PROBLEM SET 8

Problem 1. Show that the question of whether 13 is a square modulo an odd prime p can be decided by looking at the residue of p modulo 13, and make this explicit. Similarly, show that the question of whether 11 is a square modulo p can be decided by looking at the residue of p modulo 44, and make this explicit. What analogous statements can be made for the question of whether a general prime number q is a square mod p? What about a general number a, not necessarily prime, instead of q?

Problem 2. A *discrete valuation* on a field F is a homomorphism $v : F^\times \to \mathbb{Z}$ such that $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in F^\times$ with $x + y \neq 0$. Show that if v is a discrete valuation on a field F, then the set of $x \in F$ with $v(x) \geq 0$ is a subring $\mathcal{O} \subset F$ which has a unique maximal ideal $\mathfrak{m}$ given by the set of $x \in F$ with $v(x) > 0$. The quotient $k = \mathcal{O}/\mathfrak{m}$ is called the *residue field*. Make all of this explicit for the p-adic valuation on $\mathbb{Q}$.

Problem 3. Let v be a discrete valuation on a field F as in the previous exercise. Show that the function which sends $a, b \in F^\times$ to

$$(a, b)_v := (-1)^{v(a)v(b)} \cdot \overline{a^{v(b)}/b^{v(a)}}$$

is a Steinberg symbol on F with values in $k^\times$, called the *tame symbol* associated to v. Here the bar on top stands for reduction modulo $\mathfrak{m}$.

The following two problems were essentially also given by Akhil in problem set 4 in the language of absolute values, but perhaps it is good to revisit them in the language of discrete valuations.

Problem 4. Let k be a field. Recall that the ring of polynomials $k[t]$ has unique prime factorization. It is somewhat analogous to the ring of integers $\mathbb{Z}$. In this analogy, prime numbers correspond to monic irreducible polynomials. Show that to every monic irreducible polynomial $f \in k[t]$ there corresponds a discrete valuation on the field of fractions $k(t)$, defined analogously to the p-adic valuation. Identify the associated residue field with the quotient $k[t]/(f)$.

Problem 5. Besides the discrete valuations corresponding to monic irreducible polynomials, show that there is a further discrete valuation on $k(t)$ defined by $v(f) = -\deg(f)$, where this means $\deg(a) - \deg(b)$ if we write f as the quotient of two polynomials a and b. In the analogy with the integers, this discrete valuation corresponds to the usual absolute value on $\mathbb{Q}$ giving rise to the real numbers by completion. Show that, up to isomorphism, all of these discrete valuations you produced are distinct and that they give all discrete valuations on $k(t)$ which are trivial on the constants $k^\times$.

Date: July 21, 2021.