Generalities on Iwasawa Theory

Gürkan Dogan

Universität Duisburg-Essen

ESAGA Research Seminar, Summer Term 2020

May 28, 2020

Overview

Preliminaries - Assumptions

Throughout the section, A is a commutative, Noetherian and integrally closed domain with $Quot(A) = K$. We let

$$\mathcal{P}(A) = \{\mathfrak{p} \subseteq A \text{ prime} \mid \mathrm{ht}(\mathfrak{p}) = 1\}.$$

Observe that $A_\mathfrak{p}$ is a DVR for any $\mathfrak{p} \in \mathcal{P}(A)$, and we have

$$A = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} A_\mathfrak{p}.$$

Reflexive Modules

Definition

An A-module M is reflexive if

$$\varphi_M : M \to M^{++} = \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A),$$
$$m \mapsto (f \mapsto f(m))$$

is an isomorphism.

If M is a finitely-generated torsion-free A-module, then for any prime $\mathfrak{p}$, $M_{\mathfrak{p}}$ is a torsion-free $A_{\mathfrak{p}}$-module and we have

$$M \hookrightarrow M_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K = M \otimes_A K =: V,$$

$$M^+ \hookrightarrow (M^+)_{\mathfrak{p}} \hookrightarrow (M^+)_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K = M^+ \otimes_A K = \mathrm{Hom}_K(V, K) = V^\vee.$$

If M is a finitely-generated torsion-free A-module, then for any prime $\mathfrak{p}$, $M_\mathfrak{p}$ is a torsion-free $A_\mathfrak{p}$-module and we have

$$M \hookrightarrow M_\mathfrak{p} \hookrightarrow M_\mathfrak{p} \otimes_{A_\mathfrak{p}} K = M \otimes_A K =: V,$$

$$M^+ \hookrightarrow (M^+)_\mathfrak{p} \hookrightarrow (M^+)_\mathfrak{p} \otimes_{A_\mathfrak{p}} K = M^+ \otimes_A K = \mathrm{Hom}_K(V, K) = V^\vee.$$

Thus,

$$M^+ \simeq \{\lambda \in V^\vee \mid \lambda(m) \in A \ \forall m \in M\},$$

$$(M^+)_\mathfrak{p} \simeq \{\lambda \in V^\vee \mid \lambda(m) \in A_\mathfrak{p} \ \forall m \in M_\mathfrak{p}\} = (M_\mathfrak{p})^+ =: M_\mathfrak{p}^+.$$

Proposition

Let M be a finitely-generated torsion-free A-module. Then

$$(i)\ M^+ = \bigcap_{\mathfrak{p}\in\mathcal{P}(A)} M_{\mathfrak{p}}^+,$$

$$(ii)\ M^{++} = \bigcap_{\mathfrak{p}\in\mathcal{P}(A)} M_{\mathfrak{p}},$$

$$(iii)\ M = \bigcap_{\mathfrak{p}\in\mathcal{P}(A)} M_{\mathfrak{p}} \text{ if and only if } M \text{ is reflexive.}$$

Proof.

For item (i), let $\lambda \in \bigcap_{\mathfrak{p} \in P(A)} M_{\mathfrak{p}}^{+}$. Then for all $m \in M$, $\lambda(m) \in A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathcal{P}(A)$. So for all $m \in M$, $\lambda(m) \in \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} A_{\mathfrak{p}} = A$, hence $\lambda \in M^{+}$.

As for item (ii), since $M_{\mathfrak{p}}$ is a finitely-generated torsion-free module over $A_{\mathfrak{p}}$ that is a DVR, $M_{\mathfrak{p}}$ is free and hence is reflexive. So we get by (i) that $\bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M_{\mathfrak{p}} = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M_{\mathfrak{p}}^{++} = M^{++}$.

Finally, (iii) is obvious from (ii). □

Corollary

If M is a finitely-generated A-module, then M^+ is reflexive.

