Finite fields & p-adic numbers

Marine Rougnant

19/02/2024 - 23/02/2024

1 Finite fields

Exercise 1.

Let $L = \mathbb{F}_2[X]/(X^2 + X + 1)$.

1. Define a generator g of L.
2. Retrieve, from g, the polynomial defining the field L.
3. Determine the characteristic of L.
4. L is a field with four elements. Write its addition and multiplication tables.

Exercise 2.

1. Find a polynomial T defining $\mathbb{F}_{27} = \mathbb{F}_3(t)/(T)$.
2. Check that T is actually $t^3 + t^2 + t + 2$ and irreducible over $\mathbb{F}_3$.
3. We want to factor T over $\mathbb{F}_{27}$. Change the name of the variable of T so that the variable associated to the base field has lower priority than the variables of polynomials whose coefficients are taken in that base field (section on Variable priorities in the user's manual).
4. Factor T over the finite field $\mathbb{F}_3(t)/(T)$. *(see* `factorff`)
   Recall that $Gal(\mathbb{F}_{27}/\mathbb{F}_3)$ is cyclic of ordre 3 generated by the Frobenius homomorphism. The roots founded give the action of the powers of the Frobenius on t.

Exercise 3.

1. Compute a monic irreducible polynomial $P \in \mathbb{F}_5[w]$ defining $\mathbb{F}_{125}$ and give its lift in $\mathbb{Z}[w]$.
2. Is w a element of the field $\mathbb{F}_3[w]/(P)$? Compute a generator g of the field.
3. Express w^31 in terms of the basis elements 1 and w.
4. Confirm by comtuting the order of g. Is it a primitive root ?
5. Use `ffprimroot` to compute a primitive root.

2 p-adic Numbers

Exercise 4 (Operations on p-adic Numbers)**.**

A p-adic number has a unique representation in the form of a p-adic expansion. This representation defines it in PARI/GP. p-adic numbers are expressed as a series with a user-defined p-adic precision e.

1. The p-adic zero with precision e is given by `O(p^e)`. Try:

```
a=3+O(2^4)
type(a)
b=lift(a)
type(b)
```

2. Verify for some values of p and a precision of `e`=20 the identity $\frac{1}{1-p} = \sum_{n=0}^{\infty} p^n$.
3. The p-adic valuation is given by `valuation`. Try:

```
valuation(54,3)     valuation(1/512,2)      valuation(9!,3)     valuation(2748 + O(2^12))
```

4. The four arithmetic operations are well-defined for p-adic numbers.
   (a) Determine the 5-adic representations of 53 and -53. Verify that their sum equals 0 (in $\mathbb{Q}_5$).
   (b) What should be the 7-adic valuation of 7×123? Verify it.
   (c) Define 179 and 12 in $\mathbb{Q}_2$ with a precision `e`=15. Compute their quotient.
5. Compute the square root s of $a = 569$ in $\mathbb{Q}_7$ (`sqrt`). Verify the result by typing `s^2-a`.

Exercise 5 (Polynomial Factorization and Roots)**.**

1. Factorize the polynomial $X^4 - X$ in $\mathbb{Q}_p$ with four p-adic digits for $p = 5$ (`factorpadic`). Let F be the matrix returned by the software.
2. Using the function `eval`, deduce the four fourth roots of unity in $\mathbb{Q}_5$.
3. Retrieve these roots using `polrootspadic`.
4. Using `vecprod` and the matrix F, define the polynomial $X^4 - X$ in $\mathbb{Q}_5[X]$.
   (a) Retrieve its factorization with `factor`.
   (b) Determine the fourth root of unity in $\mathbb{Q}_5$ that is congruent to $3 \bmod 5$ using `padicappr`.