



POLYNOMIALS & GALOIS EXTENSIONS

Marine Rognant

Université Marie & Louis Pasteur (Besançon, France)

Algebraic Days of Gabon

École Normale Supérieure (ENS), Libreville, Gabon

10/03/25 – 14/03/25



UNIVERSITÉ
MARIE & LOUIS
PASTEUR

Polynomials can be defined explicitly or by the vector of all coefficients (faster) :

```
? P = 1 + x^2 + 27*x^10
% = 27*x^10 + x^2 + 1
? Q = sum(i = 1, 10, (i+1) * x^i)
% = 11*x^10 + 10*x^9 + 9*x^8 + 8*x^7 + 7*x^6 + 6*x^5 + ...
? v=[1,2,3,4];
? T=Pol(v)
% = x^3 + 2*x^2 + 3*x + 4
? U=Polrev(v)
% = 4*x^3 + 3*x^2 + 2*x + 1
? polrecip(T)==U
% = 1
```

POLYNOMIALS

- ? $P=x^3 - 6*x^2 + 11*x - 6$;
? `polroots(P)`
% = [1.000 + 0.E-38*I, 2.000]
- Find a polynomial in $\mathbb{Z}[x]$ of degree at most k with x as an (approximate) root, x being real/complex or p -adic :
? $z = 2^{(1/6)}+3^{(1/5)}$;
? `algdep(z, 30)`
% = $2*x^{30} - 3*x^{29} - \dots - 2$
- Interpolate a polynomial through n points (x_i, y_i) :
? `a=[1,2,3];b=[4,0,2]`;
? `polinterpolate(a,b)`
% = $3*x^2 - 13*x + 14$
- Find a monic polynomial whose roots are the component of the vector a with multiplicities :
? `polfromroots(a)`
% = $x^3 - 6*x^2 + 11*x - 6$
- See also : `polhermite`, `pollaguerre`, `pollegendre`, `poltchebi`, ...

If you define a polynomial with several variables, then GP will choose the “main variable”. One ranking sequence is $x > y > z > w > u > v$.

```
f=3*x^2+x*y+4*y;
? polcoef(f,1)
% = y
? d=poldegree(f);d
% = 2
? pollead(f)==polcoef(f,d)
% = 1
? polcoef(f,1,y)
% = x + 4
? dy=poldegree(f,y);dy
% = 1
? pollead(f,y)==polcoef(f,d,y)
% = 0
```

POLYNOMIALS : FACTORISATION

Over \mathbb{Q} (or \mathbb{Z}) :

```
? f= x^5 + x^4 + 5*x^3 + 3*x^2 + 3*x - 1;
```

```
? factor(f)
```

```
% =
```

```
[ x^2 + x + 1 1]
```

```
[x^3 + 4*x - 1 1]
```

```
? pol = x^4 - 4*x^2 + 16
```

```
% = x^4 - 4*x^2 + 16
```

```
? polisirreducible(pol)
```

```
% = 1
```

```
? factor(pol)
```

```
% =
```

```
[x^4 - 4*x^2 + 16 1]
```

POLYNOMIALS : FACTORISATION

Over \mathbb{Q}_p , to p -adic precision 10 :

```
? factor(poldisc(pol))
```

```
% =
```

```
[2 16]
```

```
[3 2]
```

```
? factorpadic(pol, 3, 10)
```

```
% =
```

```
[(1 + 0(3^10))*x^4 + .... + (1 + 2*3 + 3^2 + 0(3^10)) 1]
```

```
? factorpadic(pol, 5, 10)
```

```
% =
```

```
[(1+0(5^10))*x^2 + (4+...+0(5^10))*x + (1+4*5+...+0(5^10)) 1]
```

```
[(1+0(5^10))*x^2 + (1+... +0(5^10))*x + (1+4*5+...+0(5^10)) 1]
```

