Lecture 1. 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 \( \Gamma \) a topological group which is isomorphic to the additive group of \( p \)-adic integers \( \mathbb{Z}_p \). Thus, for each \( n \geq 0 \), \( \Gamma \) will have a closed subgroup of index \( p^n \), which we will denote by \( \Gamma_n \), and \( \Gamma / \Gamma_n \) will then be a cyclic group of order \( p^n \). The Iwasawa algebra \( \Lambda(\Gamma) \) of \( \Gamma \) 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 \( m = (p, T) \). We say that a monic polynomial \( q(T) = \sum_{i=0}^{n} a_i T^i \) in \( R \) is distinguished if \( a_0, \ldots, a_{n-1} \in p\mathbb{Z}_p \).

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 \( \mu \geq 0 \), \( q(T) \) is distinguished polynomial, and \( u(T) \) is a unit in \( R \).

**Proposition 1.1.** Let \( \gamma \) be a fixed topological generator of \( \Gamma \). Then there is a unique isomorphism of \( \mathbb{Z}_p \)-algebras

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

which maps \( \gamma \) to \( 1 + T \).

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

Let \( X \) be any profinite abelian \( p \)-group, on which \( \Gamma \) acts continuously. Then the \( \Gamma \)-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 \( X / mX \) is finite, where \( m = (p, \gamma - 1) \), with \( \gamma \) a topological generator of \( \Gamma \), is the maximal ideal of \( \Lambda(\Gamma) \). We write \( \mathcal{R}(\Gamma) \) for the category of finitely generated \( \Lambda(\Gamma) \)-rank of \( X \) to be the \( Q(\Gamma) \)-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 \( \alpha \) in \( \Lambda(\Gamma) \).

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

---

1please feel free to contact me with corrections: robert.j.mcdonald@uconn.edu
Theorem 1.2. For each $X$ in $\mathcal{R}(\Gamma)$, we have an exact sequence of $\Lambda(\Gamma)$-modules

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

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

We list some of the main consequences of the structure theory used in Iwasawa theory. First, $X$ 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 $\geq 0$, $q_X(T)$ is a distinguished polynomial, and $u(T)$ is a unit in $\Lambda(\Gamma)$. Clearly $\mu(X)$ and $q_X(T)$ are uniquely determined by $X$, and we define the degree $\lambda(X)$ of $q_X(T)$ to be the $\lambda$-invariant of $X$.

Ex 1.1. 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 $\Gamma_n$ denotes the unique subgroup of $\Gamma$ of index $p^n$. Thus, if $\Gamma$ has a topological generator $\gamma$, then $\Gamma_n$ is topologically generated by $\gamma p^n$. If $X$ is in $\mathcal{R}(\Gamma)$, we define $X^{\Gamma_n}$ and $X_{\Gamma_n}$ to be the largest submodule and quotient submodule of $X$, respectively, on which $\Gamma_n$ acts trivially. Thus

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

Ex 1.2. Assume $X$ is in $\mathcal{R}(\Gamma)$, and that, for all $n \geq 0$, we have

$$\mathbb{Q}_p\text{-dimension of } (X)_{\Gamma_n} \bigotimes_{\mathbb{Z}_p} \mathbb{Q}_p = mp^n + \delta_n,$$

where $m$ is independent of $n$, and $\delta_n$ is bounded as $n \to \infty$. Prove that $X$ has $\Lambda(\Gamma)$-rank equal to $m$, and that $\delta_n$ is constant for $n$ sufficiently large.

Ex 1.3. Assume $X$ in $\mathcal{R}(\Gamma)$ 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) $X_\Gamma$ is finite, and
(iii) $X^{\Gamma}$ is finite.

When all three are valid, prove the Euler characteristic formula

$$|f_X(0)|^{-1}_p = \#(X_\Gamma)/\#(X^{\Gamma})$$
1.2. **Some basic class field theory.** 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 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 $\text{Gal}(L/F)$ and $\text{Gal}(M/F)$, in which we simply write isomorphisms for the relevant Artin maps. Firstly, we have

