Number theory, midterm exam

24th October 2024, 2pm - 4:30pm

In all the exercises, K is a discrete valuation field, with valuation ring $\mathcal{O}_K$, maximal ideal $\mathfrak{m}_K$ and residue field k. The corresponding absolute value on K is denoted by $|\ |$.

Exercise 1 (Structure of the group of units) Let $U^{(0)} = \mathcal{O}_K^*$ be the multiplicative group of the units of $\mathcal{O}_K$. Denote by $\mathfrak{m}_K$ the maximal ideal of $\mathcal{O}_K$, and for all $n \geq 1$, denote

$$U^{(n)} := 1 + \mathfrak{m}_K^n = \{1 + x \mid x \in \mathfrak{m}_K^n\}$$

1. Show that $U^{(n)}$ is a subgroup of $U^{(0)}$.
2. Show that the quotient map $s : \mathcal{O}_K \to k$ induces an isomorphism of groups
$$U^{(0)}/U^{(1)} \to k^*.$$
3. Fix a uniformizing element π_K of $\mathcal{O}_K$. Show that the map $1 + \mathfrak{m}_K^n \to k$, $1 + x \mapsto s(\pi_K^{-n} x)$, induces an isomorphism of groups
$$U_K^{(n)}/U_K^{(n+1)} \simeq k$$
for all $n \geq 1$.

Exercise 2 Consider $P(X) = X^3 - X + 2 \in \mathbb{Z}[X]$. Its discriminant is $-104 = -2^3.13$.

1. Show that $P(X)$ is irreducible in $\mathbb{Q}[X]$.
2. Let p be a prime number $\neq 2, 13$. Explain why $X^3 - X + 2$ is separable in $\mathbb{F}_p[X]$.
3. Let $L = \mathbb{Q}[\alpha]$ be the extension of $\mathbb{Q}$ generated by a root $\alpha \in \mathbb{C}$ of $P(X)$. Let $p \neq 2, 13$. Show that $L/\mathbb{Q}$ is unramified for the p-adic valuation.
4. Let $\widetilde{\mathcal{O}}_2$ be the integral closure of $\mathbb{Z}_{2\mathbb{Z}}$ in L.
    (a) Show that $N_{L/\mathbb{Q}}(\alpha - 1) = -2$ and that $\alpha - 1$ is not invertible in $\widetilde{\mathcal{O}}_2$.
    (b) Let $\mathfrak{m}$ be a maximal ideal of $\widetilde{\mathcal{O}}_2$ containing $\alpha - 1$. Show that $\mathbb{Z}_{2\mathbb{Z}} \to (\widetilde{\mathcal{O}}_2)_{\mathfrak{m}}$ is ramified.

Exercise 3 Let $p > 2$ be a prime number. Consider $L = \mathbb{Q}_p(\xi_{p^2})$ for some primitive p^2-th of unit $\xi_{p^2} \in \mathbb{C}_p$. Let $K = \mathbb{Q}_p(\xi_p)$ with $\xi_p = \xi_{p^2}^p$. We know that $\lambda_p := \xi_p - 1$ is a uniformizing element of $\mathcal{O}_K$ and that $p \in \lambda_p^{p-1}\mathcal{O}_K^*$.

1. Why is the integral closure of $\mathcal{O}_K$ in L a discrete valuation ring $\mathcal{O}_L$?
2. Show that $[L : K] \leq p$.
3. Let $\lambda_{p^2} = \xi_{p^2} - 1$. Find a relation between λ_{p^2} and λ_p.
4. Show that $\mathcal{O}_K \to \mathcal{O}_L$ has ramification index $\geq p$.

