# Math 581d, Fall 2010, Homework 7

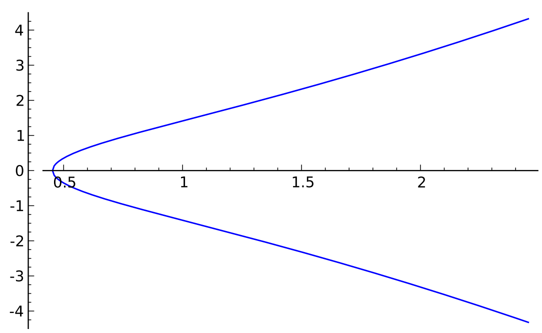
William Stein

Due: November 17, 2010

Do the following 10 problems, and turn them in by Wednesday, November 17, 2010. As usual, you can find the latex of this file at `http://wstein.org/edu/2010/581b/hw/`. You may use mathematics software however you want in this problem set.

Let $E$ be the elliptic curve defined by equation $y^2 = x^3 + 2x - 1$.

```
sage: E = EllipticCurve([2,-1]); E
Elliptic Curve defined by y^2 = x^3 + 2*x - 1 over Rational Field
sage: E.plot(plot_points=300)
```




1. How many elements $P \in E(\mathbf{C})$ have additive order dividing 2?

2. Let $K$ be the number field $\mathbf{Q}(E[2])$, i.e., the number field got by adjoining to $\mathbf{Q}$ the $x$ and $y$ coordinates of every element of order 2 in $E(\mathbf{C})$. What is $n = [K : \mathbf{Q}]$?

3. What is the Galois group of $K$ over $\mathbf{Q}$? In addition to the `galois_group` command in Sage, I find the `embeddings` command useful, since it gives every element of the Galois group explicitly as a map. This will be useful later in Problem 9 below.

```
sage: phi = K.embeddings(K); phi
...
Ring endomorphism of Number Field in b with defining polynomial ...
  Defn: b |--> -140/12461*b^5 + ...
sage: phi[1](K.0)
...
```

4. What is the abstract structure of the unit group of $K$? I.e., if you write $U_K = \mathcal{O}_K^\times$ as $T \times \mathbf{Z}^m$, with $T$ finite, what is $T$ and what is $m$?

5. What is the structure of the class group of the ring of integers of $K$?

6. Which primes are ramified in the field $K$? (Recall that a prime $p$ *ramifies* in a field $K$ if the prime factorization of $p\mathcal{O}_K$ is not square free, and the primes that ramify are exactly the primes that divide the discriminant of $\mathcal{O}_K$.)

7. Describe a fixed choice of injective homomorphism $\mathrm{Gal}(K/\mathbf{Q}) \hookrightarrow \mathrm{GL}_2(\mathbf{F}_2)$. Congratulations, you are now the proud owner of a mod 2 Galois representation $\rho : \mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_2)$.

8. How does the prime ideal $5\mathcal{O}_K$ factor in $K$? What about the primes $7\mathcal{O}_K$ and $11\mathcal{O}_K$?

9. Let $\mathfrak{p}$ be one of the primes of $\mathcal{O}_K$ lying over 5, i.e., dividing $5\mathcal{O}_K$. Compute $\rho(\mathrm{Frob}_\mathfrak{p}) \in \mathrm{GL}_2(\mathbf{F}_2)$ explicitly. Do the same for $p = 7$ and $p = 11$.

10. Let $N_p$ be the number of points on $E$ modulo $p = 5$, $p = 7$, and $p = 11$, and let $a_p = p + 1 - N_p$.

```
sage: E.Np(5)
7
```

As a consistency check, you should find that $\mathrm{Trace}(\rho(\mathrm{Frob}_\mathfrak{p})) \equiv a_p \pmod 2$.