Harvard Math 129: Algebraic Number Theory
Homework Assignment 9

William Stein

Due: Thursday, April 28, 2005

The problems have equal point value (except 4 below), 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. Suppose G is a finite group and A is a finite G-module. Prove that for any q, the group $\mathrm{H}^q(G, A)$ is a torsion abelian group of exponent dividing the order $\#A$ of A.

2. Let $K = \mathbb{Q}(\sqrt{5})$ and let $A = U_K$ be the group of units of K, which is a module over the group $G = \mathrm{Gal}(K/\mathbb{Q})$. Compute the cohomology groups $\mathrm{H}^0(G, A)$ and $\mathrm{H}^1(G, A)$. (You shouldn't use a computer, except maybe to determine U_K.)

3. Let $K = \mathbb{Q}(\sqrt{-23})$ and let C be the class group of $\mathbb{Q}(\sqrt{-23})$, which is a module over the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Determine $\mathrm{H}^0(G, C)$ and $\mathrm{H}^1(G, C)$. (Use of a computer is fine.)

4. [This problem is double credit, i.e., it counts as two problems.] Let E be the elliptic curve $y^2 = x^3 + x + 1$. Let $E[2]$ be the group of points of order dividing 2 on E. Let
$$\overline{\rho}_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[2])$$
be the mod 2 Galois representation associated to E.
   (a) Find the fixed field K of $\ker(\overline{\rho}_{E,2})$.
   (b) Is $\overline{\rho}_{E,2}$ surjective?
   (c) Find the group $\mathrm{Gal}(K/\mathbb{Q})$.
   (d) Which primes are ramified in K?
   (e) Let I be an inertia group above 2, which is one of the ramified primes. Determine $E[2]^I$ explicitly for your choice of I. What is the characteristic polynomial of Frob_2 acting on $E[2]^I$.
   (f) What is the characteristic polynomial of Frob_3 acting on $E[2]$?