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

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 $\equiv 1 \mod v$. Put

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

If $W$ is any $\mathbb{Z}_p$-module, we define the $\mathbb{Z}_p$-rank of $W$ to be $\dim_{\mathbb{Q}_p}(W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. 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 $\equiv 1 \mod v$ for all primes $v$ of $F$ lying 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 $E_F$ into $U_F$ and we define $E_F$ to be the closure in the $p$-adic topology of the image of $E_F$ (equivalently, $E_F$ 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

$$U_F/E_F \xrightarrow{\sim} \text{Gal}(M/L),$$

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

**Theorem 1.3.** Let $M$ be the maximal abelian $p$-extension of $F$ which is unramified outside the primes of $F$ lying above $p$. Then $\text{Gal}(M/F)$ 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 $F_\infty$ of $F$ such that the Galois group of $F_\infty$ 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 $\mu_m$ denote the group of $m$-th roots of unity, and put $\mu_\infty = \bigcup_{n \geq 1} \mu_{p^n}$. The action of the Galois group of $\mathbb{Q}(\mu_{p^n})$ over $\mathbb{Q}$ on $\mu_\infty$ 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 \( \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) = \Delta \times \Gamma \), where \( \Gamma \sim \mathbb{Z}_p \) and \( \Delta \) is cyclic of order 2 or \( p - 1 \), according as \( p = 2 \) or \( p > 2 \). Thus
\[
\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^n})^\Delta
\]
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 \( p \) and \( p^* \). Then global class field theory shows that there is a unique \( \mathbb{Z}_p \)-extension \( K_\infty \) of \( K \) in which only the prime \( p \) (but not \( p^* \)) 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, 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 1.4.** Let \( F \) be a number field. If \( F_{\infty} \) is the cyclotomic \( \mathbb{Z}_p \)-extension of \( F \), prove that there are only finitely many places of \( F_{\infty} \) 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 \( J_\infty/F \) a Galois extension such that \( \text{Gal}(J_\infty/F) = \mathbb{Z}_p^d \) for some \( d \geq 1 \). If a prime \( v \) of \( F \) is ramified in \( J_\infty \), then \( v \) must divide \( p \).

**Proof.** If \( v \) is a prime of \( F \) not dividing \( p \), then its inertia group in \( J_\infty/F \) 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 \( \text{Gal}(J_\infty/F) \). \( \square \)

**Lecture 2.**

2.1. 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, \( F_{\infty}/F \) will denote an arbitrary \( \mathbb{Z}_p \)-extension of \( F \), where \( p \) is any prime number. Put \( \Gamma = \text{Gal}(F_{\infty}/F) \), and let \( \Gamma_n \) denote the unique closed subgroup of \( \Gamma \) of index \( p^n \). Let \( F_n \) denote the fixed field of \( \Gamma_n \), so that \( [F_n:F] = p^n \). Let \( M_\infty \) be the maximal abelian \( p \)-extension of \( F_{\infty} \), which is unramified outside the set of places of \( F_{\infty} \) lying above \( p \), and put \( X(F_{\infty}) = \text{Gal}(M_{\infty}/F_{\infty}) \). For each \( n \geq 0 \), let \( M_n \) be the maximal abelian \( p \)-extension of \( F_n \) unramified outside \( p \). Since \( F_{\infty}/F \) is unramified outside \( p \), we see that \( M_n \supset F_n \) and that \( M_n \) is the maximal abelian extension of \( F_n \) contained in \( M_\infty \). We next observe that there is a canonical (left) action of \( \Gamma \) on \( X(F_{\infty}) \), which is defined as follows. By maximality, it is clear that \( M_\infty \) is Galois over \( F \), so that we have the exact sequence of groups
\[
0 \to X(F_{\infty}) \to \text{Gal}(M_\infty/F) \to \Gamma \to 0.
\]
If \( \tau \in \Gamma \), let \( \tilde{\tau} \) denote any lifting of \( \tau \) to \( \text{Gal}(M_\infty/F) \). 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 $\Gamma_n$ of $\Gamma$ acts trivially. Since $M_n$ is the maximal abelian extension of $F_n$ contained in $M_\infty$, it follows easily that
\[ X(F_\infty)_{\Gamma_n} = \text{Gal}(M_n/F_\infty). \]
In particular, since class field theory tells us that $\text{Gal}(M_0/F_\infty)$ 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 $\Gamma$-action by linearity and continuity. For each $n \geq 0$, 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 $\geq r_2$. 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 1.2) that, provided $n$ is sufficiently large, we have
\[ \mathbb{Z}_p\text{-rank } X(F_\infty)_{\Gamma_n} = mp^n + c \]
where $m$ is the $\Lambda(\Gamma)$-rank of $X(F_{\infty})$, and $c$ is a constant integer $\geq 0$. On the other hand, since $X(F_\infty)_{\Gamma_n} = \text{Gal}(M_n/F_\infty)$, we conclude from Theorem 1.3 applied to the extension $M_n/F_n$ that
\[ \mathbb{Z}_p\text{-rank of } X(F_\infty)_{\Gamma_n} = r_2p^n + \delta_{F_n,p}; \]
here we are using the fact that the number of complex places of $F_n$ is $r_2p^n$, because no real place can ramify in the $\mathbb{Z}_p$-extension $F_\infty/F$. The equalities (1) and (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.