Proof.

$M^+ = \mathrm{Hom}_A(M, A)$ is a finitely-generated torsion-free A-module. Using (ii) and (i) of the above proposition respectively, we get

$$M^{+++} = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M_{\mathfrak{p}}^+ = M^+.$$

□

Pseudo-Null Modules and Pseudo-Isomorphisms

Definition

A finitely-generated A-module M is pseudo-null if $M_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$ of A with $\mathrm{ht}(\mathfrak{p}) \leq 1$.

Definition

A homomorphism $f : M \to N$ of finitely-generated A-modules is called a pseudo-isomorphism if ker(f) and coker(f) are pseudo-null; equivalently, if $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is an isomorphism for all $\mathfrak{p}$ with $\mathrm{ht}(\mathfrak{p}) \leq 1$. We write $f : M \xrightarrow{\approx} N$.

Proposition

Let M be a finitely-generated A-module. Let $T_A(M)$ be its torsion submodule. Then there exist a finite family $(\mathfrak{p}_i)_i$ of prime ideals of height 1 in A, a finite family $(n_i)_i$ of natural numbers and a pseudo-isomorphism

$$g : T_A(M) \xrightarrow{\approx} \bigoplus_i A/\mathfrak{p}_i^{n_i}.$$

Proof.

Let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\} = \mathrm{supp}(T_A(M)) \cap \mathcal{P}(A)$ and assume $h > 0$. Let $S = \bigcap_{i=1}^{h} A \setminus \mathfrak{p}_i$. Then, being a semi-local Dedekind domain (the maximal ideals of $S^{-1}A$ are $\mathfrak{p}_i$), $S^{-1}A$ is a PID. Since $S^{-1}A$-module $S^{-1}T_A(M)$ is the torsion submodule of $S^{-1}M$, using the structure theorem, we can let

$$E \simeq \bigoplus_{i=1}^{h} \bigoplus_{j=1}^{r_i} A/{\mathfrak{p}_\mathfrak{i}}^{n_j}$$

such that there is an isomorphism $g_0 : S^{-1}T_A(M) \to S^{-1}E$. Using the ismorphism $\mathrm{Hom}_{S^{-1}A}(S^{-1}T_A(M), S^{-1}E) \simeq S^{-1}\mathrm{Hom}_A(T_A(M), E)$, we obtain a morphism $g : T_A(M) \to E$ such that there is $s \in S$ with $g = sg_0$. Then g is indeed a pseudo-isomorphism. □

Iwasawa Modules - Assumptions

Let $\mathcal{O}$ be a commutative, Noetherian local ring with maximal ideal $\mathfrak{m}$, with finite residue field $k = \mathcal{O}/\mathfrak{m}$, complete in its $\mathfrak{m}$-adic topology. Let $p = \text{char}(k)$ and $\Gamma \simeq \mathbb{Z}_p$, a free pro-p group of rank 1.

We consider the complete group algebra of Γ over $\mathcal{O}$ given by

$$\mathcal{O}[[\Gamma]] = \varprojlim_n \mathcal{O}[\Gamma/\Gamma_n],$$

where Γ_n runs through the open normal subgroups of Γ.

Proposition

Assume γ *is a topological generator of* $\Gamma \simeq \mathbb{Z}_p$*. Then there is an isomorphism*

$$\mathcal{O}[[T]] \to \mathcal{O}[[\Gamma]],\ T \mapsto \gamma - 1.$$

Definition

The complete group ring $\Lambda = \mathbb{Z}_p[[\Gamma]]$ is called the Iwasawa algebra and a compact Λ-module an Iwasawa module.

Lemma

The prime ideals of height 1 *in* Λ *are* $\mathfrak{p} = (p)$ *and* $\mathfrak{p} = (F)$, *where* F *is a Weierstraß polynomial over* $\mathbb{Z}_p$; *i.e., a polynomial of the form* $F = T^s + a_{s-1}T^{s-1} + \cdots + a_0$ *with coefficients in* $a_i \in (p)$.

