D-MATH
Prof. Richard Pink

Number Theory II

FS 2024

Solutions 23

Ramification Filtration

1. Let L/K be a finite Galois extension of nonarchimedean local fields with Galois group Γ.

   (a) Compute $\eta_{L/K}(s)$ for all $s \geqslant -1$ with $\Gamma_1 \subset \Gamma_s$.

   (b) Compute the upper numbering filtration of Γ when L/K is tame.

   (c) Compute the upper numbering filtration of Γ when $[L/K]$ is prime.

   Solution

   (a) For all $-1 < x < 0$ we have $\Gamma_x = \Gamma_0$. Thus for all $-1 \leqslant s \leqslant 0$ we have

   $$\eta_{L/K}(s) \;=\; \int_0^s \frac{dx}{[\Gamma_0 : \Gamma_0]} \;=\; s.$$

   Next take $s > 0$ with $\Gamma_1 \subset \Gamma_s$. Then for all $0 < x < s$ we have $\Gamma_x = \Gamma_1$ and hence

   $$\eta_{L/K}(s) \;=\; \int_0^s \frac{dx}{[\Gamma_0 : \Gamma_1]} \;=\; \frac{s}{[\Gamma_0 : \Gamma_1]}.$$

   (b) The extension L/K is tame if and only if $\Gamma_s = 1$ for all $s > 0$. From (a) and the definition of the upper numbering we deduce that $\Gamma^t = \Gamma_t$ for all $t \geqslant -1$.

   (c) If Γ has prime order, there exists a unique integer $r \geqslant -1$ such that $\Gamma_x = \Gamma$ for all $x \leqslant r$ and $\Gamma_x = 1$ for all $x > r$. For any $s \leqslant r$ we deduce that

   $$\eta_{L/K}(s) \;=\; \int_0^s \frac{dx}{[\Gamma_0 : \Gamma]} \;=\; s.$$

   As $\eta_{L/K}$ is strictly monotone increasing, we deduce that $\eta_{L/K}(s) > \eta_{L/K}(r) = r$ for all $s > r$. Using the definition of the upper numbering we conclude that $\Gamma^t = \Gamma_t$ for all $t \geqslant -1$.

2. Determine the lower and upper numbering filtrations on $\mathrm{Gal}(K/\mathbb{Q}_2)$ for the following fields K:

   (a) The splitting field of the polynomial $x^2 - 2$.

   (b) The splitting field of the polynomial $x^4 - 2$.

Solution

(a) By the Eisenstein criterion the polynomial is irreducible. Its roots in $\bar{\mathbb{Q}}_2$ are $\pi := \sqrt{2}$ and $-\sqrt{2}$. The computation $\pi^2 = 2$ shows that $K/\mathbb{Q}_2$ has ramification degree 2 and that $v(\pi) = 1$ for the normalized valuation v on K. In particular this implies that $\mathcal{O}_K = \mathbb{Z}_2[\pi]$. Letting γ denote the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q}_2)$, we deduce that

$$v({}^\gamma\pi - \pi) \;=\; v\big((-\sqrt{2}) - (\sqrt{2})\big) \;=\; v(-2\sqrt{2}) \;=\; 3.$$

Using the definition of the lower numbering filtration and Lemma 11.5.3 we deduce that $\gamma \in \Gamma_s$ if and only if $s \leqslant 2$. Thus $\Gamma_s = \Gamma$ for all $s \leqslant 2$ and $\Gamma_s = 1$ for all $s > 2$. By part (c) of the preceding exercise we deduce that $\Gamma^t = \Gamma$ for all $t \leqslant 1$ and $\Gamma^t = 1$ for all $t > 2$.

(b) The polynomial $x^4 - 2$ is irreducible by the Eisenstein criterion, and one of the roots is $\alpha := \sqrt[4]{2}$ and a uniformizer of the intermediate field $\mathbb{Q}_2(\alpha)$. The other roots are $-\alpha$ and $\pm i\alpha$ for $i = \sqrt{-1}$, so we first want to find out whether i is contained in $\mathbb{Q}_2(\alpha)$.

