24. November 2014

Exercise 7 for Number theory III[1]

Kay Rülling

Exercise 7.1. Let K be a local field ($\neq \mathbb{R}, \mathbb{C}$). Show that there is a unique unramified $\mathbb{Z}_p$-extension of K, i.e. an unramified Galois extension L/K with Galois group $G(L/K) \cong \mathbb{Z}_p$.

Exercise 7.2 (The Legendre Symbol)**.** Let p be an odd prime number and denote by $v_p : \mathbb{Q}^\times \to \mathbb{Z}$ the p-adic valuation. For a rational number $a \in \mathbb{Q}$ with $v_p(a) = 0$ define the *Legendre symbol* $\left(\frac{a}{p}\right) \in \{\pm 1\}$ by

$$\left(\frac{a}{p}\right) = 1 \Longleftrightarrow a \text{ is a square mod } p.$$

(1) We view $\{\pm 1\}$ as subgroup of $\mathbb{F}_p^\times$. Show that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$.
(2) Show $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (*Hint:* For the second formula first observe that $\frac{p^2-1}{8} \equiv 1 \bmod 2$ iff $p \equiv \pm 1 \bmod 8$. Then show that if $\alpha \in \bar{\mathbb{F}}_p$ is an 8-th root of 1 and $y := \alpha + \alpha^{-1}$, then $\left(\frac{2}{p}\right) = y^{p-1}$ and conclude.)
(3) Show $\sum_{a \in (\mathbb{Z}/\ell)^\times} \left(\frac{a}{\ell}\right) = 0$.
(4) Show that the extension $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ is unramified of degree ≤ 2.
(5) Show that if we view $G(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p)$ as a subgroup of $\{\pm 1\}$, then

$$\rho_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p}(p) = \left(\frac{a}{p}\right),$$

where

$$\rho_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p} : \mathbb{Q}_p^\times/\mathrm{Nm}(\mathbb{Q}_p(\sqrt{a})^\times) \to G(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p)$$

is the local Artin map.

[1]This exercise sheet will be discussed on December 5. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `kindler@math.fu-berlin.de` or `l.zhang@fu-berlin.de`

Exercise 7.3 (Gauß Reciprocity Law)**.** The aim of this exercise is to show the Gauß Reciprocity law: Let p, ℓ be two distinct odd prime numbers, then

$$(*) \qquad \left(\frac{\ell}{p}\right) \cdot \left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}.$$

To this end proceed as follows: Set $\ell^* := (-1)^{\frac{\ell-1}{2}}\ell$.

(1) Show that $(*)$ is equivalent to $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$.

(2) Show

$$\mathrm{Nm}(\mathbb{Q}_p(\sqrt{\ell^*})^\times) = \begin{cases} \mathbb{Q}_p^\times, & \text{if } \mathbb{Q}_p(\sqrt{\ell^*}) = \mathbb{Q}_p, \\ < p^2 > \times \mathbb{Z}_p^\times, & \text{else,} \end{cases}$$

where $< p^2 >$ denotes the infinite cyclic group multiplicatively generated by p^2.

(3) Conclude that $\left(\frac{\ell^*}{p}\right) = 1 \Leftrightarrow \mathbb{Q}_p(\sqrt{\ell^*}) = \mathbb{Q}_p$.

(4) Let $\zeta \in \bar{\mathbb{Q}}$ be an ℓ-th root of 1. Show that $\mathbb{Q}(\sqrt{\ell^*}) \subset \mathbb{Q}(\zeta)$. (*Hint*: Set $\tau := \sum_{n \in (\mathbb{Z}/\ell)^\times} \left(\frac{n}{\ell}\right)\zeta^n$ and use Excercise, 7.2, 3 to show $\left(\frac{-1}{\ell}\right) \cdot \tau^2 = \ell$.)

(5) Conclude from 4 that: $\mathbb{Q}_p(\sqrt{\ell^*}) = \mathbb{Q}_p \Leftrightarrow \frac{\ell-1}{2} | [\mathbb{Q}_p(\zeta) : \mathbb{Q}_p]$.

(6) Show that $\mathbb{Q}_p(\zeta)$ is unramified over $\mathbb{Q}_p$ of degree f, where f is the minimal positive integer with $p^f \equiv 1 \bmod \ell$.

(7) Conclude from 5 and 6 that: $\mathbb{Q}_p(\sqrt{\ell^*}) = \mathbb{Q}_p \Leftrightarrow \left(\frac{p}{\ell}\right) = 1$. Put all together to conclude $(*)$.

Exercise 7.4. Is 105 a square modulo 257?