EXERCICES "ALGEBRAIC CURVES AND AUTOMORPHIC FORMS"

Some definitions

Let K be a field endowed with a discrete valuation $v_K : K \to \mathbb{Z}$ (with the convention $v_K(0) = \infty$). We assume that K is complete with respect to the topology induced by the norm

$$|\cdot|_K : K \longrightarrow \mathbb{R}, \quad |\alpha|_K = e^{-v_K(\alpha)}.$$

Such K is called a *local field*.

Let

$$O_K = \{\alpha \in K : v_K(\alpha) \geq 0\} = \{\alpha \in K : |\alpha|_K \leq 1\},$$

$$m_K = \{\alpha \in K : v_K(\alpha) > 0\} = \{\alpha \in K : |\alpha|_K < 1\}.$$

Then, O_K is a discrete valuation ring with residue field $k := O_K/m_K$. This is a finite field.

Let L/K be a finite extension of degree n.

Fact: There is a unique extension of the norm $|\cdot|_K$ to a norm

$$|\cdot|_L : L \to \mathbb{R}.$$

This extension is given by

$$|\alpha|_L = |N_{L/K}(\alpha)|_K^{1/n}, \quad \alpha \in L. \tag{0.1}$$

This fact is not obvious, but we will assume it as a black box (for a proof, see [Neu99], (4.8) Theorem, p.131). The field L, endowed with this extension, is also a local field.

We define O_L, m_L as before and set $\ell := O_L/m_L$. Since O_L is a DVR, we have that there exists $e \in \mathbb{N}$ with $m_K O_L = m_L^e$. The integer e is called the ramification index of the extension L/K. We say that L/K is unramified if the extension is separable and $e = 1$. Otherwise, we say that L/K is ramified.

The exercices

(1) Let $p \geq 3$ be a prime number.
   a) Show that $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$ is a ramified extension.
   b) Let $D \in \mathbb{Z}$. Show that $\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p$ is unramified whenever p does not divide D

(2) Assume L/K is a unramifed and galois. Show that

$$Gal(L/K) \simeq Gal(l/k).$$

(3) Let $\hat{\mathbb{Z}} := \prod_{p \text{ prime}} \mathbb{Z}_p$. Show that for all prime numbers p we have that $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$.

The solutions are on the back. Look only after careful thought

The solutions

(1) Let $p \geq 3$ be a prime number.

a) Show that $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$ is a ramified extension.

Solution: set $L = \mathbb{Q}_p(\sqrt{p})$ and $K = \mathbb{Q}_p$. Let $f(x) = x^2 - p$ ant let $\pi \in L$ be a root of f.

We remark that $f(x)$ is irreducible over $\mathbb{Q}_p$. Indeed, if f were not irreducible, then $\pi \in \mathbb{Q}_p$. But then $2v_p(\pi) = v_p(\pi^2) = v_p(p) = 1$, whence $v_p(\pi) = 1/2$. However, this is not possible, as v_p takes values in $\mathbb{Z}$ (alternatively, one can use Eisenstein's criterion).

Since $f(x)$ is irreducible, we have that $[L : K] = 2$ and $N_{L/K}(\pi) = \pm p$. Hence, $|\pi|_L = |p|_p^{1/2} < 1$. In particular, π belongs to m_L.

Let's check that $\pi \notin m_K O_L$. Assume for contradiction that π belongs to $m_K O_L$. Since $m_K = p\mathbb{Z}_p$, this means that $\pi = p\alpha$, with $\alpha \in m_L$. But then the calculation in the previous paragraph shows that $|\alpha|_L = |p|_p^{-1/2} > 1$. Hence $\alpha \notin m_L$, a contradiction.

We deduce that $pO_L \neq m_L$, hence the extension is ramified.

Comment: a bit more calculation shows that the ramification index is 2.

b) Let $D \in \mathbb{Z}$. Show that $\mathbb{Q}_p(\sqrt{D})/\mathbb{Q}_p$ is unramified whenever p does not divide D

Solution: set $L = \mathbb{Q}_p(\sqrt{p})$ and $K = \mathbb{Q}_p$. We may assume D is squarefree. We may also assume that the polynomial $g(x) = x^2 - D$ is irreducible over $\mathbb{Q}_p$ (for otherwise $L = K$ and there is nothing to prove). In particular, $[L : K] = 2$ and L/K is Galois.

First we remark that the Galois group acts on L by isometries. Indeed, if $\sigma \in Gal(L/K)$, then $|\sigma(\cdot)|_L$ is a norm on L extending $|\cdot|_K$. Hence $|\sigma(\cdot)|_L = |\cdot|_L$ because of the **Fact** stated at the beginning.

We need to show that $m_L \subseteq m_K = p\mathbb{Z}_p$. Let $\pi \in L$ be a root of $g(x)$. Since p does not divide D, we have that $|\pi|_L = |D|_p^{1/2} = 1$. Hence, π is a unit in O_L.

Let $\alpha \in m_L$. Since $N_{L/K}(\alpha) = \pm \prod_{\sigma \in Gal(L/K)} \sigma(\alpha)$ and the trace $T_{L/K}(\alpha) = \pm \sum_{\sigma \in Gal(L/K)} \sigma(\alpha)$ are polynomials on the conjugates of α, and the Galois group acts by isometries, we have that $|N_{L/K}(\alpha)|_L < 1$ and $|T_{L/K}(\alpha)|_L < 1$.