**Theorem 2.2.** Let $p$ be any prime number and $F_\infty/F$ 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. **Multiplicative Kummer theory.** For each integer $m > 1$, $\mu_m$ will denote the group of $m$-th roots of unity in $\mathbb{Q}$. Until further notice, we shall assume that $F_\infty/F$ is the cyclotomic $\mathbb{Z}_p$-extension, and that
\[ \mu_p \subset F \text{ if } p > 2, \mu_4 \subset F \text{ if } p = 2. \]
Thus, we have
\[ F_\infty = F(\mu_{p^\infty}). \]
Since $\mu_{p^\infty} \subset F_\infty$, classical multiplicative Kummer theory is as follows. Let $F^{\infty}_{\text{ab}}$ be the multiplicative group of $F_\infty$, and let $F^{\text{ab}}_{\infty}$ be the maximal abelian extension of $F_\infty$. Then we have the canonical dual pairing
\[ \langle \sigma, \alpha \rangle : \text{Gal}(F^{\text{ab}}_\infty/F_\infty) \times (F^{\infty}_\infty \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}_p) \to \mu_{p^\infty} \]
given by (here $\alpha \in F^{\infty}_\infty$ and $a \geq 0$)
\[ \langle \sigma, \alpha \otimes (p^{-a} \mod \mathbb{Z}_p) \rangle = \sigma \beta/\beta \text{ where } \beta^{p^a} = \alpha. \]
Of course, there is a natural action of $\Gamma = \text{Gal}(F_\infty/F)$ on all of these groups, and the pairing gives rise to an isomorphism of $\Gamma$-modules
\[ \text{Gal}(F_\infty^\text{ab}/F_\infty) \xrightarrow{\sim} \text{Hom}(F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mu_p^\infty). \]

As before, let $M_\infty$ be the maximal abelian $p$-extension of $F_\infty$ which is unramified outside of $p$. Since $M_\infty \subset F_\infty$, the Kummer pairing induces an isomorphism of $\Gamma$-modules
\[ \text{Gal}(M_\infty/F_\infty) \xrightarrow{\sim} \text{Hom}(M_\infty, \mu_p^\infty), \]
for a subgroup $M_\infty \subset F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$, which can be described explicitly as follows. Recall that, as $F_\infty/F$ is the cyclotomic $\mathbb{Z}_p$-extension, there are only finitely many primes of $F_\infty$ lying above each rational prime number, and that the primes which do not lie above $p$ all have discrete valuations.

Let $I'_\infty$ be the free abelian group on the primes of $F_\infty$ 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 proven.

**Lemma.** $M_\infty$ is the subgroup of all elements of $F_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ of the form $\alpha \otimes p^{-a} \mod \mathbb{Z}_p$ where $\alpha \in F_\infty^\times$ is such that $(\alpha)' \in I'_\infty$.

We can then analyze $M_\infty$ by the following exact sequence. Let $E'_\infty$ be the graph of all elements $\alpha$ in $F_\infty^\times$ with $(\alpha)' = 1$. We have the obvious map
\[ i_\infty : E'_\infty \otimes \mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p \rightarrow M_\infty \]
given by $i_\infty(\varepsilon \otimes p^{-a} \mod \mathbb{Z}_p) = \varepsilon \otimes p^{-a} \mod \mathbb{Z}_p$, which is easily seen to be injective. Moreover, the map
\[ j_\infty : M_\infty \rightarrow A'_\infty \]
is defined by $j_\infty(\alpha \otimes p^{-a} \mod \mathbb{Z}_p) = d(a)$ where $(\alpha)' = a^{\nu_a}$. Both $i_\infty$ and $j_\infty$ are obviously $\Gamma$-homomorphisms.

