Math 204A (Number Theory), UCSD, fall 2020
Problem Set 3 – due Thursday, October 29, 2020

This problem set refers to the L-Functions and Modular Forms Database, and specifically to the tables of number fields. Go to `https://www.lmfdb.org/NumberField/` to get started.

1. Let K be a number field of degree n with signature (r_1, r_2). We derive Minkowski's improved estimate for the minimum norm of an ideal in an ideal class of K.

   (a) Prove that for any $t > 0$, the region
   $$X = \{(z_\tau) \in K_\mathbb{R} : \sum_\tau |z_\tau| < t\}$$
   has volume $2^{r_1}\pi^{r_2}\frac{t^n}{n!}$. (Hint: it may be easiest to set this up as a multiple integral, using polar coordinates for each complex embedding.)

   (b) Show that any nonzero ideal I of $\mathcal{O}_K$ contains a nonzero element α satisfying
   $$\left|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)\right| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}[\mathcal{O}_K : I].$$
   (Hint: apply Minkowski's lattice point theorem to the region X from (a), then use the arithmetic-geometric mean inequality.)

   (c) Deduce (as in lecture) that every ideal class of K is represented by some integral ideal of norm at most $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$.

2. Let K be a number field for which $|d_K| = 1$. Prove that $K = \mathbb{Q}$. (Hint: show that $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^n < 1$ for $n > 1$, then apply the previous exercise.)

3. Use the improved Minkowski estimate to show that $\mathbb{Q}(\sqrt{11})$ has class number 1.

4. Let K be the number field $\mathbb{Q}[x]/(x^3 - x^2 + x + 1)$.

   (a) Find the home page of K in the LMFDB.

   (b) Report what the LMFDB says about the signature of K and the structure of the group $\mathcal{O}_K^\times$ (including generators).

   (c) Prove that this answer is correct.

5. Repeat part (a) and (b) of the previous exercise for the fields
   $$\mathbb{Q}(2^{1/3}), \qquad \mathbb{Q}(\sqrt{3}, \sqrt{5}), \qquad \mathbb{Q}(\zeta_5).$$
   (Hint: it may help to filter by signature and/or Galois group.)