Harvard Math 129: Algebraic Number Theory
Homework Assignment 3

William Stein

Due: Thursday, March 3, 2005

The problems have equal point value, and multi-part problems are of the same value. There are **five** *problems. In any problem where you use a computer, include in your solution the exact commands you type and their output. You may use any software, including (but not limited to) MAGMA and PARI.*

1. Let $\varphi : R \to S$ be a homomorphism of (commutative) rings.
   (a) Prove that if $I \subset S$ is an ideal, then $\varphi^{-1}(I)$ is an ideal of R.
   (b) Prove moreover that if I is prime, then $\varphi^{-1}(I)$ is also prime.

2. Let $\mathcal{O}_K$ be the ring of integers of a number field. The Zariski topology on the set $X = \mathrm{Spec}(\mathcal{O}_K)$ of all prime ideals of $\mathcal{O}_K$ has closed sets the sets of the form
$$V(I) = \{\mathfrak{p} \in X : \mathfrak{p} \mid I\},$$
where I varies through *all* ideals of $\mathcal{O}_K$, and $\mathfrak{p} \mid I$ means that $I \subset \mathfrak{p}$.
   (a) Prove that the collection of closed sets of the form $V(I)$ is a topology on X.
   (b) Let Y be the subset of nonzero prime ideals of $\mathcal{O}_K$, with the induced topology. Use unique factorization of ideals to prove that the closed subsets of Y are exactly the finite subsets of Y along with the set Y.
   (c) Prove that the conclusion of (a) is still true if $\mathcal{O}_K$ is replaced by an order in $\mathcal{O}_K$, i.e., a subring that has finite index in $\mathcal{O}_K$ as a $\mathbb{Z}$-module.

3. Explicitly factor the ideals generated by each of 2, 3, and 5 in the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$. (Thus you'll factor 3 separate ideals as products of prime ideals.) You may assume that the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$, but do *not* simply use a computer command to do the factorizations.

4. Let $K = \mathbb{Q}(\zeta_{13})$,where ζ_{13} is a primitive 13th root of unity. Note that K has ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{13}]$ (you do not have to prove this).

   (a) Factor 2, 3, 5, 7, 11, and 13 in the ring of integers $\mathcal{O}_K$. You may use a computer.

   (b) For $p \neq 13$, find a conjectural relationship between the number of prime ideal factors of $p\mathcal{O}_K$ and the order of the reduction of p in $(\mathbb{Z}/13\mathbb{Z})^*$.

   (c) Compute the minimal polynomial $f(x) \in \mathbb{Z}[x]$ of ζ_{13}. Reinterpret your conjecture as a conjecture that relates the degrees of the irreducible factors of $f(x) \pmod p$ to the order of p modulo 13. Does your conjecture remind you of quadratic reciprocity?

5. (a) Find by hand and with proof the ring of integers of each of the following two fields: $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i)$.

   (b) Find the ring of integers of $\mathbb{Q}(x^5 + 7x + 1)$ using a computer.