-

<u>Theorem</u> 1.3. Let M be the maximal abelian p-extension of F which is unramified outside the primes of F lying above p. Then $\mathrm{Gal}(M/F)$ is a finitely generated $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to $r_2 + 1 + \delta_{F,p}$.

Leopoldt's Conjecture. $\delta_{F,p} = 0$.

The conjecture follows from Baker's theorem on linear forms in the p-adic logarithms of algebraic numbers when F is a finite abelian extension of either $\mathbb{Q}$ or an imaginary quadratic field.

1.3. $\mathbb{Z}_p$-extensions.

Let F be a finite extension of $\mathbb{Q}$. A $\mathbb{Z}_p$-extension of F is defined to be any Galois extension F_∞ of F such that the Galois group of F_∞ over F is topologically isomorphic to $\mathbb{Z}_p$.

The most basic example of a $\mathbb{Z}_p$-extension is the cyclotomic $\mathbb{Z}_p$-extension of F. For each $m > 1$, let μ_m denote the group of m-th roots of unity, and put $\mu_{p^\infty} = \bigcup_{n \geq 1} \mu_{p^n}$. The action of the Galois group of $\mathbb{Q}(\mu_{p^\infty})$ over $\mathbb{Q}$ on μ_{p^∞} defines an injection of this Galois group into $\mathbb{Z}_p^\times$, and this injection is an isomorphism by the irreducibility of the p-power cyclotomic polynomials. Put $V = 1 + 2p\mathbb{Z}_p$, so that V is isomorphic to $\mathbb{Z}_p$ under the p-adic logarithm. Then $\mathbb{Z}_p^\times = \mu_2 \times V$ when $p = 2$, and $\mu_{p-1} \times V$ when $p > 2$. Hence $\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}\right) = \Delta \times \Gamma$, where $\Gamma \xrightarrow{\sim} \mathbb{Z}_p$, and Δ is cyclic of order 2 or $p-1$, according as $p = 2$ or $p > 2$. Thus

$$\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Delta$$

will be a $\mathbb{Z}_p$-extension of $\mathbb{Q}$, which we call the cyclotomic $\mathbb{Z}_p$-extension. Theorem 1.3 shows that it is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. If now F is any finite extension, the compositum $F\mathbb{Q}_\infty$ will be a $\mathbb{Z}_p$-extension of F, called the cyclotomic $\mathbb{Z}_p$-extension of F. Note that, if F is totally real, we see from Theorem 1.3 that, provided Leopoldt's conjecture is valid for F, then the cyclotomic $\mathbb{Z}_p$-extension is the unique $\mathbb{Z}_p$-extension of F.

Here is another example of a $\mathbb{Z}_p$-extension. Let K be an imaginary quadratic field, and let p be a rational prime which splits in K into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$. Then global class field theory shows that there is a unique $\mathbb{Z}_p$-extension K_∞ of K in which only the prime $\mathfrak{p}$ (but not $\mathfrak{p}^*$) is ramified. If now F is any finite extension of K, the compositum $F_\infty = FK_\infty$ will be another example of a $\mathbb{Z}_p$-extension of F, which is not the cyclotomic $\mathbb{Z}_p$-extension. We shall call this $\mathbb{Z}_p$-extension the split prime $\mathbb{Z}_p$-extension of F. Interestingly, the cyclotomic and the split prime $\mathbb{Z}_p$-extensions of any number field seem to have many properties in common.

Ex 4. Let F be a number field. If F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F, prove that there are only finitely many places of F_∞ lying above each finite prime of F. If F contains an imaginary quadratic field K, and p splits in K, prove the same assertion for the split prime $\mathbb{Z}_p$-extension of F.

Finally, we point out the following result.

Proposition 1.4. Let F be a finite extension of $\mathbb{Q}$, and J_∞/F a Galois extension such that $\mathrm{Gal}(J_\infty/F) = \mathbb{Z}_p^d$ for some $d \geq 1$. If a prime v of F is ramified in J_∞, then v must divide p.

