Math 204A (Number Theory), UCSD, fall 2020
Problem Set 4 – due Thursday, November 5, 2020

Unless otherwise specified, you may use SageMath (or another computer algebra system, but please specify which one) without restriction.

1. Let R be a Dedekind domain. Prove that the following statements are equivalent.

   (a) The ring R is a principal ideal domain.

   (b) The ring R is a unique factorization domain.

   (c) The class group of R is trivial.

   (Hint: for (b) $\implies$ (c), it is enough to show that every prime ideal $\mathfrak{p}$ is trivial. First show that $\mathfrak{p}$ contains an irreducible element α, then show that α generates a nonzero prime ideal.)

2. Let p be an odd prime and put $K = \mathbb{Q}(\zeta_p)$. Using results from previous homework, show that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

3. Let p be an odd prime.

   (a) By computing signatures, verify 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. (Hint: use PS1 problem 7.)

   (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 $j \in \{0, \dots, p-1\}$ such that $(\zeta_p^j \alpha)^2 \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]^\times$.)

4. 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 $P(x) \in \mathbb{Q}[x]$.

5. 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.)