5. Show that $[L : K] = p$ with ramification index p and trivial residue extension.

Exercise 4 (Henselian discrete valuation ring) A discrete valuation ring $\mathcal{O}_K$ is said to be *Henselian* if it satisfies the conclusion of Hensel's lemma, namely: *for any polynomial $P(X) \in \mathcal{O}_K[X]$, if we have a decomposition*

$$\bar{P}(X) = f(X)g(X) \in k[X]$$

with coprime $f(X), g(X)$, then there exist $F(X), G(X) \in \mathcal{O}_K[X]$ such that $P(X) = F(X)G(X)$ with $\bar{F}(X) = f(X)$, $\bar{G}(X) = g(X)$ and $\deg F(X) = \deg f(X)$. For example, if K is complete, then $\mathcal{O}_K$ is Henselian.

1. Let p be a prime number. Show that $\mathbb{Z}_{p\mathbb{Z}}$ is not Henselian by considering a suitable quadratic polynomial in $\mathbb{Z}_{p\mathbb{Z}}[X]$.

2. Show that in the conclusion of Hensel's lemma, the polynomials $F(X), G(X)$ are coprime.

3. Suppose $\mathcal{O}_K$ Henselian. We want to prove that for any finite extension L/K, there is a unique extension of $| \ |$ to L. Equivalently, the integral closure of $\mathcal{O}_K$ in L is a discrete valuation ring.

   (a) Let $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in K[X]$ be a monic irreducible polynomial with $|a_0| > 1$. Show that $|a_0| > |a_i|$ for all $i > 0$ (consider the polynomial $a_{i_0}^{-1}P(X)$ for the smallest i_0 such that $|a_{i_0}| = \max_{0 \leq i \leq d-1} |a_i|$).

   (b) Suppose that $P(\alpha) = 0$ for some $\alpha \in L$. Show that $|\alpha|_L > 1$ for any extension $| \ |_L$ of $| \ |$ to L.

   (c) Let $| \ |_L$ be an extension of $| \ |$ with valuation ring $\mathcal{O}_L$. Show that $\mathcal{O}_L$ is integral over $\mathcal{O}_K$, thus equal to the integral closure of $\mathcal{O}_K$ in L.

4. (Construction of a Henselian discrete valuation ring). Let K_h be the algebraic closure of K in $\widehat{K}$, endowed with the restriction of $| \ |_{\widehat{K}}$.

   (a) Let $P(X) \in K_h[X] \setminus \{0\}$. Suppose that we have a decomposition

   $$P(X) = \widehat{F}(X)\widehat{G}(X), \quad \widehat{F}(X), \widehat{G}(X) \in \widehat{K}[X]$$

   in $\widehat{K}[X]$ with $\widehat{F}(X)$ monic. By considering the roots of $\widehat{F}(X)$ in some algebraic closure of $\widehat{K}$, show that $\widehat{F}(X) \in K_h[X]$ and hence $\widehat{G}(X) \in K_h[X]$.

   (b) Show that $\mathcal{O}_{K_h}$ is Henselian.

5. Suppose $\mathrm{char}(K) = p > 0$. Let L/K be an algebraic purely inseparable extension (for all $x \in L$, $x^{p^r} \in K$ for some $r \geq 0$). Endow L with an extension of $| \ |$ and suppose that $\mathcal{O}_L$ is Henselian. We want to show that $\mathcal{O}_K$ is Henselian.

   (a) Let $P(X) \in K[X] \setminus \{0\}$ and suppose that we have

   $$P(X) = F_L(X)G_L(X), \quad F_L(X), G_L(X) \in L[X]$$

   be a decomposition in $L[X]$ with coprime $F_L(X), G_L(X)$ and $F_L(X)$ monic.

i. Show that for some $r \geq 0$ we have $F_L(X)^{p^r} \in K[X]$, and that $\gcd(P(X), F_L(X)^{p^r}) \in K[X]$ (by convention the gcd is a monic polynomial).

ii. Determine the above gcd and conclude that $F_L(X) \in K[X]$, and hence $G_L(X) \in K[X]$.

(b) Show that $\mathcal{O}_K$ is Henselian (use Question (2) of this exercise).

6. Let K^h be the separable closure of K in $\widehat{K}$. Show that for any field L with $K^h \subseteq L \subseteq K_h$, $\mathcal{O}_L$ is Henselian.