Iwasawa theory

Background material

Óscar Rivero Salgado

TCC Course on Iwasawa theory

10/12/2021

p-adic numbers

We assume familiarity with the notion of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

- Algebraically:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

  $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$.

- Topologically: in $\mathbb{Q}$, consider the absolute value

$$|\cdot|_p : \mathbb{Q} \longrightarrow p^{\mathbb{Z}}, \quad p^n \cdot \frac{a}{b} \mapsto p^{-n},$$

  where $(ab, p) = 1$ and with the convention that $0 \mapsto 0$.
  Then, $\mathbb{Q}_p = \hat{\mathbb{Q}}$ with respect to this norm, and

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \text{ with } |x|_p \leq 1\}.$$

Valuations

A multiplicative valuation on a field K is a function

$$|\cdot| : K \longrightarrow \mathbb{R}, \quad x \mapsto |x|$$

satisfying the following properties.

(a) $|x| \geq 0$ for all x, and $|x| = 0$ if and only if $x = 0$.

(b) $|xy| = |x| \cdot |y|$ for all $x, y \in K$.

(c) $|x + y| \leq |x| + |y|$. If we further have $|x + y| \leq \max\{|x|, |y|\}$, we say that $|\cdot|$ is a non-archimedean valuation.

The additive valuation associated to $|\cdot|$ is

$$v : K^\times \longrightarrow \mathbb{R}, \quad x \mapsto v(x) = -\log |x|.$$

If $v(K^\times) \subset \mathbb{R}$ is discrete, we say that the valuation is discrete.

Non-archimedean valuations

- Non-archimedean valuation $|\cdot|$.

$$A = \{a \in K \text{ with } |a| \leq 1\}$$

  is the ring of integers of K or the valuation ring.
- The units of A are

$$A^{\times} = \{a \in K \text{ with } |a| = 1\},$$

- A has a unique maximal ideal given by

$$\mathfrak{m} = \{a \in K \text{ with } |a| < 1\}.$$

  The maximal ideal $\mathfrak{m}$ is principal if and only if the valuation is discrete.
- The residue field of A is $k = A/\mathfrak{m}$.

Uniformizing parameters

K field with a discrete non-archimedean valuation $|\cdot|$.

- A local uniformizing parameter π is an element of K such that $|\pi|$ has the largest value smaller than 1.
- π generates the maximal ideal $\mathfrak{m}$. We say that v is normalised if $v(\pi) = 1$.
- Note that $|\cdot|$ gives to K the structure of a metric space, and in particular there is a notion of completeness.
  For instance, if $K = \mathbb{Q}_p$:
  - The ring of integers is $\mathbb{Z}_p$,
  - The units are $\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$.
  - The maximal ideal is $p\mathbb{Z}_p$.
  - p is a uniformizer (or pu, with $u \in \mathbb{Z}_p^\times$).
  - The residue field is $\mathbb{Z}/p\mathbb{Z}$.

Some general results

K complete field with respect to a non-archimedean valuation $|\cdot|_K$. L/K finite separable extension. Let A be the discrete valuation ring of K, and k the residue field of A.

- A is a Dedekind domain (discrete valuation rings are Dedekind domain).
- The integral closure of A in L is also a Dedekind domain (more precisely, let A be a Dedekind domain, K its fraction field, and L/K a finite and separable extension. Let B stand for the integral closure of A in L. Then, B is a Dedekind domain).
- (Hensel's lemma) If $\bar{f} = g_0 h_0$, with g_0 and h_0 monic and coprime in $k[X]$, then there exist polynomials g, $h \in A[x]$, with $f = gh$, $\bar{g} = g_0$ and $\bar{h} = h_0$.

Extensions of valuations

Theorem

The valuation $|\cdot|_K$ extends uniquely to a discrete valuation $|\cdot|_L$ on L.

Proof.

- A and B Dedekind domains. The valuations of L extending $|\cdot|_K$ correspond to ideals in B above $\mathfrak{p}$.
- Assume there exist distinct primes $\mathfrak{P}_1, \mathfrak{P}_2$ in B dividing $\mathfrak{p}$. Then, there exists $\beta \in B$ such that $\mathfrak{P}_1 \cap A[\beta] \neq \mathfrak{P}_2 \cap A[\beta]$.
- $f(x)$ be the minimal polynomial of β over K. $A[\beta] \cong A[x]/(f(x))$.
- $\bar{f}(x)$ is the power of an irreducible polynomial (Hensel).
- $A[\beta]/\mathfrak{p}A[\beta] = (A/\mathfrak{p})[x]/(\bar{f}(x))$, a contradiction.