**Lemma.** The sequence of $\Gamma$-modules
\[ (3) \quad 0 \rightarrow E'_\infty \otimes \mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{i_\infty} M_\infty \xrightarrow{j_\infty} A'_\infty \rightarrow 0 \]
is exact.

The proof of exactness is completely straightforward. In view of the exact sequence (3), we can now break up the Iwasawa module $X(F_\infty) = \text{Gal}(M_\infty/F_\infty)$ into two parts. Define
\[ N'_\infty = F_\infty((\sqrt[\nu]{\varepsilon}) \text{ for all } \varepsilon \in E'_\infty \text{ and all } n \geq 1) \]
Then, thanks to (3), the Kummer pairing induces $\Gamma$-isomorphisms
\[ \text{Gal}(N'_\infty/F_\infty) \xrightarrow{\sim} \text{Hom}(E'_\infty \otimes \mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p, \mu_p^\infty) \]
and
\[ \text{Gal}(M_\infty/N'_\infty) \xrightarrow{\sim} \text{Hom}(A'_\infty, \mu_p^\infty). \]

Let $T_p(\mu) = \lim \mu_p^n$ be the Tate module of $\mu_p^\infty$. Thus, $T_p(\mu)$ is a free $\mathbb{Z}_p$-module of rank 1 on which $\Gamma$ acts via the character giving the action of $\Gamma$ on $\mu_p^\infty$.1 Thus, if we now define
\[ Z'_\infty = \text{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p), \]
we see immediately that $\text{Gal}(M_\infty/N'_\infty) = Z'_\infty \otimes \mathbb{Z}_p T_p(\mu)$, endowed with the diagonal action of $\Gamma$.

**Theorem A** (Iwasawa). $Z'_\infty$ is always a finitely generated torsion $\Lambda(\Gamma)$-module.
In fact, Iwasawa proves Theorem A for an arbitrary \( \mathbb{Z}_p \)-extension \( F_\infty/F \) (the definition of \( A'_\infty \) we have given must be slightly modified for an arbitrary \( \mathbb{Z}_p \)-extension).

Now it is easy to see that if \( Z'_\infty \) 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.** \( \text{Gal}(M_\infty/N'_\infty) \) is a finitely generated \( \Lambda(\Gamma) \)-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 \( \text{Gal}(N'_\infty/F_\infty) \) 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 \( \text{Gal}(N'_\infty/F_\infty) \).

Of course, Theorem A and Theorem B together imply that \( \text{Gal}(M_\infty/F_\infty) \) 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 \( F_\infty/F \)

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

\[
E'_{n} = E'_{n}/W_n, \quad E'_\infty = E'_\infty/W_\infty;
\]

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, \( E'_n \) is a free abelian group of rank \( r_2 p^n + s_n - 1 \), where \( r_2 = |F : \mathbb{Q}|/2 \). Moreover, \( E'_{\infty} \) is the union of the increasing sequence of subgroups \( E'_n \).

**Lemma.** \( E'_\infty \) is a free abelian group, and, for all \( n \geq 0 \), \( E'_n \) is a direct summand of \( E'_\infty \).

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

**Lecture 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 \( n \geq 0 \), we have the exact sequence

\[
0 \rightarrow E'_n \rightarrow E'_n \otimes_{\mathbb{Z}} \mathbb{Q}' \rightarrow E'_n \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \rightarrow 0.
\]

Also, we have the exact sequence

\[
0 \rightarrow E'_\infty \rightarrow E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}' \rightarrow E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \rightarrow 0.
\]

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

\[
(E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}')^{\Gamma_n} = E'_n \otimes_{\mathbb{Z}} \mathbb{Q}'.
\]
Also, for all \( n \geq 0 \),

\[
H^1(\Gamma_n, \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}') = \lim_{m \to \infty} H^1(\text{Gal}(K_m/K_n), \mathcal{E}_m' \otimes_{\mathbb{Z}} \mathbb{Q}'),
\]

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

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

Thus, taking \( \Gamma_n \)-cohomology of the exact sequence (4), we immediately obtain:

**Proposition 3.1.** For all \( n \geq 0 \), we have the exact sequence

\[
0 \to \mathcal{E}_n' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to (\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\Gamma \to H^1(\Gamma_n, \mathcal{E}_\infty') \to 0.
\]

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 \( \mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \) is a finitely generated \( \Lambda(\Gamma) \)-module. However, a more intrinsic proof, which in the end yields more information about the structure of \( \text{Gal}(\mathcal{E}_\infty'/\mathcal{E}_\infty) \) 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 \( P'_n = \{\langle \alpha \rangle' : \alpha \in F_n^\times \} \) 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 \( I'_n \to I'_\infty \), and this induces a homomorphism \( A'_n \to A'_\infty \).

