

Shimura Varieties: Problem sheet 3

Local fields

22 October 2014

Notation: if K is a field complete with respect to a valuation v , we write

$$\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\},$$

$$\mathfrak{m}_K = \{x \in K \mid v(x) > 0\},$$

$$k_K = \mathcal{O}_K / \mathfrak{m}_K.$$

1. Hensel's lemma and squares

- (a) Prove Hensel's lemma: Let K be a complete discretely valued field and $f(X)$ a polynomial with coefficients in \mathcal{O}_K . If $\bar{a} \in k_K$ is a simple root of f modulo \mathfrak{m}_K , then there is a unique $a \in \mathcal{O}_K$ such that $f(a) = 0$ and $\bar{a} \equiv a \pmod{\mathfrak{m}_K}$.
- (b) Prove the strong form of Hensel's lemma: Let K be a complete discretely valued field and $f(X)$ a monic polynomial with coefficients in \mathcal{O}_K . Suppose that f factors as $\bar{g}\bar{h}$ modulo \mathfrak{m}_K , where \bar{g} and \bar{h} are monic and relatively prime in $k_K[X]$. Then there are unique monic polynomials $g, h \in \mathcal{O}_K[X]$ such that $f = gh$, $\bar{g} = g \pmod{\mathfrak{m}_K}$ and $\bar{h} = h \pmod{\mathfrak{m}_K}$.
- (c) Prove that if p is an odd prime, then $x \in \mathbb{Q}_p^\times$ has a square root in \mathbb{Q}_p^\times if and only if $x = p^{2m}a$ for some $m \in \mathbb{Z}$ and $a \in \mathbb{Z}_p^\times$ such that a reduces to a quadratic residue modulo p .
- (d) Prove that if p is odd, then \mathbb{Q}_p has exactly three quadratic extensions: $\mathbb{Q}_p(\sqrt{u})$, $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{pu})$, where u is any non-square in \mathbb{Z}_p^\times .
- (e) Let K be a local field and let q be the cardinality of the residue field. Prove that the set $\mu_{q-1}(K)$ of $(q-1)$ -th roots of unity in K has cardinality $q-1$, and that there is exactly one $(q-1)$ -th root of unity in each non-zero residue class modulo \mathfrak{m}_K .

Deduce that the multiplicative group K^\times splits as a direct product $(1 + \mathfrak{m}_K) \times \mu_{q-1}(K) \times \pi^{\mathbb{Z}}$ where π is a uniformiser.

2. p -adic exponential and logarithm

Consider the power series

$$\exp(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots,$$

$$\log(1 + X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \cdots.$$

- (a) Show that in a field with an ultrametric absolute value, the series $\sum_{n=0}^{\infty} a_n$ converges if and only if $a_n \rightarrow 0$.
(An absolute value is **ultrametric** if it satisfies $|x + y| \leq \max(|x|, |y|)$.)
- (b) Show that $\log(1 + x)$ converges p -adically for all $x \in p\mathbb{Z}_p$.
We can thus define a function $\log: 1 + p\mathbb{Z}_p \rightarrow \mathbb{Z}_p$.
- (c) Show that $\exp(x)$ converges p -adically for all $x \in p\mathbb{Z}_p$ if p is odd, and for all $x \in 4\mathbb{Z}_2$ if $p = 2$.
- (d) Observe that \log is a group homomorphism $(1 + p\mathbb{Z}_p, \times) \rightarrow (p\mathbb{Z}_p, +)$ and \exp is a group homomorphism $(p^r\mathbb{Z}_p, +) \rightarrow (1 + p^r\mathbb{Z}_p, \times)$ where $r = 2$ if $p = 2$ and $r = 1$ otherwise. Furthermore $\log \circ \exp = \text{id}$ and $\exp \circ \log = \text{id}$ wherever these are defined. These all hold because the relevant identities hold in the ring $\mathbb{Q}[[X]]$ of formal power series with rational coefficients.
Deduce that \log and \exp form a mutually inverse pair of group isomorphisms between $(1 + p^r\mathbb{Z}_p, \times)$ and $(p^r\mathbb{Z}_p, +)$.

3. Weak and strong approximation theorems

Let K be any field.

