Algebra and discrete mathematics, homework sheet 5

Due: 25 March 2014, 8:45

You can hand in alone or in groups of two; specify names and student numbers. To hand in send email to `tanja@hyperelliptic.org` with your program. Please include your program as a .txt or .sage file or save it as a worksheet.

1. You can generate a finite field with p elements (i.e. a field isomorphic to $\mathbb{Z}/p$) using `FiniteField(p)`. This command also takes prime powers, in this case you should specify the polynomial variable as follows: `k.<x>= FiniteField(p^n)`. Internally sage uses a polynomial representation $(\mathbb{Z}/p)[x]/(f(x))$.
   Generate a field with 81 elements and find out what polynomial is used internally.
   Hint: $1, x, x^2, \ldots$ form a basis.

2. Example 7.4.32 shows how to compute the fixed field of a homomorphism by hand. For the field with 81 elements generated in the first part of this homework sheet find the elements fixed by the map $x \mapsto x^9$ and those fixed by $x \mapsto x^3$. (This should be simpler than the steps done by hand.)

3. Find all irreducible polynomials of degree 5 over $\mathbb{Z}/2$.
   Hint: polynomials have a `.is_irreducible()` function. Make sure that your polynomials are defined over $\mathbb{Z}/2$.