Iwasawa theory

A quick overview

Óscar Rivero Salgado

TCC Course on Iwasawa theory

10/12/2021

This session

Overview

Iwasawa theory

TCC Course

- Instructor: Óscar Rivero Salgado (University of Warwick).
- Email: Oscar.Rivero-Salgado@warwick.ac.uk
- Write to me if you want to follow this course, and please indicate the following:
  - Your name, institution and year.
  - Your background in number theory.
  - Whether you are taking the course for credit or not.
- This course is administrated by the Taught Course Centre (TCC) and available to the Universities of Bath, Bristol, Imperial, Oxford and Warwick.

Iwasawa theory

TCC Course

- **Schedule:** Tuesday mornings, from 10.00 to 12.00. Five minute break around 11.00.
- First class on October 12th and last class on November 30th.
- The materials will be available at the web-page of the course: https://www.oscarrivero.org/tcc-iwasawa.
  - Materials for the lectures.
  - Exercise sheet.
  - Glossary of things we assume along the course (algebraic number theory or p-adic numbers).
- Only this first class will be using slides. The rest of the days I will use a tablet.

Cyclotomic fields

Brief review

- Iwasawa theory begins with the study of cyclotomic fields.
- It dates back to attempts at proving Fermat's last theorem (mid 1800's).
- The N-th cyclotomic field $\mathbb{Q}(\zeta_N)$ is given by adjoining the primitive N-root of unity $\zeta_N = e^{2\pi i/N}$ to $\mathbb{Q}$.
- Each element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ carries ζ_N to another primitive N-th root of unity, ζ_N^i, with $(i, N) = 1$.
- Isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times,$$

known as the N-th cyclotomic character.

Bernoulli numbers

Kummer's criterion

- A prime p is called irregular if p divides the class number of $\mathbb{Q}(\zeta_p)$, and regular elsewhere.
- For $k \geq 0$, the k-th Bernoulli number $B_k \in \mathbb{Q}$ is the k-th derivative at 0 of $\frac{x}{e^x-1}$.

Theorem (Kummer)

A prime p is irregular if and only if p divides the numerator of B_k for some positive even $k < p$.

- Relation between algebraic object (class group) and analytic one (Bernoulli number).
- Let A be the p-part of the class group. What more does the fact an odd p divides a particular Bernoulli number tell us about A?

The Herbrand–Ribet theorem

A very remarkable result

- Consider the action of $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ on A.
- For $\delta \in (\mathbb{Z}/p\mathbb{Z})^\times$, there is a unique element $\omega(\delta) \in \mathbb{Z}_p^\times$ of order dividing $p-1$ reducing to δ.
- Hence, the group A breaks up as a direct sum

$$A = \bigoplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} A^{(i)},$$

$$A^{(i)} = \{a \in A \text{ such that } \delta(a) = \omega(\delta)^i a \text{ for all } \delta \in \Delta\}.$$

Theorem (Herbrand–Ribet)

If k is a positive even integer with $0 < k < p-1$, then p divides B_k if and only if $A^{(p-k)} \neq 0$.

Towers of fields

Brief review

- Iwasawa theory: growth of arithmetic objects in towers of number fields.
- Base field F. For simplicity, we may take $F = \mathbb{Q}(\zeta_p)$ (make some results easier).
- Sequence F_n of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_\infty = \cup_{n=0}^{\infty} F_n,$$

  with F_n/F cyclic of degree p^n. When $F = \mathbb{Q}(\zeta_p)$, you may consider for instance the case $F_n = \mathbb{Q}(\zeta_{p^{n+1}})$.
- The Galois group $\Gamma = \mathrm{Gal}(F_\infty/F)$ is the inverse limit of the groups $\Gamma_n = \mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$. Isomorphic to $\mathbb{Z}_p$ (and it is thus a compact group under the p-adic topology).

Towers of fields

Galois extensions of number fields

Theorem (Iwasawa)

There exist non-negative integers λ and μ and an integer ν such that $|A_n| = p^{p^n\mu+n\lambda+\nu}$ for all sufficiently large n.

