18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 5, due Thursday, March 23

1. Janusz p. 58, exercise 5.

2. Janusz p. 62, exercise 3.

3. Let K be an abelian extension of $\mathbb{Q}$ whose Galois group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$ for some n, and which is unramified over all rational primes $p \neq 2$. Prove that $K \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ (so that in particular $n \leq 2$).

4. (a) Prove that for each prime p and each positive integer n, there exists an abelian extension of $\mathbb{Q}$ whose Galois group is cyclic of order p^n, and which is only ramified above p. (Hint: find it inside a cyclotomic field. The case $p = 2$ is a little bit special.)
   (b) For $p = 3, 5$ and $n = 1$, find an explicit polynomial $P(x)$ such that the extension in (a) is isomorphic to $\mathbb{Q}[x]/(P(x))$.

5. Let p, q be distinct primes which are both congruent to 1 modulo 4.
   (a) Prove that the class group $\mathbb{Q}(\sqrt{pq})$ contains a nontrivial element of order 2.
   (b) Prove that $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is everywhere unramified over $\mathbb{Q}(\sqrt{pq})$.

   (The relationship between these two statements will be explained later in terms of class field theory.)

6. Janusz p. 73, exercise 1 (this is related to the previous problem).

7. Let E be the elliptic curve $y^2 = x^3 + x + 1$ over $\mathbb{Q}$. On a previous problem set, I explained how the $\overline{\mathbb{Q}}$-points of E form an abelian group.
   (a) Find the polynomial whose roots are the x-coordinates of the nontrivial 3-torsion points of E. (Hint: equate $2P$ with $-P$.)
   (b) Check your answer for (a) using SAGE. (Hint: you computed a "division polynomial".)
   (c) Use SAGE to compute the Galois group of the number field generated by the roots of the polynomial you computed in (a).
   (d) (Optional) Repeat (a) and (c) for the 5-torsion (the degree of the polynomial should be 12), then note that the answer is not S_{12} (its order is too small). How could you have predicted this before doing the calculation? (Hint: the action of the Galois group commutes with the addition law.)
   (e) (Optional) The discriminant of the polynomial $x^3 + x + 1$ turns out to be -31. Why does that imply (without further calculation) that the number field you considered in (c) is unramified above all primes $p \notin \{3, 31\}$? (Hint: for such p, the computation of the division polynomial commutes with reduction modulo p.)