Proof. If v is a prime of F not dividing p, then its inertia group in J_∞/F must be tamely ramified. But then, by class field theory, such a tamely ramified group must be finite, and so it must be 0 in $\mathrm{Gal}(J_\infty/F)$.

<u>2a</u> . <u>2.1</u> Henceforth, F will denote a finite extension of $\mathbb{Q}$, and r_2 will always denote the number of complex places of F. For the moment, F_∞/F will denote an arbitrary $\mathbb{Z}_p$-extension of F, where p is any prime number. Put $\Gamma = \mathrm{Gal}(F_\infty/F)$, and let Γ_n denote the unique closed subgroup of F of index p^n. Let F_n denote the fixed field of Γ_n, so that $[F_n : F] = p^n$. Let M_∞ be the maximal abelian p-extension of F_∞, which is unramified outside the set of places of F_∞ lying above p, and put $X(F_\infty) = \mathrm{Gal}(M_\infty/F_\infty)$. For each $n \geqslant 0$, let M_n be the maximal abelian p-extension of F_n unramified outside p. Since F_∞/F is unramified outside p, we see that $M_n \supset F_\infty$ and that M_n is the maximal abelian extension of F_n contained in M_∞. We next observe that there is a canonical (left) action of Γ on $X(F_\infty)$, which is defined as follows. By maximality, it is clear that M_∞ is Galois over F, so that we have the exact sequence of groups

$$0 \longrightarrow X(F_\infty) \longrightarrow \mathrm{Gal}(M_\infty/F) \longrightarrow \Gamma \longrightarrow 0.$$

If $\tau \in \Gamma$, let $\tilde{\tau}$ denote any lifting of τ to $\mathrm{Gal}(M_\infty/F)$. We then define, for x in $X(F_\infty)$, $\tau x = \tilde{\tau} x \tilde{\tau}^{-1}$. This action is well defined because $X(F_\infty)$ is abelian, and is continuous. Now let $X(F_\infty)_{\Gamma_n}$ be the largest quotient of $X(F_\infty)$ on which the subgroup Γ_n of Γ acts trivially. Since M_n is the maximal abelian extension of F_n contained in M_∞, it follows easily that

$$X(F_\infty)_{\Gamma_n} = \mathrm{Gal}(M_n/F_\infty).$$

In particular, since class field theory tells us that $\mathrm{Gal}(M_0/F_\infty)$

is a finitely generated $\mathbb{Z}_p$-module, it follows from Nakayama's lemma that $X(F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module, where the $\Lambda(\Gamma)$-action is given by extending the Γ-action by linearity and continuity. For each $n \geqslant 0$, let $\delta_{F_n,p}$ denote the discrepancy of the Leopoldt conjecture for the field F_n (see §1).

Proposition 2.1. The $\Lambda(\Gamma)$-rank of $X(F_\infty)$ is always $\geqslant r_2$. It is equal to r_2 if and only if the $\delta_{F_n,p}$ are bounded as $n \to \infty$.

Proof. Since $X(F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module, it follows from the structure theory (see Ex. 2) that, provided n is sufficiently large, we have

(2.1) $\mathbb{Z}_p$- rank $X(F_\infty)_{\Gamma_n} = m p^n + c$,

where m is the $\Lambda(\Gamma)$-rank of $X(F_\infty)$, and c is a constant integer $\geqslant 0$. On the other hand, since $X(F_\infty)_{\Gamma_n} = \mathrm{Gal}(M_n/F_\infty)$, we conclude from Theorem 1.3 applied to the extension M_n/F_n that

(2.2) $\mathbb{Z}_p$-rank of $X(F_\infty)_{\Gamma_n} = r_2 p^n + \delta_{F_n,p}$;

here we are using the fact that the number of complex places of F_n is $r_2 p^n$, because no real place can ramify in the $\mathbb{Z}_p$-extension F_∞/F. The equalities (2.1) and (2.2) immediately imply the Proposition.

Ex 2.1. If $\delta_{F,p} = 0$, prove that the $\delta_{F_n,p}$ are bounded as $n \to \infty$.

