Polynomials, Galois extensions an finite fields

Marine Rougnant

19/02/2024 - 23/02/2024

1 Polynomials

Exercise 1.

- Implement a function `mycyclo(m)` constructing the cyclotomic polynomial $\Phi_m \in \mathbb{Z}[X]$ from the complex roots.
- Compare with `polcyclo`.

Exercise 2.
Write a command which prove the following :

$$\forall N \in \mathbb{N}, \Pi_{d|N}\Phi_d(X) = X^N - 1.$$

Exercise 3.
Consider the polynomial $pol = x^2 + 1$ and try :

```
factor(pol)
factor(pol *1.)
factor(pol * (1 + 0*I))
factor(pol * (1 + 0.*I))
factor(pol * Mod(1,2))
factor(pol * Mod(1, Mod(1,3)*(t^2+1)))
```

Exercise 4.

1. Prove that $x^3 - 2$ and $x^3 - 3$ are irreducible over $\mathbb{Q}(i)$.
2. Factorize $x^8 - x$ into irreducible polynomials over $\mathbb{F}_2$.

Exercise 5.
Consider le polynomial $f = x^5 + x^4 + 5x^3 + 3x^2 + 3x - 1$.

1. Is f irreducible ? If not, give its factorization.
2. Can you predict if f is irreducible over $\mathbb{Q}_2$? $\mathbb{Q}_5$?
3. Factorize f over $\mathbb{F}_3$. Check the result.
4. Write a Pari/GP command for checking the factorization over $\mathbb{F}_p$ of a given polynomial P and a given prime p.

2 Galois extensions

Exercise 6.

1. Check that $F = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a Galois extension of $\mathbb{Q}$ and $Gal(F/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.
2. (a) Find a polynomial defining $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (see `polcompositum`).

(b) Check that K is Galois, with $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) List all the subgroups of $Gal(K/\mathbb{Q})$.

(d) Give explicit generators of each of these subgroups.

Exercise 7. Consider $K = \mathbb{Q}({}^3\sqrt{2})$ and $L/\mathbb{Q}$ the Galois closure of $K/\mathbb{Q}$.

1. Compute the degree of the extension $L/\mathbb{Q}$ and give the structure of its Galois group. Is K Galois ?
   S_3 is group `GAP4(6,1)`
2. Find the polynomial defining L (see `galoisgetpol`)
3. Give the list of all the subfields of L.

Exercise 8.

Let ζ be a 8th-root of unity and $K = \mathbb{Q}(\zeta)$.

1. Define f, the minimal polynomial of ζ over $\mathbb{Q}$.
2. Compute $Gal(K/\mathbb{Q})$. Is it an abelian group ? Give its structure.
3. Denote by σ an τ its generators. Give their the explicit action on ζ (see `galoispermtopol`).
4. Compute the polynomial defining the fixed field of K by the subgroup generated by τ.
5. Show that over that subfield we have : $x^4 + 1 = (x^2 - \sqrt{-2}x - 1)(x^2 + \sqrt{-2}x - 1)$

Exercise 9.

Consider $K = \mathbb{Q}(\sqrt[3]{5}, \zeta_3)$.

1. Compute f, the irreducible polynomial defining K.
2. Compute $G = Gal(K/\mathbb{Q})$.
3. Compute the character table of G (see `galoischartable`), and for each character, give :
   - the corresponding conjugacy class (see `galoisconjclasses`),
   - the list of characteristic polynomials $det(1 - \rho(g)T)$, where g runs through representatives of the conjugacy classes (see `galoischarpoly`).

3 Finite fields

Exercise 10.

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 11.

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 $w^3 1$ 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.