ZAHLENTHEORIE II – ÜBUNGSBLATT 10

PROF. DR. HÉLÈNE ESNAULT AND DR. LEI ZHANG

Exercise 1. Let A be a local ring with residue field k. If $f, g \in X$ are such that $\bar{f}$ and $\bar{g}$ are relatively prime and f is monic. Show that

(a) The A-module $M := A[X]/(f, g)$ is finitely generated.
(b) We have $(f, g) = A[X]$.
(c) There exist $u, v \in A[X]$ with $\deg u < \deg g$ and $\deg v < \deg f$ such that $uf + vg = 1$.

Exercise 2. Let A be a local ring with residue field k. Suppose $f = gh = g'h'$ with g, h, g', h' all monic, and $\bar{g} = \bar{g'}, \bar{h} = \bar{h'}$ with $\bar{g}$ and $\bar{h}$ relatively prime. Then $g = g'$ and $h = h'$.

Exercise 3. Let $p \neq 2$ be a prime. Prove that the following are equivalent:

(a) There exists $b \in \mathbb{Q}_p^*$ such that $u = b^2$.
(b) There exists $b \in \mathbb{Z}_p^*$ such that $u = b^2$.
(c) There exists $b \in \mathbb{F}_p^*$ such that if $\bar{u}$ denotes the reduction of u modulo p, then $\bar{u} = b^2$.

Exercise 4. Let A be a complete DVR with fraction field is K and maximal ideal $\mathfrak{m}$. Let L/K be a finite separable field extension. In this case the integral closure $\mathcal{O}_L$ is a local ring and $\mathfrak{m}\mathcal{O}_L$ is a power of the maximal ideal $\mathfrak{m}_L$ of $\mathcal{O}_L$, in other words, with the notation of the ramification $g = 1$. Using this to show that the maximal ideal $\mathfrak{m}$ of A is *unramified* if and only if $\mathfrak{m}\mathcal{O}_L$ is a prime ideal in $\mathcal{O}_L$, and this is also equivalent to saying that $[\mathcal{O}_L/\mathfrak{m}_L : A/\mathfrak{m}]$ is equal to the degree of the extension L/K. If L satisfies one of the equivalent properties, then L is called *unramified.*

Exercise 5. We will show step by step that for each prime number p and each $f \in \mathbb{N}$ there is a unique unramified extension L of $K := \mathbb{Q}_p$ of degree f.

(a) Take a primitive $(p^f - 1)$-th roots of unity α in $\mathbb{F}_{p^f}$. Let $\bar{g}(X) \in \mathbb{F}_p[X]$ be the minimal polynomial of α. Use Hensel's lemma to show that there exists a unique monic polynomial $g(X) \in \mathbb{Z}_p[X]$ lifting $\bar{g}(X)$ such that $g(X)|X^{p^f-1}$.
(b) Take a root β of $g(X)$ and set $L := \mathbb{Q}_p(\beta)$. Show that L is a degree f unramified extension of $\mathbb{Q}_p$, and the reduction $\bar{\beta}$ of β in F_{p^f} is again a $(p^f - 1)$-th roots of unity.
(c) Show that β is a primitive $(p^f - 1)$-th roots of unity in $\overline{\mathbb{Q}_p}$. So L is the splitting field of $X^{p^f-1} - 1 = 0$.
(d) Show that any unramified extension of $\mathbb{Q}_p$ is the splitting field of $X^{p^f-1} - 1 = 0$.

If you want your solutions to be corrected, please hand them in just before the lecture on Juli 10, 2018. If you have any questions concerning these exercises you can contact Dr. Lei Zhang via `l.zhang@fu-berlin.de` or come to Arnimallee 3 112A.