Lemma

The prime ideals of height 1 *in* Λ *are* $\mathfrak{p} = (p)$ *and* $\mathfrak{p} = (F)$, *where* F *is a Weierstraß polynomial over* $\mathbb{Z}_p$; *i.e., a polynomial of the form* $F = T^s + a_{s-1}T^{s-1} + \cdots + a_0$ *with coefficients in* $a_i \in (p)$.

Proposition

Let M *be a finitely-generated* A*-module. Let* $T_A(M)$ *be the torsion submodule. Then there exist a finite family of prime ideals* $(\mathfrak{p}_i)_i$ *of height* 1 *in* A, *a finite family* $(n_i)_i$ *of natural numbers and a pseudo-isomorphism*

$$g : T_A(M) \xrightarrow{\approx} \bigoplus_i A/\mathfrak{p}_i^{n_i}.$$

Structure Result for Iwasawa Modules

We see that if M is a finitely-generated torsion Iwasawa module, then there exist irreducible Weierstraß polynomials F_j, numbers m_i, n_j and a pseudo-isomorphism

$$M \xrightarrow{\approx} \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/F_j^{n_j}.$$

We define the characteristic polynomial of M by

$$p^{\mu} \prod_{j=1}^{t} F_j^{n_j},$$

where $\mu = \sum_{i=1}^{s} m_i$ is the μ-invariant.

We define the characteristic polynomial of M by

$$p^{\mu} \prod_{j=1}^{t} F_j^{n_j},$$

where $\mu = \sum_{i=1}^{s} m_i$ is the μ-invariant. The first Chern class of M is

$$\begin{aligned} c_1(M) &= \text{length}_{\Lambda_p}(M_p) \cdot (p) + \sum_{j=1}^{t} \text{length}_{\Lambda_{(F_j)}}(M_{(F_j)}) \cdot (F_j) \\ &= \mu \cdot (p) + \sum_{j=1}^{t} n_j \cdot (F_j). \end{aligned}$$

Leopoldt Conjecture

Let K be a number field, and let r_1 and r_2 be the number of real and complex places of K, respectively. For every local field $k \mid \mathbb{Q}_p$, there is a uniquely defined logarithm map on $k^\times$, which extends to a function $\log_p : \mathbb{C}_p^\times \to \mathbb{C}_p$. We consider

$$j_p : K^\times \to \prod_{\sigma \in \mathrm{Hom}(K, \mathbb{C}_p)} \mathbb{C}_p^\times \xrightarrow{\prod_\sigma \log_p(\ )} \prod_{\sigma \in \mathrm{Hom}(K, \mathbb{C}_p)} \mathbb{C}_p,$$

defined by

$$j_p(x)_\sigma := \log_p(\sigma(x)).$$

Let $\epsilon_1, \dots, \epsilon_{r_1+r_2-1}$ be a basis for the unit group E_K of K modulo torsion. We list the elements of $\mathrm{Hom}(K, \mathbb{C}_p)$ as $\sigma_1, \dots, \sigma_d$ where $d = [K : \mathbb{Q}]$.

Definition

We define the regulator matrix

$$\mathcal{R}_p(\epsilon_1, \dots, \epsilon_{r_1+r_2-1}) = \begin{pmatrix} \log_p \sigma_1(\epsilon_1) & \dots & \log_p \sigma_d(\epsilon_1) \\ \vdots & & \vdots \\ \log_p \sigma_1(\epsilon_{r_1+r_2-1}) & \dots & \log_p \sigma_d(\epsilon_{r_1+r_2-1}) \end{pmatrix}$$

and call the rank

$$\mathrm{rr}_p(K) = \mathrm{rank}(\mathcal{R}_p(\epsilon_1, \dots, \epsilon_{r_1+r_2-1}))$$

the p-adic regulator rank of K.

