Exercises: Week 2

Computation in Algebra and Arithmetic

David Loeffler & Tim Gehrunger

11.3.2022

Sage provides standard constructions for polynomials. A brief introduction on how they are implemented can be found here: `https://doc.sagemath.org/html/en/tutorial/tour_polynomial.html`.

1 Polynomials over finite fields I

Find out, without directly using the method is_irreducible(), which of the following Polynomials are irreducible in $\mathbf{F}_2$.
Hint: You might want to consider using the polynomial $t^{2^N} - t$ for some N.

(1) $t^5 + t^4 + t^2 + 1$;

(2) $t^8 + t^7 + t^5 + t^3 + t^2 + 1$;

(3) $t^5 + t^4 + t^3 + t^2 + 1$.

(4) $t^{20} + t^{19} + t^{17} + t^9 + t^8 + t^7 + t^6 + t^3 + t^2 + t + 1$

If you are not convinced that computer algebra programs are useful, try one of these computations by hand.

2 Polynomials over finite fields II

Consider the polynomials from the first exercise, now over $\mathbf{F}_4$. Compute, for each polynomial given polynomial f, a distinct degree factorization, that is find polynomials $g_j \in \mathbf{F}_4[t]$ which are products of irreducible polynomials of degree exactly j such that

$$f = \prod_{j=1}^{m} g_j.$$

Note that $2^2 = 4$ and that you can recycle some computations from the first exercise.

3 Irreducibility over different fields

Consider the polynomial $t^4 + 1$. Verify in sage that it is irreducible over $\mathbf{Q}$ but reducible over $\mathbf{F}_2, \mathbf{F}_3, \mathbf{F}_4, \mathbf{F}_5, \mathbf{F}_7, \mathbf{F}_{11}$. Also compute and have a look at the factors. Can you prove that $t^4 + 1$ is reducible over every finite field?

4 Being square-free over different fields

Consider the polynomial $t^2 + 1$.

1. Show that it is square-free over $\mathbf{Q}$.
2. Can you find a prime p such that the polynomial is not square-free over $\mathbf{F}_p$?
3. Show that the polynomial is square-free over all but finitely many primes.
4. In this spirit, show that any polynomial which is square-free over $\mathbf{Q}$ is square-free over all but finitely many primes by explicitly constructing an integer in the ideal (f, f').