Math 129: Algebraic Number Theory
Homework Assignment 7

William Stein

Due: Thursday, April 8, 2004

1. 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 (1a) to write down an explicit embedding $S_3 \hookrightarrow \mathrm{GL}_2(\mathbf{C})$.
   (c) Let K be the number field $\mathbf{Q}(\sqrt[3]{2}, \omega)$, 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
   $$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) \cong S_3 \subset \mathrm{GL}_2(\mathbf{C}).$$
   Compute a representative matrix of Frob_p and the characteristic polynomial of Frob_p for $p = 5, 7, 11, 13$.

2. Let $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$. Show that K is Galois over $\mathbf{Q}$, compute the Galois group of K, and compute Frob_{37}.

3. Decide on a final project for this course. Here are some possible ideas, though you need not do a project on one of these. Joint projects are a possibility (see me).
   (a) How to compute class groups of number fields.
   (b) How to compute the unit group of a number field (we didn't even prove the unit group is computable in class).
   (c) How to solve the norm equation $\mathrm{Norm}_{K/\mathbf{Q}}(x) = d$.
   (d) Explore relations between quadratic reciprocity and class field theory for $\mathbf{Q}$.
   (e) The Chebotarev Density Theorem: read about it and explain what the point is, and something about why it is true (e.g., for quadratic fields).
   (f) Give a proof of Dirichlet's theorem on primes in an arithmetic progression (connected to the Chebotarev project above).
   (g) Connection between ideal class groups of quadratic imaginary fields and classes of positive definite binary quadratic forms. Gauss's class number problem.
   (h) The conjecture that there are infinitely many number fields of class number 1. What is known? What do the Cohen-Lenstra heuristics predict? Why is this problem so hard?
   (i) Quadratic imaginary fields and complex multiplication elliptic curves.
   (j) Elements of Shafarevich-Tate groups: give complete examples with proofs of equations like $3x^3 + 4y^3 + 5z^3 = 0$ that have a solution (with not all x, y, z zero) over every p-adic field $\mathbf{Q}_p$ and over $\mathbf{R}$, but not over $\mathbf{Q}$.