18.786 Problem Set 11 (due Thursday May 6 in class)

1. Prove the local Kronecker-Weber theorem using Local class field theory, as follows. The local reciprocity map gives an isomorphism $G_K^{ab} \cong U_K \times \hat{\mathbb{Z}}$, using a splitting of the exact sequence

$$0 \to U_K \to K^\times \to \mathbb{Z} \to 0$$

i.e. a choice of uniformizer π.

   (a) Prove that $\mathbb{Q}_p^{un} = \mathbb{Q}_p(\zeta_m)_{(m,p)=1}$.

   (b) The "ramified" part of K^{ab}/K, denoted K_π, is defined to be the fixed field of $Frob_K \in G_K^{ab}$, and by the above structure theorem for G_K^{ab}, the Galois group of K_π/K is isomorphic to U_K. To prove the local Kronecker-Weber theorem we need to show that when $K = \mathbb{Q}_p, K_\pi = \mathbb{Q}_p(\zeta_{p^n})_{n \in \mathbb{Z}}$. Show it suffices to prove that the image of the norm map $N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\zeta_{p^n})$ is $U_K^{(n)} \times \mathbb{Z} \subset U_K \times \mathbb{Z} = \mathbb{Q}_p^\times$.

   (c) Now prove $N_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}\mathbb{Q}_p(\zeta_{p^n}) = U_K^{(n)} \times \mathbb{Z}$. First show that the norm of $1 - \zeta_{p^n}$ is p, and then use the index of the norm subgroup to conclude.

2. Check the assertion made in Milne V.4.1 (pg 166): i.e. check that $\mathbb{I}_{S_\infty}$ is a closed subspace of $\mathbb{I}_K$ and that the quotient is a direct sum of countably many copies of $\mathbb{Z}$ with the discrete topology.

3. Let K be a number field and let M_K be its set of valuations, normalized to be extend the valuation from $\mathbb{Q}_p$ or $\mathbb{R}$ or $\mathbb{C}$. (For example, we still have $|p|_v = 1/p$ if v lies above a prime p of $\mathbb{Q}$). Define the local degree of a valuation v to be $n_v = [K_v : \mathbb{Q}_p]$, where p is the restriction of v to $\mathbb{Q}$. For $x \in K_v$, let $\|x_v\| = |x|_v^{n_v}$. Show that for $x \in K$,

$$\prod_{v \in M_K} \|x_v\| = 1.$$

This is the product formula for number fields. (Hint: use problem 3 on problem set 7).

4. Let K be a nonarchimedean local field and $n \geq 2$ an integer. Assume K contains the n'th roots of unity. Prove the following properties of the Hilbert symbol $(,) = (,)_n$.

   (a) If $a \in K^\times$ and $x \in K$ are such that $x^n - a \neq 0$, then $(a, x^n - a) = 1$. Deduce that $(a, -a) = 1, (a, 1 - a) = 1$ and $(a, a) = (a, -1)$.

   (b) Let $a, b \in K^\times$ with $a + b \neq 0$. Show that

$$(a, b) = (a, a + b)(a + b, b)(-1, a + b)$$

   (c) Let n be odd and $a, b, c \in K^\times$ with $a + b + c = 0$. Show that $(a, b)(b, c)(c, a) = 1$.

5. Let k be a field.

   (a) Let A be the set of $a \in k^\times$ which are represented over k by the binary form $x^2 + by^2$ (i.e. there exist $x, y \in k$ such that $a = x^2 + by^2$). Show that A is a subgroup of $k^\times$.

   (b) Let $a, b \in k^\times$. Show that the form $x_1^2 + ax_2^2 + bx_3^2$ represents 0 nontrivially over k if and only iff the form $x_1^2 + ax_2^2 + bx_3^2 + abx_4^2$ does.

6. Use gp/Pari to do Exercise 3.14 in Milne. Provide output of your code and some explanation.

7. For each $p \in \{2, 3, 5, 7, 31\}$, let M be a splitting field of $X^3 - 2$ over $\mathbb{Q}_p$. Describe $\mathrm{Nm}_{M/\mathbb{Q}_p} M^\times$ as a subgroup of $\mathbb{Q}_p^\times$.

8. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial with integer coefficients, such that the degree of f is prime. Show that the reduction of $f \pmod{p}$ is irreducible for a positive density of primes p. (Hint: consider the splitting field of f and use the Chebotarev density theorem).

9. Prove the Artin-Whaples weak approximation theorem: Let $| \ |_1, \ldots, | \ |_n$ be nontrivial inequivalent valuations of a field K, and let $a_i \in K_{v_i}$, the completion of K with respect to $| \ |_i$, for each $i = 1 \ldots n$. For any $\epsilon > 0$, there is an element $a \in K$ such that $|a - a_i|_i < \epsilon$ for all i.

10. For a ring R, let $SL_n(R)$ be the group of $n \times n$ matrices with detrminant 1. Show that for any integer N, the reduction map $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/N\mathbb{Z})$ is surjective.