**Math 204A (Number Theory), UCSD, fall 2020**
**Problem Set 8 – due Thursday, December 10, 2020**

1. Show that every quadratic extension of $\mathbb{Q}_2$ is contained in $\mathbb{Q}_2(\zeta_{24})$. (Hint: first compute $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.) This is a first step towards the Kronecker-Weber theorem, which we will discuss in more detail in Math 204B.

2. Let $L/K$ be an extension of number fields. Let $\mathfrak{p}$ be a prime ideal of $K$ and suppose that there is a *unique* prime ideal $\mathfrak{q}$ of $L$ above $\mathfrak{p}$. Let $\alpha \in \mathcal{O}_K$ be an element whose image in $\mathcal{O}_L/\mathfrak{q}$ is a primitive element over $\mathcal{O}_K/\mathfrak{p}$.

   (a) Let $P(T) \in \mathcal{O}_K[T]$ be a monic polynomial whose reduction modulo $\mathfrak{q}$ is the minimal polynomial of $\alpha$ over $\mathcal{O}_K/\mathfrak{p}$. Show that there exists $\beta \in \mathcal{O}_L$ congruent to $\alpha$ modulo $\mathfrak{q}$ such that $P(\beta) \in \mathfrak{q} \setminus \mathfrak{q}^2$. (Hint: use the first-order Taylor expansion of $P$ at $\alpha$, as in the proof of Hensel's lemma.)

   (b) For $\beta$ as in (a), prove that $\mathcal{O}_{L,\mathfrak{q}} = \mathcal{O}_{K,\mathfrak{p}}[\beta]$. (This is Lemma II.10.4 of Neukirch, but try it yourself first.)

3. Let $L/K$ be a Galois extension of number fields of degree $n$. Let $\mathfrak{q}$ be a prime ideal of $L$ lying above the prime ideal $\mathfrak{p}$ of $K$.

   (a) Prove that the $\mathfrak{q}$-adic valuation of the different of $L/K$ is at most $e - 1 + v_{\mathfrak{q}}(e)$ where $e = e(\mathfrak{q}/\mathfrak{p})$. (Hint: reduce to the case where $e = [L : K]$, then look at the minimal polynomial of an element of $\mathfrak{q} - \mathfrak{q}^2$. If you get stuck, see Theorem III.2.6 of Neukirch.)

   (b) Use (a) to prove that for any fixed positive integers $n$ and $D$, there are only finitely many number fields of degree $n$ with discriminant $\pm D$. Recall that this was the missing step in the proof of the Hermite-Minkowski theorem.

4. (a) Let $K$ be a field complete with respect to a nonarchimedean absolute value. Let $P(T) \in \mathcal{O}_K[T]$ be a polynomial, and suppose $\alpha \in \mathcal{O}_K$ satisfies

$$|P(\alpha)| < |P'(\alpha)|^2.$$

   Define the sequence $\alpha = \alpha_0, \alpha_1, \dots$ by the *Newton-Raphson recursion*

$$\alpha_{n+1} = \alpha_n - \frac{P(\alpha_n)}{P'(\alpha_n)}.$$

   Prove that this sequence converges to a root of $P$ in $K$. (Hint: show that $|P'(\alpha_{n+1})| = |P'(\alpha_n)|$ but $|P(\alpha_{n+1})|$ is much smaller than $|P(\alpha_n)|$.)

   (b) Apply (a) to recover the fact that any element of $\mathbb{Z}_2$ congruent to 1 modulo 8 is a perfect square, then formulate an analogous statement for any finite extension $K$ of $\mathbb{Q}_2$.

5. (a) Let $K$ be a field equipped with (but not necessarily complete with respect to) a nonarchimedean absolute value $|\cdot|_K$. Let $K(T)$ be the fraction field of the polynomial ring $K[T]$. Prove that there exists a unique absolute value $|\cdot|_G$ on $K(T)$ such that for all $f = \sum_n f_n T^n \in K[T]$,

$$|f|_G = \max\{|f_n|_K : n = 0, 1, \dots\}.$$

This is called the *Gauss norm* on $K(T)$.

(b) Let $L$ be any field containing $K$, not necessarily a finite extension. Prove that there exists at least one extension of $|\cdot|_K$ to an absolute value on $L$. (Hint: using Zorn's lemma, reduce to the case where $L$ is generated over $K$ by a single element $\alpha$. If $\alpha$ is algebraic over $K$, use what we proved in class; otherwise, use (a).)

6. (Optional) In this exercise, we give Monsky's amazing proof of the following theorem: a square in the Euclidean plane cannot be dissected into an *odd* number of triangles, all of the same area.

(a) Let $|\cdot|_2$ be a nonarchimedean absolute value on $\mathbb{R}$ such that $|2|_2 < 1$ (which exists by the previous exercise, applying (b) with $K = \mathbb{Q}$ and $|\cdot|_K = |\cdot|_2$). Define the following partition of $\mathbb{R}^2$ into three subsets:

$$\begin{aligned} S_1 &= \{(x, y) \in \mathbb{R}^2 : |x|_2 < 1, |y|_2 < 1\} \\ S_2 &= \{(x, y) \in \mathbb{R}^2 : |x|_2 \geq 1, |x|_2 \geq |y|_2\} \\ S_3 &= \{(x, y) \in \mathbb{R}^2 : |y|_2 \geq 1, |y|_2 > |x|_2\}. \end{aligned}$$

Show that all three sets are stable under translation by any $(x, y) \in S_1$.

(b) Prove that no line in $\mathbb{R}^2$ intersects all three subsets. (Hint: reduce to the case where the line passes through $(0, 0)$.)

(c) Suppose we have a dissection of the square $[0, 1] \times [0, 1]$ into triangles. Show that there exists a triangle with one vertex in each of $S_1, S_2, S_3$. (Hint: assuming there is no such triangle, count segments with one vertex in $S_1$ and the other in $S_2$ and find a parity violation. A result of a similar nature is *Sperner's lemma*; see Zulip for more discussion.)

(d) Deduce that if there are $m$ triangles in the dissection and they all have area $1/m$, then $|1/m|_2 < 1$ and therefore $m$ is even.