Math 204A (Number Theory), UCSD, fall 2020
Problem Set 7 – due Thursday, December 3, 2020

1. (a) Let p be a prime number. Prove that for any commutative ring R, any ideal I, and any $x, y \in R$ such that $x \equiv y \pmod{I}$, we have $x^p \equiv y^p \pmod{I^p + pI}$.

   (b) Let L/K be a Galois extension of number fields, let $\mathfrak{q}$ be a nonzero prime ideal of $\mathcal{O}_L$, and choose $\pi \in \mathfrak{q} \setminus \mathfrak{q}^2$. Suppose that $\sigma \in \mathrm{Gal}(L/K)_{\mathfrak{q},0}$ satisfies $\sigma(\pi)/\pi \equiv 1 \pmod{\mathfrak{q}^n}$ for some positive integer n. Prove that $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{n+1}}$ for all $\alpha \in \mathcal{O}_L$. (Hint: every element of $\mathcal{O}_L$ can be written as $\beta^p + \pi\gamma$ for some $\beta, \gamma \in \mathcal{O}_L$, and similarly even if you replace the exponent p with a higher power of p.)

2. Let K be the number field $\mathbb{Q}(2^{1/4})$. Let L be the Galois closure of K and put $G = \mathrm{Gal}(L/K)$.

   (a) Compute the ring of integers $\mathcal{O}_L$ (e.g., using SageMath).

   (b) Check that there is a single prime $\mathfrak{q}$ of L above 2 and that $\mathfrak{q}$ is totally ramified over 2.

   (c) Compute the groups $G_{\mathfrak{q},s}$ for all s.

   (d) Use the answer to (c) to compute the different of $L/\mathbb{Q}$.

3. Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K lying above the prime p of $\mathbb{Q}$. Let $\mathfrak{q}$ be a prime above L. Suppose that $e = e(\mathfrak{q}/\mathfrak{p})$ is not divisible by p (that is, $\mathfrak{q}$ is *tamely ramified* over $\mathfrak{p}$).

   (a) Show that $G_{\mathfrak{q},1}$ is the trivial group. (Hint: use what we know about the quotients $G_{\mathfrak{q},s}/G_{\mathfrak{q},s+1}$.)

   (b) Show that
   $$\mathcal{D}_{\mathcal{O}_{L,\mathfrak{q}}/\mathcal{O}_{K,\mathfrak{p}}} = \mathfrak{q}^{e-1}.$$
   (Hint: first reduce to the case $f(\mathfrak{q}/\mathfrak{p}) = 1$.)

4. Prove that an element x of $\mathbb{Z}_2 \setminus 2\mathbb{Z}_2$ is a perfect square if and only if $x \equiv 1 \pmod{8}$.

5. (a) Prove that $\mathbb{Z}[\![x]\!]/(x-p) \cong \mathbb{Z}_p$. This is done in Neukirch, but try it yourself first.

   (b) Prove that $\mathbb{Z}((x))/(x-p) \cong \mathbb{Q}_p$.

6. Prove the following facts that were stated without proof in lecture.

   (a) If p is a prime and m is a positive integer, then
   $$\varprojlim_n \mathbb{Z}/(p^m)^n\mathbb{Z} \cong \mathbb{Z}_p.$$

   (b) If m_1, m_2 are coprime integers greater than 1, then
   $$\varprojlim_n \mathbb{Z}/(m_1m_2)^n\mathbb{Z} \cong \varprojlim_n \mathbb{Z}/m_1^n\mathbb{Z} \times \varprojlim_n \mathbb{Z}/m_2^n\mathbb{Z}.$$

7. (a) Prove that the field $\mathbb{R}$ has no automorphisms other than the identity, using the fact that the squares in $\mathbb{R}$ are precisely the nonnegative elements.

   (b) Let $p > 2$ be a prime. Show that every element of $\mathbb{Z}_p$ congruent to 1 modulo p^2 has a p-th root, using the binomial series.

   (c) Optional: For $p > 2$, prove that the field $\mathbb{Q}_p$ has no automorphisms other than the identity. (See Zulip for hints.)