- (a) Show that if $|\cdot|_1$ and $|\cdot|_2$ are inequivalent absolute values on K , then there exists $x \in K$ such that $|x|_1 > 1$ and $|x|_2 < 1$.
- (b) Show by induction on n that if $|\cdot|_1, \dots, |\cdot|_n$ are inequivalent absolute values on K , then there exists $x \in K$ such that $|x|_1 > 1$ and $|x|_i < 1$ for $2 \leq i \leq n$.
- (c) Prove the weak approximation theorem: if $|\cdot|_1, \dots, |\cdot|_n$ are inequivalent absolute values on K , ϵ is a positive real number and x_1, \dots, x_n are elements of the associated completions K_1, \dots, K_n , then there exists $x \in K$ such that $|x - x_i|_i < \epsilon$ for all i ($1 \leq i \leq n$).
- (d) Now suppose that K is a number field. Prove the strong approximation theorem: if $|\cdot|_0, |\cdot|_1, \dots, |\cdot|_n$ are inequivalent values on K , ϵ is a positive real number and x_1, \dots, x_n are elements of the associated completions K_1, \dots, K_n , then there exists $x \in K$ such that

$$|x - x_i|_i < \epsilon \text{ for } 1 \leq i \leq n$$

and

$$|x| \leq 1 \text{ for every absolute value on } K \text{ not equivalent to any } |\cdot|_i, 0 \leq i \leq n.$$

(We have imposed a condition on x for every equivalence class of absolute values except $|\cdot|_0$.)

When $K = \mathbb{Q}$ and $|\cdot|_0$ is the archimedean absolute value, this reduces to the Chinese remainder theorem.

4. Unramified extensions of local fields

Let K be a complete field with valuation $v: K^\times \rightarrow \mathbb{Z}$, and L/K a finite extension of degree n . Then there is a unique valuation $w: L^\times \rightarrow \frac{1}{n}\mathbb{Z}$ extending v . L is complete with respect to w and

$$\mathcal{O}_L = \{x \in L \mid x \text{ is an algebraic integer relative to } \mathcal{O}_K\}.$$

We say that L/K is **unramified** if the extension of residue fields k_L/k_K is separable and $\mathfrak{m}_L = \mathfrak{m}_K \mathcal{O}_L$.

The terminology makes sense geometrically: if $f: X \rightarrow Y$ is a non-constant morphism of algebraic curves, then it induces a finite extension of the function fields $f^*: \mathbb{C}(Y) \hookrightarrow \mathbb{C}(X)$. For each point x in X , we get a finite extension of the completions

$$\widehat{\mathbb{C}(Y)}_{f(x)} \hookrightarrow \widehat{\mathbb{C}(X)}_x.$$

This extension of completions is unramified if and only if f is unramified at x in the sense of complex analysis.

An example of a ramified extension is $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\sqrt{p})$ because $\sqrt{p} \in \mathfrak{m}_L$ but $\sqrt{p} \notin \mathfrak{m}_K \mathcal{O}_L = p\mathcal{O}_L$.

- (a) Show that L/K is unramified if and only if k_L/k_K is separable and the images of the valuations v and w are the same.
- (b) Show that for any finite extension L/K of complete valued fields, $[k_L : k_K] \leq [L : K]$. Show that L/K is unramified if and only if k_L/k_K is separable and $[k_L : k_K] = [L : K]$.
- (c) Suppose that K is a local field, and let $q = \#k_K$. Use 1(d) to show that if L/K is unramified, then L contains a complete set of $(q^n - 1)$ -th roots of unity.
- (d) Let ζ_{q^n-1} be a primitive $(q^n - 1)$ -th root of unity, and consider the field $K(\zeta_{q^n-1})$. This is the splitting field of $X^{q^n-1} - 1$ over K . Observe that $X^{q^n-1} - 1$ has no repeated roots in the residue field of $K(\zeta_{q^n-1})$, and use Hensel's lemma to deduce that the $(q^n - 1)$ -th roots of unity in $K(\zeta_{q^n-1})$ are in distinct residue classes.
Deduce that the residue field of $K(\zeta_{q^n-1})$ is the finite field of order q^n , and that $[K(\zeta_{q^n-1}) : K] \geq n$.
- (e) Let f be the minimal polynomial of ζ_{q^n-1} over K . Use the strong form of Hensel's lemma to show that the reduction of f modulo \mathfrak{m}_K is irreducible in $k_K[X]$.
Deduce that $[K(\zeta_{q^n-1}) : K] = n$.
- (f) Conclude that for each n , there is a unique (up to isomorphism) unramified extension of K of degree n , namely $K(\zeta_{q^n-1})$.