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 $a_0, \cdots, a_{n-1} \in p\mathbb{Z}_p$. 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

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

where D_1 and D_2 have finite cardinality, and $f_i \neq 0$ for $i = 1, \ldots, m$. Moreover, the ideal $c(X) = f_1 \ldots f_m \Lambda(\Gamma)$ 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 $\geqslant 0$, $q_X(T)$ 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.

Ex 1. Assume X in $\mathfrak{R}(\Gamma)$ 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 $\mathfrak{R}(\Gamma)$, 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

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

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

$$\mathbb{Q}_p\text{-dimension of}\left((X)_{\Gamma_n} \underset{\mathbb{Z}_p}{\otimes} \mathbb{Q}_p\right) = m\, p^n + \delta_n,$$

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 $\dim_{\mathbb{Q}_p}(W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. 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 $\equiv 1 \bmod v$ 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 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma$, 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.

<u>Ex 4</u>. 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.

<u>Proposition</u> 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.

<u>Proof</u>. 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 $\mathrm{Gal}(J_\infty/F)$.