**Proposition 3.2.** For all \( n \geq 0 \), we have

\[
H^1(\Gamma_n, \mathcal{E}_\infty') = \ker(A'_n \to A'_\infty).
\]

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 \( F_\infty/F \) 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 \( \ker(A'_n \to A'_\infty) \) 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 \( \ker(A'_n \to A'_\infty) \) 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 \( r_2p^n + s_n - 1 \). Moreover, since \( p \) is totally ramified in the extension \( \mathbb{Q}(\mu_p^\infty)/\mathbb{Q} \), it follows that there exists \( n_0 \geq 0 \) such that every prime above \( p \) is totally ramified in the extension \( F_\infty/F_{n_0} \). Hence, we conclude that \( s_n = s \), where \( s = s_{n_0} \) for all \( n \geq n_0 \). Thus, since \( H^1(\Gamma_n, \mathcal{E}_\infty') \) is finite, it follows from Proposition 3.1 that, provided \( n \geq n_0 \), the maximal divisible subgroup of \( (\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)_\Gamma \) has \( \mathbb{Z}_p \)-corank \( r_2p^n + s - 1 \).

Put

\[
Y'_\infty = \text{Hom}(\mathcal{E}_\infty' \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p).
\]

Then it follows immediately from Pontrjagin duality that \( (Y'_\infty)_\Gamma \) has \( \mathbb{Z}_p \)-rank \( r_2p^n + s - 1 \) for all \( n \geq n_0 \). Now \( Y'_\infty \) 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 Ex 1.2) that \( Y'_\infty \) has \( \Lambda(\Gamma) \)-rank equal to \( r_2 \). But Kummer theory immediately shows that

\[
Y'_\infty \otimes_{\mathbb{Z}_p} \text{Tr}_p(\mu) = \text{Gal}(N_\infty'/F_\infty).
\]
Thus Theorem B follows from the following simple algebraic exercise.

**Ex 3.1.** Let $W$ be any finitely generated $\Lambda(\Gamma)$-module. Assume $\mu_{p^{\infty}} \subset F_{\infty}$ and let $V = W \otimes_{\mathbb{Z}_p} T_p(\mu)$, where $\Gamma$ 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 $\text{Gal}(N'_{\infty}/F_{\infty})$. Let $t(\text{Gal}(N'_{\infty}/F_{\infty}))$ denote the $\Lambda(\Gamma)$-torsion submodule of $\text{Gal}(N'_{\infty}/F_{\infty})$. Then Iwasawa proves the following facts:

(i) $\text{Gal}(N'_{\infty}/F_{\infty})$ contains non non-zero $\mathbb{Z}_p$-torsion,

(ii) $t(\text{Gal}(N'_{\infty}/F_{\infty}))$ is a free $\mathbb{Z}_p$-module of rank $s - 1$ where $s$ = number of primes above $p$ in the extension $F_{\infty}/F_0$ as above, and he determines exactly its characteristic power series (even its structure up to pseudo-isomorphism), and

(iii) $\text{Gal}(N'_{\infty}/F_{\infty})/t(\text{Gal}(N'_{\infty}/F_{\infty}))$ is a free $\Lambda(\Gamma)$-module if and only if $H^1(\Gamma_n, \mathcal{E}'_{\infty}) = 0$ for all $n \geq a$, where $a$ is an explicitly determined integer $\leq s - 1$.