Our aim in these lectures is to prove the following theorem, which is one of the principal results of Iwasawa's 1973 Annals paper.

<u>Theorem</u>. Let p be any prime number and F_∞/F the cyclotomic $\mathbb{Z}_p$-extension. Then $X(F_\infty)$ has $\Lambda(\Gamma)$-rank r_2, or equivalently $\delta_{F_n,p}$ is bounded as $n \to \infty$.

The essential idea of Iwasawa's proof is to use multiplicative Kummer theory. We do not know how to prove this result for non-cyclotomic $\mathbb{Z}_p$-extensions.

2.2. <u>Multiplicative Kummer theory</u>. For each integer $m > 1$, μ_m will denote the group of m-th roots of unity in $\overline{\mathbb{Q}}$. Until further notice, we shall assume that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, and that

(2.3) $\mu_p \subset F$ if $p > 2$, $\mu_4 \subset F$ if $p = 2$.

Thus we have

(2.4) $F_\infty = F(\mu_{p^\infty})$.

Since $\mu_{p^\infty} \subset F_\infty$, classical multiplicative Kummer theory is as follows. Let $F_\infty^\times$ be the multiplicative group of F_∞, and let F_∞^{ab} be the maximal abelian p-extension of F_∞. Then we have the canonical dual pairing

(2.5) $\langle\, ,\rangle : \mathrm{Gal}(F_\infty^{ab}/F_\infty) \times (F_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mu_{p^\infty}$

given by (here $\alpha \in F_\infty^\times$ and $a \geqslant 0$)

$$\langle \sigma, \alpha \otimes (p^{-a} \bmod \mathbb{Z}_p)\rangle = \sigma\beta/\beta \quad \text{where } \beta^{p^a} = \alpha.$$

Of course, there is a natural action of $\Gamma = \mathrm{Gal}(F_\infty/F)$ on all of these groups, and the pairing gives rise to an isomorphism of Γ-modules

$$\mathrm{Gal}(F_\infty^{ab}/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}).$$

As before, let M_∞ be the maximal abelian p-extension of F_∞ which is unramified outside p. Since $M_\infty \subset F_\infty$, the Kummer pairing induces an isomorphism of Γ-modules

$$(2.6) \qquad \mathrm{Gal}(M_\infty/F_\infty) \xrightarrow{\sim} \mathrm{Hom}(\mathfrak{M}_\infty, \mu_{p^\infty}),$$

for a subgroup $\mathfrak{M}_\infty \subset F_\infty^\times \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_p/\mathbb{Z}_p$, which can be described explicitly as follows. Recall that, as F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension, there are only finitely many primes of F_∞ lying above each rational prime number, and that the primes which do not lie above p all have discrete valuations. Let I_∞' be the free abelian group on the primes of F_∞ which do not lie above p. Then every $\alpha \in F_\infty^\times$ determines a unique ideal $(\alpha)' \in I_\infty'$. The following lemma is then easily proven.

<u>Lemma</u>. $\mathfrak{M}_\infty$ is the subgroup of all elements of $F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ of the form $\alpha \otimes p^{-a} \bmod \mathbb{Z}_p$ where $\alpha \in F_\infty^\times$ is such that $(\alpha)' \in I_\infty^{p^a}$.

We can then analyse $\mathfrak{M}_\infty$ by the following exact sequence. Let E_∞' be the group of all elements α in $F_\infty^\times$ with $(\alpha)' = 1$. We have the obvious map

$$i_\infty : E_\infty' \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathfrak{M}_\infty$$

given by $i_\infty(\varepsilon \otimes p^{-a} \bmod \mathbb{Z}_p) = \varepsilon \otimes p^{-a} \bmod \mathbb{Z}_p$, which is easily seen to be injective. Moreover, the map

$$j_\infty : \mathfrak{M}_\infty \longrightarrow A_\infty'$$

is defined by $j_\infty(\alpha \otimes p^{-a} \bmod \mathbb{Z}_p) = cl(\mathfrak{a})$, where $(\alpha)' = \mathfrak{a}^{p^a}$. Both i_∞ and j_∞ are obviously Γ-homomorphisms.