Here i is a root of the polynomial X^2+1. This factors as $(X-1)^2$ modulo (2); hence we substitute $X = Y + 1$, yielding the polynomial $Y^2 + 2Y + 2$. Here we can substitute $Y = \alpha^2 Z$ and obtain the polynomial $Z^2 + \alpha^2 Z + 1$. This polynomial factors as $(Z-1)^2$ modulo (α); hence we substitute $Z = U+1$ and obtain the polynomial $U^2 + (\alpha^2 + 2)U + (\alpha^2 + 2)$. The substitution $U = \alpha V$ now yields $V^2 + (\alpha + \alpha^3)V + (1 + \alpha^2)$. Yet again this polynomial becomes a square modulo (α), so we substitute one more time $V = W + 1$ and obtain

$$(*) \qquad W^2 + (\alpha + \alpha^3 + 2)W + (\alpha + \alpha^2 + \alpha^3 + 2).$$

This is an Eisenstein polynomial with respect to the maximal ideal (α) of $\mathbb{Z}_2[\alpha]$. Thus the splitting field $K := \mathbb{Q}_2(\alpha, i)$ is ramified of degree 2 over $\mathbb{Q}_2(\alpha)$ and any root of the polynomial $(*)$ is a uniformizer. Substituting back we find that one root is

$$\beta \;:=\; \frac{i - 1 - \alpha^2 - \alpha^3}{\alpha^3},$$

so we have $\mathcal{O}_K = \mathbb{Z}_2[\beta]$.

The Galois group $\Gamma := \mathrm{Gal}(K/\mathbb{Q}_2)$ must act by $\alpha \mapsto \pm\alpha, \pm i\alpha$ and $i \mapsto \pm i$, and since $[K/\mathbb{Q}_2] = 8$, all combinations of these substitutions are possible. In particular we have $\Gamma \cong D_4$. Direct computation shows the effect on β of the following elements $\sigma_\nu \in \Gamma$:

σ	${}^\sigma\alpha$	${}^\sigma i$	${}^\sigma\beta$	${}^\sigma\beta - \beta$	$\mathrm{ord}_\beta({}^\sigma\beta - \beta)$
σ_1	$-\alpha$	i	$-\beta - 2$	$-2\beta - 2$	8
σ_2	$i\alpha$	i	$-\beta + \alpha^2 + \alpha^2\beta - 2$	$-2\beta + \alpha^2 + \alpha^2\beta - 2$	4
σ_3	α	$-i$	$\beta - \alpha i$	$-\alpha i$	2

Thus for the lower numbering filtration we have $\sigma_1 \in \Gamma_7 \smallsetminus \Gamma_8$ and $\sigma_2 \in \Gamma_3 \smallsetminus \Gamma_4$ and $\sigma_3 \in \Gamma_1 \smallsetminus \Gamma_2$. Since $\sigma_1 = \sigma_2^2$ we deduce that

$$\Gamma_s \;=\; \begin{cases} 1 & \text{if } \; s > 7, \\ \langle\sigma_1\rangle & \text{if } \; 3 < s \leqslant 7, \\ \langle\sigma_2\rangle & \text{if } \; 1 < s \leqslant 3, \\ \Gamma & \text{if } \; s \leqslant 1. \end{cases}$$

Using the definition of $\eta_{K/\mathbb{Q}_2}$ elementary computations yield $\eta_{K/\mathbb{Q}_2}(1) = 1$ and $\eta_{K/\mathbb{Q}_2}(3) = 2$ and $\eta_{K/\mathbb{Q}_2}(7) = 3$, hence for the upper numbering filtration we get

$$\Gamma^t \;=\; \begin{cases} 1 & \text{if } \; t > 3, \\ \langle\sigma_1\rangle & \text{if } \; 2 < t \leqslant 3, \\ \langle\sigma_2\rangle & \text{if } \; 1 < t \leqslant 2, \\ \Gamma & \text{if } \; t \leqslant 1. \end{cases}$$

3. Determine the lower and upper numbering filtrations on the local galois group

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p) \;\cong\; (\mathbb{Z}/p^m\mathbb{Z})^\times.$$

Solution Fix a primitive p^m-th root of unity ζ. From Theorems 3.6.6 and 3.6.7 we know that $\mathbb{Q}(\mu_{p^m})/\mathbb{Q}$ has Galois group isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^\times$ and is totally ramified at p, that the ideal $(1-\zeta)$ is the unique prime ideal above (p), and that the ring of integers in $\mathbb{Q}(\mu_{p^m})$ is $\mathbb{Z}[\zeta]$. Setting $K := \mathbb{Q}_p(\mu_{p^m})$, it follows that $\Gamma := \mathrm{Gal}(K/\mathbb{Q}_p)$ is also isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^\times$ and that $\mathcal{O}_K = \mathbb{Z}_p[\zeta]$ with the maximal ideal $(1-\zeta)$. Let v denote the normalized valuation on K.

