Math 204A (Number Theory), UC San Diego, fall 2022
Problem Set 4 – due Thursday, October 27, 2022

Submit *at most five* of the listed problems.

1. Neukirch, exercise I.7.6: Let K be a totally real number field, let $X := \mathrm{Hom}(K, \mathbb{R})$, and let T be a nonempty proper subset of X. Then there exists a unit $\epsilon \in \mathfrak{o}_K^\times$ satisfying $0 < \tau(\epsilon) < 1$ for all $\tau \in T$ and $\tau(\epsilon) > 1$ for all $\tau \notin T$.

2. Neukirch, exercise I.8.4: Show that a prime ideal $\mathfrak{p}$ of a number field K is totally split in a separable extension L/K if and only if it is totally split in the Galois closure N/K of L/K.

3. Neukirch, exercise I.8.3: Show that if a prime ideal $\mathfrak{p}$ of a number field K is totally split in two separable extensions L_1/K and L_2/K, then it is also totally split in the composite extension. (You may use the previous exercise if you wish.)

4. Let p be an odd prime. For this problem, you may assume that the ring of integers in $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$ (this will be proved in class at some point).

   (a) Show that $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]^\times$ is a subgroup of finite index of $\mathbb{Z}[\zeta_p]^\times$.

   (b) Let c be the nontrivial automorphism of $\mathbb{Q}(\zeta_p)$ fixing $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Prove that for any $\alpha \in \mathbb{Z}[\zeta_p]^\times$, α/α^c is a root of unity.

   (c) Prove that the quotient $\mathbb{Z}[\zeta_p]^\times / \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^\times$ is generated by ζ_p. (Hint: first use (b) to show that if $\alpha \in \mathbb{Z}[\zeta_p]^\times$, then there exists $j \in \{0, \ldots, p-1\}$ such that $(\zeta_p^j \alpha)^2 \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^\times$.)

5. Put $K = \mathbb{Q}(\zeta_7)$.

   (a) Show by "pure thought" that K contains a subfield of degree 2 over $\mathbb{Q}$ and a subfield of degree 3 over $\mathbb{Q}$.

   (b) Describe each of these fields as $\mathbb{Q}[\alpha]/(P(\alpha))$ for some irreducible polynomial $P(x) \in \mathbb{Q}[x]$.

6. Let K be the number field $\mathbb{Q}[\alpha]/(\alpha^3 - \alpha - 1)$. Write some code in SageMath (or another system) to show that there is no modulus $m \leq 100$ for which the splitting of a prime p in K is determined by the reduction of p modulo m. (That is, for each m, you should find two primes with the same remainder modulo m but different splitting behavior.)

7. Let K be the number field $\mathbb{Q}[\alpha]/(\alpha^3 - \alpha - 1)$. Let L be the Galois closure of $K/\mathbb{Q}$. Check that L contains $\mathbb{Q}(\sqrt{-23})$ and that no prime of $\mathbb{Q}(\sqrt{-23})$ ramifies in L. (You may ask SageMath to compute $\mathfrak{o}_L$.)

8. Using Dirichlet's theorem on primes in arithmetic progressions, prove that every finite abelian group occurs as $\mathrm{Gal}(K/\mathbb{Q})$ for some number field K.