- A_n is a module over $\mathbb{Z}_p$. It is endowed with a Γ_n-action: module for the group ring $\mathbb{Z}_p[\Gamma_n]$.
- Comparing the different A_n: either via norm maps $A_{n+1} \to A_n$, or via maps $A_n \to A_{n+1}$ induced by the inclusion of F_n in F_{n+1}.
- Compatible with the action of $\mathbb{Z}_p[\Gamma_{n+1}]$ on both sides, with the action on A_n arising through the restriction map $\Gamma_{n+1} \to \Gamma_n$.
- $\Lambda = \varprojlim \mathbb{Z}_p[\Gamma_n]$ acts on both the inverse limit $\varprojlim A_n$ and the direct limit $A_\infty = \varinjlim A_n$.

Artin map

Review of class field theory

- L_n maximal unramified abelian p-extension of F_n. Artin map: $A_n \cong \mathrm{Gal}(L_n/F_n)$. Compatible with norms on class groups and restriction on Galois groups.
- Identification of $\lim_{\leftarrow} A_n$ with $Y_\infty = \mathrm{Gal}(L_\infty/F_\infty)$.
- Γ-action on the inverse limit of the A_n is identified via the Artin isomorphisms with the conjugation of Γ on Y_∞. Lift $\gamma \in \Gamma$ to $\tilde{\gamma} \in \mathrm{Gal}(L_\infty/F)$, so γ acts on $\sigma \in Y_\infty$ by

$$\gamma \ : \ \sigma \mapsto \tilde{\gamma}\sigma\tilde{\gamma}^{-1}.$$

- Y_∞ structure of Λ-module, finitely generated and torsion over Λ.
- Y_∞ compact as Λ-module, A_∞ discrete. Consider the Pontryagin dual $A_\infty^\vee = \mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$, finitely generated and torsion.

Structure theory

Some abstract algebra

- Λ is isomorphic to the power series ring $\mathbb{Z}_p[[T]]$. A homomorphism $f : M \to N$ of finitely generated Λ-modules is a pseudo-isomorphism if it has finite kernel and cokernel.

Theorem

For any finitely generated torsion Λ-module M, there is a pseudoisomorphism

$$M \longrightarrow \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j}),$$

where $r, s \geq 0$, each f_i is a monic irreducible polynomial in $\mathbb{Z}_p[T]$ such that $f_i \equiv T^{\deg f_i}$ modulo p, and each k_i and m_j is a positive integer.

Structure theory

Characteristic ideals

- $\lambda(M) = \sum_{i=1}^{r} k_i \deg f_i$ and $\mu(M) = \sum_{j=1}^{s} m_j$. The characteristic ideal is

$$\mathrm{char}(M) = \left(p^{\mu(M)} \prod_{i=1}^{r} f_i^{k_i} \right).$$

- In Y_∞, λ and μ are those in Iwasawa's growth formula. In several cases, like the one described above, it holds that $\mu = 0$.
- The module Y_∞ has an action of $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ commuting with the Λ-action.
- We can break up Y_∞ as a direct sum of Δ-eigenspaces.

p-adic L-functions

The analytic side

- The Riemann zeta function satisfies

$$\zeta(1-n) = -\frac{B_n}{n}.$$

- Kummer: for $m \equiv n \pmod{p^{j-1}(p-1)}$, then

$$(1-p^{m-1})\zeta(1-m) \equiv (1-p^{n-1})\zeta(1-n) \pmod{p^j}.$$

- Fix even k. There exists a continuous $\mathbb{Z}_p$-valued function $L_p(\omega^k, s)$ of a p-adic variable $s \in \mathbb{Z}_p$ satisfying

$$L_p(\omega^k, 1-n) = (1-p^{n-1})\zeta(1-n),$$

for all $n \equiv k \pmod{p-1}$.

- $L_p(\omega^k, s)$ determined on $s \in \mathbb{Z}_p$ by a unique power series $f_k \in \Lambda$ with

$$f_k((1+p)^s - 1) = L_p(\omega^k, s).$$

A result of Mazur–Wiles

Reformulating the conjecture

Theorem (Mazur–Wiles)

For any even integer k which is not a multiple of $p-1$, we have

$$char(Y_\infty^{(p-k)}) = (f_k).$$

- $X_\infty = \mathrm{Gal}(M_\infty/F_\infty)$, with M_∞ union of the maximal abelian p-extensions of the F_n ramified only at the unique prime $(1-\zeta_{p^{n+1}})$ over p.
- The main conjecture asserts that

$$\mathrm{char}(X_\infty^{(k)}) = (g_k),$$

where $g_k(T) = f_k((1+p)(1+T)^{-1}-1)$.