Consider a non-trivial element $\gamma \in \Gamma$ that corresponds to $[1] \neq [a] \in (\mathbb{Z}/p^m\mathbb{Z})^\times$. Then $r := \mathrm{ord}_p(a-1) < m$, and

$$v({}^\gamma\zeta - \zeta) \;=\; v(\zeta^a - \zeta) \;=\; v(1-\zeta^{a-1}),$$

where ζ^{a-1} is a primitive p^{m-r}-th root of unity. Working within $\mathbb{Q}_p(\mu_{p^{m-r}})$ in place of $\mathbb{Q}_p(\mu_{p^m})$ we know that $(1-\zeta^{a-1})^{p^{m-r-1}(p-1)}/p$ is a unit. Since v is the normalized valuation on K, we deduce that

$$v(1-\zeta^{a-1}) \;=\; \frac{v(p)}{p^{m-r-1}(p-1)} \;=\; \frac{p^{m-1}(p-1)}{p^{m-r-1}(p-1)} \;=\; p^r.$$

With Lemma 11.5.3 we conclude that $\gamma \in \Gamma_s$ if and only if $p^r = v({}^\gamma\zeta - \zeta) \geqslant s+1$.

In particular we have $\Gamma_s = \Gamma$ for all $-1 \leqslant s \leqslant 0$. For any real number $s > 0$ consider the unique integer $k \geqslant 1$ such that $p^{k-1} < s+1 \leqslant p^k$. If $k \leqslant m$, then the above condition shows that $\gamma \in \Gamma_s$ if and only if $r \geqslant k$, and so Γ_s corresponds to the subgroup of all $[a] \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ with $a \equiv 1 \bmod (p^k)$. In particular $\Gamma_s = 1$ when $k = m$, and hence also whenever $s+1 > p^{m-1}$.

The above computation also shows that for any integer $1 \leqslant k \leqslant m$ we have $[\Gamma_0 : \Gamma_x] = [\Gamma : \Gamma_x] = p^{k-1}(p-1)$ for all real numbers $p^{k-1} - 1 < x \leqslant p^k - 1$. Therefore

$$\int_{p^{k-1}-1}^{p^k-1} \frac{dx}{[\Gamma_0 : \Gamma_x]} \;=\; \frac{p^k - p^{k-1}}{p^{k-1}(p-1)} \;=\; 1.$$

For any $p^{k-1} - 1 < s \leqslant p^k - 1$ this implies that

$$\eta_{L/K} \;=\; \int_0^s \frac{dx}{[\Gamma_0 : \Gamma_x]} \;=\; k - 1 + \frac{s + 1 - p^{k-1}}{p^{k-1}(p-1)}$$

and hence $k-1 < \eta_{L/K}(s) \leqslant k$. Since $\Gamma^{\eta_{L/K}(s)} = \Gamma_2$ this implies that Γ^t corresponds to $\big\{[a] \in (\mathbb{Z}/p^m\mathbb{Z})^\times \;\big|\; a \equiv 1 \bmod (p^k)\big\}$ for all $k - 1 < t \leqslant k$. In other words Γ^t corresponds to $\big\{[a] \in (\mathbb{Z}/p^m\mathbb{Z})^\times \;\big|\; a \equiv 1 \bmod (p^{\lceil t \rceil})\big\}$ for all $t > 0$, and $\Gamma^t = \Gamma$ for all $-1 \leqslant t \leqslant 0$.

4. Let G be a finite group of order n, and let R be a unitary commutative ring such that n is invertible in R. Show that for any $R[G]$-module M the natural map $M^G \to M_G$ is an isomorphism.

   Solution The natural map $p\colon M^G \to M_G := M/\sum_{g\in G}(g-1)M$ is defined by $p(m) = [m]$ and R-linear. To construct a map in the other direction set $tm := \frac{1}{n}\sum_{g\in G} gm$ for any $m \in M$. Direct computation shows that $tm \in M^G$ and that $t(g-1)n = 0$ for all $g \in G$ and $n \in M$. In particular tm depends only on the residue class $[m] \in M_G$, and $s([m]) := tm$ defines a map $s\colon M_G \to M^G$. For any $m \in M^G$ we have $tm = m$; hence $s \circ p = \mathrm{id}$. Conversely, for any $m \in M$ and $g \in G$ we have $[gm] = [m]$, from which we deduce that $[m] = [tm]$. Thus we also have $p \circ s = \mathrm{id}$; hence s is a two-sided inverse of p, which is therefore an isomorphism.