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

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

Passing to the inductive limit over all $m \geq n$, and noting that $H^i(\Gamma_n, W_{\infty}) = 0$ for all $i \geq 1$, Proposition 3.2 will then follow. Fix a generator $\sigma$ of $\text{Gal}(F_m/F_n)$, and write $\mathcal{O}'_m$ for the ring of $p$-integers of $F_m$. If $c$ is some element of $\ker(A'_n \rightarrow A'_m)$, and $a \in I_n$ is an ideal in $c$, then $a\mathcal{O}'_m = a\mathcal{O}'_m$ for some $\alpha \in \mathcal{O}'_m$. Define $\varepsilon = \sigma\alpha/\alpha$. Thus $\varepsilon$ 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 $\varepsilon$ in $H^1(\text{Gal}(F_m/F_n), E'_m)$ 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 $H^1(\text{Gal}(F_m/F_n), E'_m)$ which is represented by an element $\varepsilon$ of $E'_m$ with $\text{N}_{F_m/F_n}(\varepsilon) = 1$. By Hilbert’s Theorem 90, we then have $\varepsilon = \alpha^{\sigma-1}$ for some $\alpha \in \mathcal{O}'_m$. Let $a$ in $I'_n$ be given by $a = \alpha^{\mathcal{O}'_m}$. Since $\varepsilon$ is in $E'_m$, we see that $\alpha \mathcal{O}'_m = \mathcal{O}'_m$. Moreover, no prime of $F_m$ which does not divide $p$ is ramified in $F_m$, and so it follows that $a$ must be the image of an ideal $b$ in $I'_n$ under the natural inclusion $I'_n \hookrightarrow I'_m$. Let $c$ be the class of $b$ in $I'_n$. One sees easily that $c$ lies in $\ker(A'_n \rightarrow A'_m)$, and $\tau_{n,m} = \{\varepsilon\}$, completing the proof.

**Lecture 4.**

We now rapidly explain Iwasawa’s proof of Theorem A. Let $F_{\infty}/F$ be an arbitrary $\mathbb{Z}_p$-extension. For each $n \geq 0$, let $\mathcal{O}'_n$ be the ring of $p$ integers of $F_n$, $I'_n$ the group of invertible $\mathcal{O}'_n$-ideals, $P'_n \subset I'_n$ the group of principle invertible $\mathcal{O}'_n$-ideals, and $A'_n$ the $p$-primary subgroup of $I'_n/P'_n$. If $n \leq m$, we have the two natural homomorphisms

$$i_{n,m} : A'_n \rightarrow A'_m, \quad N_{m,n} : A'_m \rightarrow A'_n$$

which are respectively induced by the natural inclusion of $I'_n$ into $I'_m$ and the norm map from $I'_m$ to $I'_n$. We then define the $\Gamma$-modules

$$A'_\infty = \lim_{\rightarrow} A'_n, \quad W'_\infty = \lim_{\leftarrow} A'_n,$$

where the inductive limit is taken with respect to the $i_{n,m}$ and the projective limit is taken with respect to the $N_{m,n}$, and both are endowed with their natural action of $\Gamma$. Thus $A'_\infty$ is a discrete $\Lambda(\Gamma)$-module, and $W'_\infty$ is a compact $\Lambda(\Gamma)$-module.
Proposition 4.1. \(W'_\infty\) is canonically isomorphic as a \(\Lambda(\Gamma)\)-module to \(\text{Gal}(L'_\infty/F_\infty)\) where \(L'_\infty\) denotes the maximal unramified abelian \(p\)-extension of \(F_\infty\), in which every prime \(F_\infty\) lying above \(p\) splits completely.

Proof. Let \(L'_n\) be the maximal unramified abelian \(p\)-extension of \(F_n\) in which every prime above \(p\) splits completely. By global class field theory, the Artin map induces an isomorphism \(A'_n \sim \text{Gal}(L'_n/F_n)\), which preserves the natural action of \(\Gamma/\Gamma_n\) on both abelian groups. Let \(n_0 \geq 0\) be such that every prime of \(F_{n_0}\) which is ramified in \(F_\infty\) is totally ramified in \(F_\infty\). Thus, if \(m \geq n \geq n_0\), we must have \(L_n \cap F_m = F_n\), so that \(\text{Gal}(L'_n F_m/F_m) \sim \text{Gal}(L'_n/F_n)\). Moreover, global class field theory then tells us that the diagram

\[
A'_m \xrightarrow{\sim} \text{Gal}(L'_m/F_m) \\
\downarrow \quad \downarrow \\
A'_n \xrightarrow{\sim} \text{Gal}(L'_n F_m/F_m) = \text{Gal}(L'_n/F_n)
\]

