MATH 254A PROBLEM SET 3
DUE MONDAY, SEPT. 26

BRIAN OSSERMAN

Exercise 1. Show that if I, J are non-zero ideals of a ring of integers $\mathscr{O}_K$, then $N(IJ) = N(I)N(J)$. Hint: reduce to the case that $I = \mathfrak{p}$ is a non-zero prime, then write $\#\mathscr{O}_K/(\mathfrak{p}J) = \#\mathscr{O}_K/J \cdot \#J/(\mathfrak{p}J)$, and consider $J/\mathfrak{p}J$ as a $\mathscr{O}_K/\mathfrak{p}$-vector space.

Exercise 2. Using Minkowski's bounds on the norm of representatives of each ideal class, compute the ideal class group of $\mathbb{Z}[\sqrt{-5}]$. Follow the method from the example in lecture.

The following isn't relevant to algebraic number theory, but gives an addition application of Minkowski's theorem.

Exercise 3. Use Minkowski's theorem on convex regions and lattices to give a different proof that if -1 is a square mod a prime p, then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

Hint: consider the lattice generated by $(p, 0)$ and $(x, 1)$ in $\mathbb{R}^2$, where $x^2 \equiv -1 \pmod{p}$.