Harvard Math 129: Algebraic Number Theory
Homework Assignment 7

William Stein

Due: THURSDAY, April 14, 2005

The problems have equal point value, and multi-part problems are of the same value. 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 K be a number field. Prove that $p \mid d_K$ if and only if p ramifies in K. (Note: This fact is proved in many books—finding a proof in one and rephrasing it in your own words and the context of this course is *not* cheating.)

2. Using Zorn's lemma, one can show that there are homomorphisms $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ with finite image that are not continuous, since they do not factor through the Galois group of any finite Galois extension. [Hint: The extension $\mathbb{Q}(\sqrt{d}, d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2)$ is an extension of $\mathbb{Q}$ with Galois group $X \approx \prod \mathbb{F}_2$. The index-two open subgroups of X correspond to the quadratic extensions of $\mathbb{Q}$. However, Zorn's lemma implies that X contains many index-two subgroups that do not correspond to quadratic extensions of $\mathbb{Q}$.]

3. (a) Give an example of a finite nontrivial Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_{\mathfrak{p}} = \mathrm{Gal}(K/\mathbb{Q})$.
   (b) Give an example of a finite nontrivial Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_{\mathfrak{p}}$ has order 1.
   (c) Give an example of a finite Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $D_{\mathfrak{p}}$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$.
   (d) Give an example of a finite Galois extension K of $\mathbb{Q}$ and a prime ideal $\mathfrak{p}$ such that $I_{\mathfrak{p}}$ is not a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$.

4. Let S_3 by the symmetric group on three symbols, which has order 6.
   (a) Observe that $S_3 \cong D_3$, where D_3 is the dihedral group of order 6, which is the group of symmetries of an equilateral triangle.

(b) Use (4a) to write down an explicit embedding $S_3 \hookrightarrow \mathrm{GL}_2(\mathbb{C})$.

(c) Let K be the number field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega^3 = 1$ is a nontrivial cube root of unity. Show that K is a Galois extension with Galois group isomorphic to S_3.

(d) We thus obtain a 2-dimensional irreducible complex Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \cong S_3 \subset \mathrm{GL}_2(\mathbb{C}).$$

Compute a representative matrix of Frob_p and the characteristic polynomial of Frob_p for $p = 5, 7, 11, 13$.