Lemma. The sequence of Γ-modules

$$(2.6) \quad 0 \longrightarrow E'_\infty \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{i_\infty} \mathcal{M}_\infty \xrightarrow{j_\infty} A'_\infty \to 0$$

is exact.

The proof of exactness is completly straightforward. In view of the exact sequence (2.6), we can now break up the Iwasawa module $X(F_\infty) = Gal(M_\infty/F_\infty)$ into two parts. Define

$$N'_\infty = F_\infty\left(\sqrt[p^n]{\varepsilon} \text{ for all } \varepsilon \in E'_\infty \text{ and all } n \geq 1\right).$$

Then, thanks to (2.6), the Kummer pairing induces Γ-isomorphisms

$$Gal(N'_\infty/F_\infty) \xrightarrow{\sim} Hom(E'_\infty \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty})$$

and

$$Gal(M_\infty/N'_\infty) \xrightarrow{\sim} Hom(A'_\infty, \mu_{p^\infty}).$$

Let $T_p(\mu) = \varprojlim \mu_{p^n}$ be the Tate module of μ_{p^∞}. Thus $T_p(\mu)$ is a free $\mathbb{Z}_p$-module of rank 1 on which Γ acts via the character giving the action of Γ on μ_{p^∞}. Thus, if we now define

$$(2.7) \quad Z'_\infty = Hom(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p),$$

we see immediately that $Gal(M_\infty/N'_\infty) = Z'_\infty \underset{\mathbb{Z}_p}{\otimes} T_p(\mu)$, endowed with the diagonal action of Γ.

Theorem A (Iwasawa). Z'_∞ is always a finitely generated torsion $\Lambda(\Gamma)$-module.

In fact, Iwasawa proves Theorem A for an *arbitrary* $\mathbb{Z}_p$-extension F_∞/F (the definition of A'_∞ we have given must be slightly modified for an arbitrary $\mathbb{Z}_p$-extension).

Now it is easy to see that if Z'_∞ is $\Lambda(\Gamma)$-torsion, then so is $Z'_\infty \otimes_{\mathbb{Z}_p} T_p(\mu)$. Hence, for the cyclotomic $\mathbb{Z}_p$-extension, Theorem A has the following corollary:-

Corollary. $\mathrm{Gal}(M_\infty/N'_\infty)$ is a finitely generated torsion $\Lambda(\Gamma)$-module.

In the next lecture we will outline Iwasawa's proof of the following result:—

Theorem B (Iwasawa). Let $F_\infty = F(\mu_{p^\infty})$, where $\mu_p \subset F$ if $p > 2$ and $\mu_4 \subset F$ if $p = 2$. Then $\mathrm{Gal}(N'_\infty/F_\infty)$ is a finitely generated $\Lambda(\Gamma)$-module of rank $r_2 = [F:\mathbb{Q}]/2$.

The value of r_2 is as given because F is clearly totally imaginary. As we shall see in the next lecture, Iwasawa's proof gives very precise information about the $\Lambda(\Gamma)$-torsion submodule of $\mathrm{Gal}(N'_\infty/F_\infty)$.

Of course, Theorem A and Theorem B together imply that $\mathrm{Gal}(M_\infty/F_\infty)$ has $\Lambda(\Gamma)$-rank equal to $r_2 = [F:\mathbb{Q}]/2$, proving the weak Leopoldt conjecture in this case.

2.3 Elementary properties of p-units in F_∞/F.

As a first step towards proving Theorem B, we establish some basic properties of the units E'_∞. Let W_n be the group of all roots of unity in F_n, and W_∞ the group of all roots of unity in F_∞. Thus W_∞ is the product of μ_{p^∞} with a finite group of order prime to p. Define

$$\mathcal{E}'_n = E'_n/W_n, \quad \mathcal{E}'_\infty = E'_\infty/W_\infty \quad ;$$

here E'_n denotes the group of p-units of F_n. Let s_n denote the number of primes of F_n lying above p. Then, by the generalization of the unit theorem to p-units, $\mathcal{E}_n'$ is a free abelian group of rank $r_2 p^n + s_n - 1$, where $r_2 = [F : \mathbb{Q}]/2$. Moreover, $\mathcal{E}_\infty'$ is the union of the increasing sequence of subgroups $\mathcal{E}_n'$.

