Math 204B (Number Theory), UCSD, winter 2021
Problem Set 9 – due Thursday, January 14, 2021

Some reminders: solutions should be submitted via CoCalc (same project as for 204A). Place your solutions in the folder `assignments/2021-01-14/` in your course project.

Collaboration and research is fine, as long as you do the following.

- Try the problems yourself first!
- Write the solutions in your own words.
- Acknowledge all sources (textbooks, results from class or previous problem sets, etc.) and collaborators.

New for 204B: please request all extensions *in advance* of the due date. Remember, you only need to submit 6 of 9 complete problem sets for full credit (or one fewer if you choose the final project option).

1. Let n be a positive integer and let K be a field of characteristic coprime to n. (Note that we are not assuming that $\zeta_n \in K$.)
   (a) Show that for any $a \in K^\times$, $[K(a^{1/n}) : K]$ is a divisor of n. (Hint: use induction to reduce to the case where n is prime, then compare what happens over K and $K(\zeta_n)$.)
   (b) Show that $[K(a^{1/n}) : K] = n$ if and only if $a \notin (K^\times)^p$ for each prime divisor p of n. (Hint: there is a reduction to the case where $n = p^2$ and $\zeta_p \in K$. In this case, distinguish according to whether or not $\zeta_n \in K$.)
2. Prove *Dedekind's lemma* on linear independence of automorphisms: if L/K is a field extension and $g_1, \ldots, g_n$ are distinct automorphisms of L over K, then there do not exist $x_1, \ldots, x_n \in L$ such that $x_1 g_1(y) + \cdots + x_n g_n(y) = 0$ for all $y \in L$. (Hint: choose a counterexample with n minimal, noting that necessarily $n > 1$. Since $g_1 \neq g_2$, we can find an element $z \in L^\times$ such that $g_1(z) \neq g_2(z)$. We can then modify our original relation either by multiplying on the outside by z or by rescaling the variable y by z; compare these and obtain a contradiction to the choice of n.)
3. (a) Let K be a field of characteristic zero not containing $\sqrt{-1}$. Suppose that there exists a Galois extension L of K containing $\sqrt{-1}$ with Galois group $\mathbb{Z}/4\mathbb{Z}$. Prove that there must exist $x, y \in K$ such that $x^2 + y^2 = -1$. (Hint: write L as $K(\sqrt{-1}, a^{1/2})$ for some $a \in K(\sqrt{-1})$. Let σ be a generator of $\mathrm{Gal}(L/K)$ and write $\sigma(a)/a = (x + y\sqrt{-1})^2$.)
   (b) Show that no such extension can exist when $K = \mathbb{Q}_2$.
4. (a) Show that there is no Galois extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/4\mathbb{Z})^3$. (Hint: separate cases based on whether or not this extension contains $\sqrt{-1}$, and remember the classification of quadratic extensions of $\mathbb{Q}_2$ from PS 8.)

(b) Let K be a Galois extension of $\mathbb{Q}_2$ such that $\mathrm{Gal}(K/\mathbb{Q}_2)$ is an abelian group of order a power of 2. Prove that K is contained in $\mathbb{Q}(\zeta_N)$ for some positive integer N.

5. Let p be an odd prime. Let U_1 be the set of elements of $\mathbb{Z}_p[\zeta_p]$ congruent to 1 modulo $\pi = 1 - \zeta_p$. Prove that U_1^p equals the set of elements of $\mathbb{Z}_p[\zeta_p]$ congruent to 1 modulo π^{p+1}. (Hint: use the binomial series as in PS 7 problem 7(b).)