Math 204A (Number Theory), UC San Diego, fall 2022
Problem Set 6 – due Thursday, November 10, 2022

Submit *at most five* of the listed problems.

1. Let L/K be an extension of number fields with Galois closure M and Galois group G. Put $H = \mathrm{Gal}(M/L)$. Assume that every element of G generates the decomposition group of some unramified prime of M (this is a corollary of the Chebotarev density theorem). Show that if every prime of $\mathfrak{o}_K$ which does not ramify in M has the property that all of the primes above it in L have the *same* inertial degree, then L/K is Galois. (Hint: use the fact that a cyclic group has only one subgroup of any given order.)

2. Let $K/\mathbb{Q}$ be a non-Galois cubic extension with squarefree discriminant, let L be the Galois closure of K, and let M be the quadratic subextension of L. Prove that no prime of M ramifies in L. (Optional: do the same for $K/\mathbb{Q}$ of degree n with Galois group S_n.)

3. Let L/K be an extension of number fields with Galois closure M. Let $\mathfrak{p}$ be a prime of K.

   (a) Prove that if $\mathfrak{p}$ is unramified in L, then it is unramified in M also.

   (b) Prove that if $\mathfrak{p}$ is unramified and totally split in L, then it is totally split in M also.

4. Let m be an integer which is not a perfect square, and put $K = \mathbb{Q}(m^{1/4})$. Let L be the Galois closure of $K/\mathbb{Q}$. Let p be an odd prime not dividing m and let $\mathfrak{q}$ be a prime above p in L. For each possible value for the decomposition group $G_\mathfrak{q}$, describe the corresponding splitting of p in K.

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. (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

$$\varprojlim_n \mathbb{Z}/(m_1m_2)^n\mathbb{Z} \cong \varprojlim_n \mathbb{Z}/m_1^n\mathbb{Z} \times \varprojlim_n \mathbb{Z}/m_2^n\mathbb{Z}.$$

   For example, this means that the "ring of 10-adic integers" is not an integral domain.

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

8. (a) Prove that the field $\mathbb{R}$ has no automorphisms other than the identity even if we *do not* require them to be continuous. (Hint: use 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: Prove that the field $\mathbb{Q}_p$ has no automorphisms other than the identity even if we *do not* require them to be continuous. (See Zulip for hints.)