Leopoldt's Conjecture

We have

$$\mathrm{rr}_p(K) = r_1 + r_2 - 1.$$

Leopoldt's Conjecture

We have

$$\mathrm{rr}_p(K) = r_1 + r_2 - 1.$$

Theorem

Let S be a finite set of places of K containing $S_p \cup S_\infty$. Then Leopoldt Conjecture holds if and only if $\mathrm{rank}_{\mathbb{Z}_p} H_1(G_S(K), \mathbb{Z}_p) = r_2 + 1$.

We have

$$r_1 + r_2 + 1 - \mathrm{rr}_p(K) = \mathrm{rank}_{\mathbb{Z}_p} H_1(G_S(K), \mathbb{Z}_p) - r_2 - 1,$$

which we define as the Leopoldt defect δ_p. So Leopoldt's Conjecture holds for K and p if and only if $\delta_p = 0$.

Definition

Let $L \mid K$ be a Galois extension. We call L a $\mathbb{Z}_p$-extension of K if $\mathrm{Gal}(L \mid K) \simeq \mathbb{Z}_p$. The cyclotomic $\mathbb{Z}_p$-extension of K is given by the compositum $K\mathbb{Q}_\infty$, where $\mathbb{Q}_\infty$ is the (unique) cyclotomic $\mathbb{Z}_p$ extension of $\mathbb{Q}$.

Definition

Let $L \mid K$ be a Galois extension. We call L a $\mathbb{Z}_p$-extension of K if $\mathrm{Gal}(L \mid K) \simeq \mathbb{Z}_p$. The cyclotomic $\mathbb{Z}_p$-extension of K is given by the compositum $K\mathbb{Q}_\infty$, where $\mathbb{Q}_\infty$ is the (unique) cyclotomic $\mathbb{Z}_p$ extension of $\mathbb{Q}$.

Note that the composite of all $\mathbb{Z}_p$-extensions of K is the maximal p-extension of K with a torsion-free Abelian group. This means that

$$\mathrm{rank}_{\mathbb{Z}_p} H_1(G_K, \mathbb{Z}_p)$$

is the (possibly infinite) number of independent $\mathbb{Z}_p$-extensions of K.

Proposition

If K is a number field, then every $\mathbb{Z}_p$-extension is unramified outside p and is ramified at least at one prime dividing p. The number of independent $\mathbb{Z}_p$-extensions of K is equal to $r_2 + 1 + \delta_p$. In particular, we have

$$\textit{rank}_{\mathbb{Z}_p} G_S(K)^{ab}(p) = r_2 + 1 + \delta_p \leq [K : \mathbb{Q}].$$

Corollary

Let $\widetilde{K}$ be the composite of all $\mathbb{Z}_p$-extensions of K. Then

$$Gal(\widetilde{K}/K) \simeq \mathbb{Z}_p^{r_2+1+\delta_p}.$$

Let K be a CM-extension of $\mathbb{Q}$ of degree $2d$ and K^+ its maximal totally real subfield. Let p be an odd prime such that each prime over p in K^+ splits in K. Let $\widetilde{K}$ be the compositum of all $\mathbb{Z}_p$-extensions of K. Let $\Gamma = \mathrm{Gal}(\tilde{K}/K)$. Let $r = \mathrm{rank}_{\mathbb{Z}_p}(\Gamma)$, $r_{\mathfrak{p}} = \mathrm{rank}_{\mathbb{Z}_p}(\Gamma_{\mathfrak{p}})$, and $d_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_{\mathfrak{p}}]$ for $\mathfrak{p} \in S_f = \{\text{primes over } p \text{ in } K\}$. Finally, by a CM type, we mean a set consisting of one prime of K over each of the primes over p in K^+.