- Study of the image of the cyclotomic units inside the local units.

Iwasawa's result

Objective for the course

- The Iwasawa module $\mathcal{U}_\infty$ of norm compatible sequences of local units contains submodules $\mathcal{E}_\infty$ and $\mathcal{C}_\infty$, generated by the sequences of global units and cyclotomic units: $\mathcal{U}_\infty \supset \mathcal{E}_\infty \supset \mathcal{C}_\infty$.
- By class field theory there is an exact sequence

$$0 \to \mathcal{E}_\infty/\mathcal{C}_\infty \to \mathcal{U}_\infty/\mathcal{C}_\infty \to X_\infty \to Y_\infty \to 0.$$

Take the ω^k-eigenspace.

Theorem (Iwasawa)

There is an isomorphism of Λ-modules

$$\mathcal{U}_\infty^{(k)}/\mathcal{C}_\infty^{(k)} \cong \Lambda/(g_k).$$

- Enough to show that

$$\mathrm{char}(\mathcal{E}_\infty^{(k)}/\mathcal{C}_\infty^{(k)}) \cong \mathrm{char}(X_\infty^{(k)}).$$

Schedule

Tentative planning I

The following is subject to change as the course moves along.
Rather flexible. Depending on the pace of the course, we may skip some parts. Frequently, the exercises will be *technical lemmas* whose proofs we omit in classes for a matter of time.

- **Lecture 1** (October 12th). Overview of Iwasawa theory. Cyclotomic fields. Brief review of algebraic number theory and p-adic fields.
- **Lecture 2** (October 19th). Structure theory of $\mathbb{Z}_p[[T]]$-modules.
- **Lecture 3** (October 26th). Iwasawa's control theory on $\mathbb{Z}_p$-extensions (first part).
- **Lecture 4** (November 2nd). Iwasawa's control theory on $\mathbb{Z}_p$-extensions (second part).

Schedule

Tentative planning II

The following is subject to change as the course moves along.

- **Lecture 5** (November 9th). p-adic measures and the p-adic zeta function.
- **Lecture 6** (November 16th). Coleman power series.
- **Lecture 7** (November 23rd). The Iwasawa theorem.
- **Lecture 8** (November 30th). Either *A short introduction to Euler systems* or *A short introduction to Hida theory*, discussing the relations with the Iwasawa main conjecture.

I will try to emphasize natural continuations for the topics of the course: elliptic curves, modular forms...

References

Some books we will use

- J. Coates and R. Sujatha, *Cyclotomic Fields and Zeta Values*.
- L.C. Washington, *Introduction to Cyclotomic Fields*.
- R. Sharifi, *Iwasawa theory* (lecture notes).
- See Coates and Sharifi's courses at the Arizona Winter School 2018.

Background material?

- For the first lectures, take a look at any good book in Algebraic number theory.
- There are some notes on the Internet that can be potentially useful.

Assessment

Three problem sheets

Assessment will be based on three problem sheets, to be distributed after lectures 2/3, 5/6 and 7/8.

- **Sheet 1.** Review of algebraic number theory and structure of $\mathbb{Z}_p[[T]]$ modules.
  Deadline: November 9th.
- **Sheet 2.** Iwasawa's control theory on $\mathbb{Z}_p$-extensions.
  Deadline: November 30th.
- **Sheet 3.** p-adic measures and Coleman power series.
  Deadline: December 24th.

Each homework problem set is graded on the basis of a maximum score of 100. To pass the course, you need to get 180 points in total, and at least 40 in each problem sheet.

Assessment

Rules

- Solutions must be submitted to the lecturer by electronic mail (handwriting is allowed). Submissions beyond the deadline will not be considered.
- It is allowed working together with other students (unless otherwise specified), but the writing of the solutions is an individual process.
- It is also legit looking for hints at the course references or at internet forums, but it must be clear that the final submission must be written by the student.
- Try to write the solutions in the best way you can (as you would like to find them in a textbook). Clarity of exposition will be part of the mark!