There exists $a, b \in \mathbb{Q}_p$ such that $\alpha = a + b\pi$. Since $T_{L/K}(\alpha) = 2a$ and $p \neq 2$, we deduce that $|a|_p = |2a|_p < 1$. In other words, $a \in p\mathbb{Z}_p$.

On the other hand, $N_{L/K}(\alpha) = a^2 - \pi b^2$. Since $|\pi b^2|_L = |b^2|_L$ and the norm $|\cdot|_L$ is non archimedean, we deduce that $|b|_p < 1$ (for otherwise $|N_{L/K}(\alpha)|_p = |b|^2 \geq 1$, contradicting the previous observation). Hence, $b \in p\mathbb{Z}_p$. We deduce that $\alpha \in pO_L$, as desired.

(2) Assume L/K is a unramifed and galois. Show that

$$Gal(L/K) \simeq Gal(l/k).$$

Solution: first we show that both groups have the same cardinality. Let $n = [L : K]$. Then, we need to show that $n = [\ell : k]$.

Let $m = [\ell : k]$. Let $\alpha_1, \alpha_2, \dots, \alpha_m \in O_L$ be such that their images in ℓ form a k-basis. We claim that these elements are linearly independent. Indeed, if $\sum_i a_i \alpha_i = 0$ with $a_i \in K$, we can divide this relation by an element a_i with the biggest norm and after reordering obtain a relation of the form

$$\sum_i b_i \alpha_i = 0, \quad b_i \in O_L, \quad |b_1|_L = 1.$$

Taking the image in this relation in ℓ, we obtain a nonzero linear combination of a basis of ℓ/k, a contradiction. This proves our claim.

We deduce that $m \leq n$. In order to show the other opposite inequality, we remark that any element $\alpha \in O_L$ is of the form

$$\alpha = \beta + \sum_i a_i \alpha_i, \quad \beta \in m_L, \quad a_i \in O_K.$$

Indeed, the image of α in ℓ is a k-linear combination of the images of the α_i and when we lift this relation to O_L we obtain such an expression.

Let M be the O_K-module inside O_L spanned by the α_i. The previous remark and the fact that the extension is unramified show that

$$O_L = M + m_K O_L.$$

Since O_K is a DVR, by Nakayama's lemma[1], we conclude that $O_L = M$.

Since L is the fraction field of O_L, we conclude that $n = [L : K] \leq m$, as desired.

Now let $\sigma \in Gal(L/K)$. Since $N_{L/K}(\cdot)$ is invariant under the Galois group, equation (0.1) shows that σ acts as an isometry on L. In particular, we have that $\sigma(O_L) = O_L$ and $\sigma(m_L) = m_L$. Then, there is an induced k-automorphism $\tilde{\sigma} : \ell \to \ell$. Let

$$\phi : Gal(L/K) \to Gal(\ell/k), \quad \phi(\sigma) = \tilde{\sigma}$$

be the map thus constructed. It is clearly an homomorphism between groups of the same cardinality. In order to finish, it is then enough to check that ϕ is injective.

Since ℓ/k is a separable extension (these are finite fields), there exists $a \in \ell$ such that $\ell = k(a)$. In particular, $\{1, a, a^2, \ldots, a^{n-1}\}$ is a k-basis of ℓ. Choose $\alpha \in O_L$ with image in ℓ equal to a. The previous reasoning involving Nakayama's lemma implies that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a O_K-basis of O_L. In particular, O_L is an O_K-module of finite type and α is a root of a monic degree n irreducible polynomial $h(x) \in O_K[x]$. Moreover, the image of $h(x)$ in $k[x]$ is the minimal polynomial of a. Hence, any $\sigma \in Gal(L/K)$ is determined by the element $\sigma(\alpha)$. If $\phi(\sigma) = id_\ell$, then $\tilde{\sigma}(a) = a$, implying $\sigma(\alpha) = \alpha$ (otherwise there would be two different roots of $h(x)$ mapping to a and $h(x)$ would become reducible in $k[x]$). Hence, σ is trivial. This shows that ϕ is injective, as desired.

Comment: by taking the element in $Gal(L/K)$ corresponding to the frobenius of ℓ/k throught this specific isomorphism, this is how a "frobenius" element was defined in $Gal(L/K)$ during Vincent's first lecture.

(3) Let $\hat{\mathbb{Z}} := \prod_{p \text{ prime}} \mathbb{Z}_p$. Show that for all prime numbers p we have that $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$.

Solution: For any n, we have that $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$. We fix the isomorphism by taking the frobenius automorphism to 1. With this convention, we deduce that $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \lim_n \mathbb{Z}/n\mathbb{Z}$.

On the other hand, for any prime q, we have that $\mathbb{Z}_q \simeq \lim_m \mathbb{Z}/q^m\mathbb{Z}$. Using the chinese reminder theorem, we deduce that $\hat{\mathbb{Z}} \simeq \lim_n \mathbb{Z}/n\mathbb{Z}$, as desired.

References

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. (document), 1

Facultad de Matemáticas, PUC, Vicuña Mackenna 4860, Santiago, Chile
E-mail address: rmenares@mat.uc.cl

[1] for the particular form of Nakayama's lemma needed here, see [Neu99], Chapter I, section 11, Exercice 7