Math 204B, Winter 2019

Number Theory II, Final Exam (take-home)

Due Monday March 18th in APM 6151 (under the door) by 3PM.

Problem A. Let $p \equiv 1 \pmod 3$ be a prime number.

(a) Show that every cubic Galois extension $E/\mathbb{Q}_p$ is of the form $E = \mathbb{Q}_p(\sqrt[3]{\theta})$ for some $\theta \in \mathbb{Q}_p^\times$ (not in $\mathbb{Q}_p^{\times 3}$) – and vice versa.

(b) How many cubic Galois extensions E does $\mathbb{Q}_p$ have (inside a fixed algebraic closure)? Are they all tamely ramified?

Problem B.

(a) Does the additive group $\mathbb{Q}_p$ have a maximal compact subgroup?

(b) Show that $\mathbb{Z}_p^\times$ is the unique maximal compact subgroup of $\mathbb{Q}_p^\times$. Generalize this statement – and your argument – to finite extensions of $\mathbb{Q}_p$.

(c) Let $G \subset \bar{\mathbb{Q}}_p^\times$ be a compact subgroup. Prove that G is contained in the units U_K for some finite extension $K/\mathbb{Q}_p$. (`Hint`: Write G as a countable union of closed subsets $G \cap K^\times$ and use that G is a Baire space.)

Problem C. Let K be a non-archimedean local field with valuation v_K (which extends uniquely to an algebraic closure $\bar{K}$). Let

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$$

be a polynomial with nonzero leading and constant coefficients; $a_0a_n \neq 0$.

(a) Suppose the roots $\alpha_1, \ldots, \alpha_n \in \bar{K}$ of f have distinct (finite) valuations

$$v_K(\alpha_1) > v_K(\alpha_2) > \cdots > v_K(\alpha_n).$$

Check that all $a_i \neq 0$ and join the points $P_i = \big(i, v_K(a_i)\big)$ in the plane by a piecewise linear segment. Show that the **slopes** of this convex segment are precisely $-v_K(\alpha_i)$ for $i = 1, \ldots, n$.

(b) Extend the result from (a) to the general case without assumptions on the $v_K(\alpha_i)$ (allowing distinct roots to have the same valuation).

`Hint`: Consider the "lower convex hull" of the set of points P_i. It might be helpful to do the case $n = 2$ first.

Problem D. A quaternion algebra D over $\mathbb{Q}_p$ admits a basis $\{1, i, j, k\}$ satisfying the relations

$$i^2 = a \qquad j^2 = b \qquad ij = k = -ji$$

for some $a, b \in \mathbb{Q}_p^\times$. (This follows easily from the Skolem-Noether theorem.)

(a) When $a = 1$ show that there is an isomorphism $D \xrightarrow{\sim} M_2(\mathbb{Q}_p)$ given by

$$1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \qquad i \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \qquad j \mapsto \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right) \qquad k \mapsto \left(\begin{smallmatrix} 0 & b \\ -1 & 0 \end{smallmatrix}\right).$$

(b) Show that D contains at least the following three quadratic subfields:

$$\mathbb{Q}_p(\sqrt{a}) \qquad \mathbb{Q}_p(\sqrt{b}) \qquad \mathbb{Q}_p(\sqrt{-ab}).$$

Deduce that $\mathbb{Q}_{p^2} \subset D$ (where $\mathbb{Q}_{p^2}$ is the unramified quadratic extension).

(c) Prove that the following five conditions are equivalent:

(1) D is isomorphic to the matrix algebra $M_2(\mathbb{Q}_p)$.

(2) D is <u>not</u> a division algebra.

(3) There is a nonzero $q \in D$ with norm $N(q) = q\bar{q} = 0$.

(4) The element a lies in the norm group of $\mathbb{Q}_p(\sqrt{b})$.

(5) $(a, b)_2$=1, where $(\cdot, \cdot)_2$ denotes the Hilbert symbol – that is the pairing

$$\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \longrightarrow \{\pm 1\} \qquad (a, b)_2 = \phi_{\mathbb{Q}_p}(a)(\sqrt{b})/\sqrt{b}.$$

(Here $\phi_{\mathbb{Q}_p}$ is the Artin map.)

`Hints`: For (1) $\iff$ (2) just apply Wedderburn's theorem. For the implication (5) $\implies$ (1) suppose $b^{-1} = N(r + s\sqrt{a})$ – then introduce the elements $u = rj + sk$ and $v = (1 + a)i + (1 - a)ui$ and refer to part (a).

(d) Note that your arguments in (c) work for any finite extension of $\mathbb{Q}_p$ and conclude that there is an isomorphism

$$D \otimes_{\mathbb{Q}_p} K \xrightarrow{\sim} M_2(K)$$

where $K \subset D$ is any of the three quadratic subfields from part (b).

Problem E. Let p be a prime. A "strict p-ring" is a p-adically complete p-torsion-free ring R for which $R/(p)$ is perfect (meaning the p-power Frobenius map $\varphi : R/(p) \longrightarrow R/(p)$ sending $x \mapsto x^p$ is a bijection).

(a) For such R check that $R/(p)$ is necessarily reduced (has no nonzero nilpotents).

(b) If $K/\mathbb{Q}_p$ is a finite extension, deduce that its valuation ring $\mathcal{O}_K$ is a strict p-ring if and only if $K/\mathbb{Q}_p$ is unramified.

(c) Prove that the projection map $\pi : R \longrightarrow R/(p)$ admits a **unique** multiplicative section $[\bullet] : R/(p) \longrightarrow R$ (known as the "Teichmüller map").

(`Hint`: For each n choose a lift $x_n \in R$ of $\varphi^{-n}(\bar{x})$. If s is a multiplicative section of the projection ($\pi \circ s = \mathrm{Id}$) show that $s(\bar{x}) = \lim_{n\to\infty} x_n^{p^n}$.)

(d) Show that every element $x \in R$ has a "Teichmüller expansion"

$$x = \sum_{n=0}^{\infty} [\bar{a}_n] \cdot p^n$$

for a **unique** sequence of coordinates $\bar{a}_0, \bar{a}_1, \bar{a}_2, \ldots$ in $R/(p)$.

(`Fact`: One can show that the functor $R \rightsquigarrow R/(p)$ is an equivalence between the category of strict p-rings and that of perfect rings of characteristic p. Given a perfect ring $\mathcal{R}$ there is a natural choice of a strict p-ring known as the ring of Witt vectors $W(\mathcal{R})$. For instance $W(\mathbb{F}_p) = \mathbb{Z}_p$ and $W(\bar{\mathbb{F}}_p) = \widehat{\mathbb{Z}_p^{\mathrm{ur}}}$, cf. Problem C on HW8.)