Uniformizing parameters and extensions

Let A and B be the integer rings of K and L, respectively. π and Π uniformizing parameters, and v_K, v_L for the normalized additive valuations. $\mathfrak{p} = (\pi)$ and $\mathfrak{P} = (\Pi)$

- $\mathfrak{p}B = \mathfrak{P}^e$, so $(\pi)B = (\Pi^e)$. There exists $u \in B^\times$ such that $\pi = u\Pi^e$. Then, if v_L normalized, $v_L(\pi) = e$.
- If we want to extend the valuation, that is, finding $\tilde{v}$ on L such that $\tilde{v}|_K = v_K$, then $\tilde{v}(\Pi) = 1/e$.
- We say that L/K is unramified if $e = 1$. The extension is said to be totally ramified if $e = [L : K]$.

The arithmetic of number fields

Let F be a number field. We recall several objects attached to F and finite field extensions of it.

- The ring of integers $\mathcal{O}_F$ of F.
- The unit group $\mathcal{O}_F^\times$ of F, which is to say the unit group of $\mathcal{O}_F$.
- The ideal group I_F of F, i.e., the group of non-zero finitely generated $\mathcal{O}_F$-submodules of F.
- The principal ideal group P_F of F, i.e., those $\mathcal{O}_F$-submodules (α) of F generated by a single element $\alpha \in F^\times$.
- The class group $\mathrm{Cl}_F = I_F/P_F$ of F.

The absolute norm $N\mathfrak{a}$ of a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_F$ is the index $N\mathfrak{a} = [\mathcal{O}_F : \mathfrak{a}]$.

Class groups and Dirichlet's theorem

The number of real places of F is denoted $r_1(F)$ and the number of complex places of F is denoted $r_2(F)$.
Two of the most important results in a first course of algebraic number theory are the following ones:

1. The class group Cl_F is a finite abelian group.
2. (Dirichlet's unit theorem). The unit group $\mathcal{O}_F^\times$ is a finitely generated abelian group of rank $r_1(F) + r_2(F) - 1$ with torsion subgroup the group $\mu(F)$ of roots of unity in F.

Factorization in extensions

We assume knowledge of the following concepts regarding an extension of number fields E/F and how primes of F factor at the extension of E. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$, and write

$$\mathfrak{p}\mathcal{O}_E = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \quad e_i \geq 1.$$

You should be familiarised with the following notions.

- Ramification and inertia degree ($f_i = [\mathcal{O}_E/\mathfrak{P}_i : \mathcal{O}_F/\mathfrak{p}]$).
- Formula $\sum_i e_i f_i = n$. The Galois case (all the e_i are equal, and all the f_i are equal too).
- Decomposition and inertia groups.
- Frobenius element.

The Frobenius elements

- For any Galois extension E/F and prime $\mathfrak{p}$ of F, let $\varphi_{\mathfrak{P}}$ denote a Frobenius at a prime $\mathfrak{P}$ over $\mathfrak{p}$.
- We have

$$\varphi_{\mathfrak{P}}(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

  for all $\alpha \in \mathcal{O}_E$.
- If E/F is unramified, the conjugacy class of the Frobenius in $\mathrm{Gal}(E/F)$ depends only on $\mathfrak{p}$, and we denote it by $[\varphi_{\mathfrak{p}}]$.
- If E/F is abelian and unramified, we just write $\varphi_{\mathfrak{p}}$.

Cyclotomic fields

- ζ is a primitive n-th root of 1 if $\zeta^n = 1$ but $\zeta^d \neq 1$ for any $0 < d < n$.
- The cyclotomic polynomial Φ_n is

$$\Phi_n(X) = \prod_{\substack{1 \leq m \leq n \\ (m,n)=1}} (X - \zeta_m).$$

  Degree $\varphi(n)$ and irreducible over $\mathbb{Q}$.
- Fix $\zeta = p^r$.
  (a) The ring of integers in $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$.
  (b) The element $\pi = 1 - \zeta$ is a prime element of $\mathcal{O}_K$, and $(p) = (\pi)^e$, where $e = \varphi(p^r)$.
  (c) p is the only prime to ramify in $\mathbb{Q}(\zeta)$.

The Artin map

We denote the class of a fractional ideal $\mathfrak{a} \in I_F$ by $[\mathfrak{a}] \in \mathrm{Cl}_F$. Let H_F stand for the Hilbert class field of F, which is to say the maximal unramified abelian extension of F.

Theorem

The Artin map

$$\phi_F \ : \ Cl_F \longrightarrow \mathrm{Gal}(H_F/F)$$

defined by $\phi_F([\mathfrak{p}]) = \varphi_{\mathfrak{p}}$ *for all primes* $\mathfrak{p}$ *of* F*, is an isomorphism.*