<u>Lemma</u>. $\mathcal{E}_\infty'$ is a free abelian group, and, for all $n \geqslant 0$, $\mathcal{E}_n'$ is a direct summand of $\mathcal{E}_\infty'$.

<u>Proof</u>. Now $(E_\infty')^{\Gamma_n} = E_n'$ for all $n \geqslant 0$. As $H^1(\Gamma_n, W_\infty) = (W_\infty)_{\Gamma_n} = 0$, it follows that $(\mathcal{E}_\infty')^{\Gamma_n} = \mathcal{E}_n'$ for all $n \geqslant 0$. We next observe that $\mathcal{E}_\infty' / \mathcal{E}_n'$ is torsion free. Indeed, suppose u is an element of $\mathcal{E}_\infty'$ with $u^k \in \mathcal{E}_n'$ for some integer $k \geqslant 1$. If γ is any element of Γ_n, we must then have $(\gamma u/u)^k = 1$, whence $\gamma u = u$ since $\mathcal{E}_\infty'$ is torsion free, and so $u \in \mathcal{E}_n'$ as required. Hence, for all $m \geqslant n$, $\mathcal{E}_m' / \mathcal{E}_n'$ is torsion free. As $\mathcal{E}_m'$ and $\mathcal{E}_n'$ are both finitely generated torsion free abelian groups, it follows that $\mathcal{E}_n'$ must be a direct summand of $\mathcal{E}_m'$ for all $m \geqslant n$, and the ~~final~~ assertions of the lemma follow.

§3. We now give Iwasawa's proof of Theorem B of the last lecture. Let $\mathbb{Q}'$ be the ring of all rational numbers whose denominator is a power of p. Note that $\mathbb{Q}'/\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p$. Hence, for all $n \geqslant 0$, we have the exact sequence

$$0 \longrightarrow \mathcal{E}_n' \longrightarrow \mathcal{E}_n' \otimes_{\mathbb{Z}} \mathbb{Q}' \longrightarrow \mathcal{E}_n' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

Also, we have the exact sequence

$$(3.1) \quad 0 \longrightarrow \mathcal{E}_\infty' \longrightarrow \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}' \longrightarrow \mathcal{E}_\infty' \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

Recall that, for all $n \geqslant 0$, $\mathcal{E}_n'$ is a direct summand of $\mathcal{E}_\infty'$, and $(\mathcal{E}_\infty')^{\Gamma_n} = \mathcal{E}_n'$. It follows that

$$\left(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}'\right)^{\Gamma_n} = \mathcal{E}_n' \otimes_{\mathbb{Z}} \mathbb{Q}'.$$

Also, for all $n \geqslant 0$,

$$H^1\left(\Gamma_n, \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}'\right) = \varinjlim_{m \geqslant n} H^1\left(\mathrm{Gal}(K_m/K_n), \mathcal{E}_m' \otimes_{\mathbb{Z}} \mathbb{Q}'\right),$$

and this last cohomology group is 0 because $\mathcal{E}_m' \otimes_{\mathbb{Z}} \mathbb{Q}'$ is p-divisible. Hence we have

$$H^1\left(\Gamma_n, \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}'\right) = 0.$$

Thus, taking Γ_n-cohomology of the exact sequence (3.1), we immediately obtain:–

<u>Proposition 3.1</u> For all $n \geqslant 0$, we have the exact sequence

$$0 \longrightarrow \mathcal{E}_n' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \left(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p\right)^{\Gamma_n} \longrightarrow H^1(\Gamma_n, \mathcal{E}_\infty') \to 0.$$

To prove Theorem B, we also need to know that $H^1(\Gamma_n, \mathcal{E}_\infty')$ is a finite group. In fact, it is a torsion group, and it must be finitely generated because the Pontrjagin dual of $\mathcal{E}_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a finitely generated $\Lambda(\Gamma)$-module.