Lemma

We have

(i) $r_{\mathfrak{p}} = d_{\mathfrak{p}} + 1$,

(ii) *The extension* $\widetilde{K}/K$ *has infinite residue field degree at* $\mathfrak{p}$.

Proof.

Complex conjugation acts on Γ by conjugation and leads to a decomposition $\Gamma = \Gamma^+ \oplus \Gamma^-$, where we view $\Gamma^\pm$ as quotients of Γ. Then Γ^+ corresponds to the $\mathbb{Z}_p$-extensions over the totally real subfield K^+, among which is the cyclotomic $\mathbb{Z}_p$-extension. Since no place over p splits completely in the cyclotomic $\mathbb{Z}_p$-extension, the decomposition group $(\Gamma^+)_\mathfrak{p}$ is non-trivial and we get for each $\mathfrak{p}$

$$\text{rank}_{\mathbb{Z}_p}(\Gamma^+)_\mathfrak{p} \geq 1$$

(with equality if Leopoldt's Conjecture holds, since in that case we have $\text{rank}_{\mathbb{Z}_p}\Gamma^+ = 1$). □

Proof. (continued)

By class field theory, we have an exact sequence

$$\mathcal{O}_K^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \bigoplus_{\mathfrak{p}\in S_f} \mathcal{O}_{K_\mathfrak{p}}^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \Gamma \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 0.$$

Since $\mathcal{O}_K^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathcal{O}_{K^+}^\times \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, the minus part of the leftmost term vanishes and we get an isomorphism between the minus part of the second term and $\Gamma^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Since $d = \sum_{\mathfrak{p}\in\Sigma} d_\mathfrak{p} = \mathrm{rank}_{\mathbb{Z}_p}\Gamma^-$ for any CM type Σ, we get at a prime $\mathfrak{p} \in S_f$,

$$\mathrm{rank}_{\mathbb{Z}_p}(\Gamma^-)_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p] = d_\mathfrak{p},$$

which implies $r_\mathfrak{p} \geq d_\mathfrak{p} + 1$.

Proof. (continued)

On the other hand, by class field theory the $\mathbb{Z}_p$-rank of the maximal pro-p quotient of $G_{K_\mathfrak{p}}^{\mathsf{ab}}$ is equal to that of the pro-p completion of $K_\mathfrak{p}^\times$, which is $d_\mathfrak{p} + 1$. Since $\Gamma_\mathfrak{p} = \mathsf{Gal}(\widetilde{K_\mathfrak{p}}/K_\mathfrak{p})$ is a subgroup of this quotient and $\mathsf{rank}_{\mathbb{Z}_p}\Gamma_\mathfrak{p} = r_\mathfrak{p}$, we get $r_\mathfrak{p} \leq d_\mathfrak{p} + 1$. Hence the equality.

For (ii), considering the exact sequence

$$0 \to \mathcal{I}_\mathfrak{p} \to \Gamma_\mathfrak{p} \to \mathsf{Gal}(k(\widetilde{K}_\mathfrak{p})/k(K_\mathfrak{p})) \to 0,$$

we see that $\mathsf{rank}_{\mathbb{Z}_p}\mathsf{Gal}(k(\widetilde{K}_\mathfrak{p})/k(K_\mathfrak{p})) \geq 1$, hence is infinite, as desired.

Greenberg's Conjecture

Greenberg's Conjecture

Let K be an arbitrary number field, and let $\widetilde{K}$ be the composite of all $\mathbb{Z}_p$-extensions of K. Let $\Gamma = \mathrm{Gal}(\widetilde{K}/K)$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Let L be the maximal Abelian, unramified pro-p-extension of $\widetilde{K}$, and let $X = \mathrm{Gal}(L/\widetilde{K})$, the unramified Iwasawa module over $\widetilde{K}$. Then X is a pseudo-null Λ-module.

The Conjecture is verified for when K is an imaginary quadratic field and p doesn't divide the class number of K.

Thanks for your attention!