is commutative. Hence, \(W_\infty = \lim_{\rightarrow} A'_n\) is isomorphic as a \(\Lambda(\Gamma)\)-module to \(\text{Gal}(R_\infty/F_\infty)\), where \(R_\infty = \bigcup_{n \geq 0} L_n\). Obviously, \(R_\infty \subset L_\infty\). But every element of \(L'_\infty\) satisfies an equation with coefficients in \(F_n\) for some \(n \geq n_0\), whence we see that also \(L'_\infty \subset R_\infty\), and so \(L'_\infty = R_\infty\), and \(W_\infty\) is isomorphic as a \(\Lambda(\Gamma)\)-module to \(\text{Gal}(L'_\infty/F_\infty)\), as required. \(\square\)

Proposition 4.2. Let \(s \geq 1\) be the number of primes of \(F_\infty\) which are ramified in the \(\mathbb{Z}_p\)-extension \(F_\infty/F\). Then, for all \(n \geq n_0\), we have that

\[
\text{\(Z_p\)-rank of } (W'_\infty)_{\Gamma_n} \leq s - 1.
\]

In particular, \(W'_\infty\) is a torsion \(\Lambda(\Gamma)\)-module.

Proof. For each \(n \geq 0\), let \(\mathcal{L}'_n\) denote the maximal abelian extension of \(F_n\) contained in \(L'_\infty\). Obviously, \(\mathcal{L}'_n \supset F_\infty\), and by the definition of the \(\Gamma\)-action on \(W'_\infty = \text{Gal}(L'_\infty/F_\infty)\), we have

\[
(W'_\infty)_{\Gamma_n} = \text{Gal}(\mathcal{L}'_n/F_\infty).
\]

Assume now that \(n \geq n_0\), so that there are precisely \(s\) primes of \(F_n\) which are ramified in the extension \(\mathcal{L}'_n/F_n\). Denote these primes by \(w_i\) \((i = 1, \ldots, s)\), and let \(T_i\) be the inertia group of \(w_i\) in \(\mathcal{L}'_n/F_n\). Since \(w_i\) is completely ramified in \(F_\infty/F_n\), and then splits completely in \(\mathcal{L}'_n/F_\infty\), we must have \(T_i \sim \Gamma_n \sim \mathbb{Z}_p\) for \(i = 1, \ldots, s\). Now, \(L'_n\) is the maximal unramified extension of \(F_n\) contained in \(\mathcal{L}'_n\). Hence

\[
\text{Gal}(\mathcal{L}'_n/L'_n) = T_1 \cdots T_s.
\]

Since \(\text{Gal}(L'_n/F_n)\) is finite, we conclude that the module \(\text{Gal}(\mathcal{L}'_n/F_n)\) has \(\mathbb{Z}_p\)-rank at most \(s\). As \(\text{Gal}(F_\infty/F_n)\) has \(\mathbb{Z}_p\)-rank equal to 1, it follows that

\[
\text{\(Z_p\)-rank of } \text{Gal}(\mathcal{L}'_n/F_\infty) \leq s - 1\text{ for all } n \geq n_0.
\]

In view of (5), it now follows from the structure theory that \(W'_\infty\) is a torsion \(\Lambda(\Gamma)\)-module, as claimed. \(\square\)

We end these notes by explaining, without proofs, the precise relationship between \(W'_\infty\) and \(\text{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)\) as \(\Lambda(\Gamma)\)-modules, which shows, in particular, that \(\text{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)\) is also a
torsion $\Lambda(\Gamma)$-module. Let $X$ be any finitely generated torsion $\Lambda(\Gamma)$-module. We define the $\Lambda(\Gamma)$-module $\alpha(X)$, called the adjoint of $X$ by

$$\alpha(X) = \text{Ext}^1_{\Lambda(\Gamma)}(X, \Lambda(\Gamma)).$$

It turns out that $\alpha(X)$ is pseudo-isomorphic to $X$, and contains no non-zero finite $\Lambda(\Gamma)$-submodule.

**Theorem 4.3.** $\text{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = \alpha(\text{Gal}(L'_\infty/F_\infty L'_n))$. Hence $\text{Hom}(A'_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is pseudo-isomorphic to $W'_\infty = \text{Gal}(L'_\infty/F_\infty)$, and so is $\Lambda(\Gamma)$-torsion.