However, a more intrinsic proof, which in the end yields more information about the structure of $\mathrm{Gal}(N'_\infty | F_\infty)$ as a $\Lambda(\Gamma)$-module, comes from the following result. For all $n \geq 0$, let I'_n denote the multiplicative group of all fractional ideals of F_n which are prime to p, and let $P'_n = \{(\alpha)' : \alpha \in F_n^\times\}$ be the subgroup of principal ideals. Put A'_n for the p-primary subgroup of I'_n / P'_n. For all $n \geq 0$, we have the natural injection $I'_n \longrightarrow I'_\infty$, and this induces a homomorphism $A'_n \longrightarrow A'_\infty$.

Proposition 3.2. For all $n \geq 0$, we have

$$H^1(\Gamma_n, \mathcal{E}'_\infty) = \mathrm{Ker}\,(A'_n \longrightarrow A'_\infty).$$

In particular, $H^1(\Gamma_n, \mathcal{E}'_\infty)$ is finite.

We remark that, in his 1973 Annals paper, Iwasawa proves that Proposition 3.2 is valid for every $\mathbb{Z}_p$-extension F_∞ / F in which every prime of F above p is ramified. Under the same hypotheses, he also shows that the order of $H^1(\Gamma_n, \mathcal{E}'_\infty)$ is bounded as $n \to \infty$. In his Ph.D thesis at Princeton under Iwasawa, Ralph Greenberg showed the existence of many examples when $\mathrm{Ker}\,(A'_n \longrightarrow A'_\infty)$ is non-zero. However, in the most classical case when $F = \mathbb{Q}(\mu_p)$ with p an odd prime, and $F_\infty = \mathbb{Q}(\mu_{p^\infty})$, it is still unknown whether there exist primes p such that $\mathrm{Ker}\,(A'_n \longrightarrow A'_\infty)$ is non-zero.

Before proving Proposition 3.2, we first show that Theorem B is an easy consequence of Proposition 3.1 For each $n \geq 0$, let s_n denote the number of primes of F_n lying above p. Then the analogue of Dirichlet's theorem for the E_n' tells us that $\mathcal{E}_n'$ is a free abelian group of rank $r_2 p^n + s_n - 1$. Moreover, since p is totally ramified in the extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$, it follows that there exists $n_0 \geqslant 0$ such that every prime above p is totally ramified in the extension F_∞/F_{n_0}. Hence we conclude that $s_n = s$, where $s = s_{n_0}$, for all $n \geqslant n_0$. Thus, since $H^1(\Gamma_n, \mathcal{E}_\infty')$ is finite, it follows from Proposition 3.1 that, provided $n \geqslant n_0$, the maximal divisible subgroup of $(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_n}$ has $\mathbb{Z}_p$-corank $r_2 p^n + s - 1$. Put

$$Y_\infty' = \mathrm{Hom}(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

Then it follows immediately from Pontrjagin duality that $(Y_\infty')_{\Gamma_n}$ has $\mathbb{Z}_p$-~~co~~rank $r_2 p^n + s - 1$ for all $n \geqslant n_0$. Now Y_∞' is a finitely generated $\Lambda(\Gamma)$-module because $(Y_\infty')_\Gamma$ is a finitely generated $\mathbb{Z}_p$-module, and so it follows immediately from the structure theory (see Exc 2) that Y_∞' has $\Lambda(\Gamma)$-rank equal to r_2. But Kummer theory immediately shows that

$$Y_\infty' \otimes_{\mathbb{Z}_p} T_p(\mu) = \mathrm{Gal}(N_\infty'/F_\infty).$$

Thus Theorem B then follows from the following simple algebraic exercise.

Exc 3.1. Let W be any finitely ~~alg~~ generated $\Lambda(\Gamma)$-module. Assume $\mu_{p^\infty} \subset F_\infty$, and let $V = W \otimes_{\mathbb{Z}_p} T_p(\mu)$, where Γ acts on V by the twisted action $\sigma(w \otimes \alpha) = \sigma w \otimes \sigma\alpha$, with $w \in W$ and $\alpha \in T_p(\mu)$. Prove that the $\Lambda(\Gamma)$-module V has the same $\Lambda(\Gamma)$-rank as W.

We remark that, in his 1973 Annals paper, Iwasawa shows that a further analysis of the above proof of Theorem B yields more information about the $\Lambda(\Gamma)$-module $\mathrm{Gal}(N'_\infty/F_\infty)$. Let $t(\mathrm{Gal}(N'_\infty/F_\infty))$ denote the $\Lambda(\Gamma)$-torsion submodule of $\mathrm{Gal}(N'_\infty/F_\infty)$. Then Iwasawa proves the following facts :- (i) $\mathrm{Gal}(N'_\infty/F_\infty)$ contains no non-zero $\mathbb{Z}_p$-torsion, (ii) $t(\mathrm{Gal}(N'_\infty/F_\infty))$ is a free $\mathbb{Z}_p$-module of rank $s-1$, where $s =$ number of primes above p in the extension F_∞/F_{n_0} as above, and he determines exactly its characteristic power series (even its structure up to pseudo-isomorphism), and (iii). $\mathrm{Gal}(N'_\infty/F_\infty)/t(\mathrm{Gal}(N'_\infty/F_\infty))$ is a free $\Lambda(\Gamma)$-module if and only if $H^1(\Gamma_n, \mathcal{E}'_\infty) = 0$ for all $n \geqslant a$, where a is an esplicitly determined integer $\leqslant s-1$.

Finally, we give the proof of Proposition 3.2. For all $m \geqslant n$, we will prove that there is an isomorphism

$$\tau_{n,m} : \mathrm{Ker}(A'_n \to A'_m) \xrightarrow{\sim} H^1(\mathrm{Gal}(F_m/F_n), E'_m).$$

Passing to the inductive limit overall $m \geqslant n$, and noting that $H^i(\Gamma_n, W_\infty) = 0$ for all $i \geqslant 1$, Proposition 3.2 will then follow. Fisc a generator σ of $\mathrm{Gal}(F_m/F_n)$, and write $\mathcal{O}'_m$ for the ring of p-integers of F_m. If c is some element of $\mathrm{Ker}(A'_n \to A'_m)$, and $\mathfrak{a} \in I_n$ is an ideal in c, then $\mathfrak{a}\mathcal{O}'_m = \alpha\mathcal{O}'_m$ for some $\alpha \in \mathcal{O}'_m$. Define $\varepsilon = \sigma\alpha/\alpha$. Thus ε is an element of E'_m with $N_{F_m/F_n}(\varepsilon) = 1$. It is easy to see that the cohomology class $\{\varepsilon\}$ of ε in $H^1(\mathrm{Gal}(F_m/F_n), E'_m)$ depends only on c, and we define $\tau_{n,m}(c) = \{\varepsilon\}$. One checks easily that $\tau_{n,m}$ is injective. To prove surjectivity, let $\{\varepsilon\}$ be any cohomology class in $H^1(\mathrm{Gal}(F_m/F_n), E'_m)$ which is represented by an element ε of E'_m with $N_{m,n}(\varepsilon) = 1$. By Hilbert's Theorem 90, we then have $\varepsilon = \alpha^{\sigma-1}$ for some $\alpha \in \mathcal{O}'_m$. Let $\mathfrak{a}$ in I'_m be given by $\mathfrak{a} = \alpha\mathcal{O}'_m$. Since ε is in E'_m, we see that $\mathfrak{a}^\sigma = \mathfrak{a}$. Moreover, no prime of F_n which does not divide p is ramified in F_m, and so it follows that $\mathfrak{a}$ must be the image of an ideal $\mathfrak{b}$ in I'_n under the natural inclusion $I'_n \hookrightarrow I'_m$. Let c be the class of $\mathfrak{b}$ in I'_n. One sees easily that c lies in $\mathrm{Ker}(A'_n \longrightarrow A'_m)$, and $\tau_{n,m}(c) = \{\varepsilon\}$, completing the proof.