Over \mathbb{F}_p :

```
? factormod(pol,2)
```

```
% =
```

```
[Mod(1, 2)*x 4]
```

```
? factormod(pol,5)
```

```
% =
```

```
[Mod(1, 5)*x^2 + Mod(1, 5)*x + Mod(1, 5) 1]
```

```
[Mod(1, 5)*x^2 + Mod(4, 5)*x + Mod(1, 5) 1]
```

```
? lift(%)
```

```
% =
```

```
[ x^2 + x + 1 1]
```

```
[x^2 + 4*x + 1 1]
```

Over a number field :

Number fields are defined as $K = \mathbb{Q}[t]/f(t)$ where f is an irreducible polynomial, $f(\alpha) = 0$.

```
? pol2=x^4 - 4*x^2 + 16
% = x^4 - 4*x^2 + 16
? factornf(pol2, t^2 + 1)
% =
[x^2 + Mod(-2*t, t^2 + 1)*x - 4 1]
```

```
[ x^2 + Mod(2*t, t^2 + 1)*x - 4 1]
? lift(%)
% =
[x^2 - 2*t*x - 4 1]
```

```
[x^2 + 2*t*x - 4 1]
```

In $\mathbb{Q}[i]$, $pol2 = (x^2 - 2ix - 4)(x^2 + 2ix - 4)$.

Simple operations can be made in K with Mod :

```
? g = polcyclo(30) \\
% = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1
? Mod(x,f)^5
%27 = Mod(3*x^3 - 2*x^2 + 5*x + 10, x^4 - 2*x^3 + x^2 - 5)
```

$$\alpha^5 = 3\alpha^3 - 2\alpha^2 + 5\alpha + 10$$

The roots of g are 30th roots of unity :

```
? lift(Mod(x,g)^15)
% = -1
```

Sometimes we may want to find a defining polynomial simpler for the same number field :

```
? {h = x^5 + 7*x^4 + 22550*x^3 - 281686*x^2 - 85911*x + 3821551};
? polredbest(h)
% = x^5 - x^3 - 2*x^2 + 1
```

$$\mathbb{Q}[x]/h(x) \cong \mathbb{Q}[x]/(x^5 - x^3 - 2x^2 + 1)$$

Consider a number field K defined by a polynomial f .

- Galois group of the splitting field of $f(x)$ over \mathbb{Q} :

```
? T=(x^2-1)^3-2; polgalois(T)
```

```
% = [48, -1, 1, "2S_4(6) = [2^3]S(3) = 2 wr S(3)"]
```

```
? P= x^8-7*x^6+14*x^4-8*x^2+1
```

```
% = x^8 - 7*x^6 + 14*x^4 - 8*x^2 + 1
```

```
? polgalois(P)
```

```
% = [8, 1, 2, "4[x]2"]
```

$\mathbb{Q}[x]/T(x)$ is not Galois. Its splitting field has Galois group of order 48 ($S_4 \times \mathbb{Z}/2\mathbb{Z}$).

$\mathbb{Q}[x]/P(x)$ is Galois of Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If P defines a Galois extension of \mathbb{Q} , then use `galoisinit` to compute its Galois group :

```
? gal=galoisinit(P);
```

If T defines a non-Galois extension of \mathbb{Q} , then use `galoissplittinginit` to compute the Galois group of the splitting field :

```
? gal2=galoissplittinginit(T);  
? poldegree(gal2.pol)  
% = 48
```

```
? gal=galoisinit(P);
? gal.pol \\ P
% = x^8 - 7*x^6 + 14*x^4 - 8*x^2 + 1
? gal.roots \\ p-adic roots of pol as integers implicitly
                modulo gal.mod
% = [98914554976133331819135, 5527858468618611375478, ...]~
? gal.group \\ Galois group G expressed as a vector of
                permutations of gal.roots
% = [Vecsmall([1,2,3,4,5,6,7,8]),Vecsmall([3,1,5,7,2,4,8,6]),...]
? gal.gen \\ generating subset of G expressed as a vector
                of permutations of gal.roots
% = [Vecsmall([3,1,5,7,2,4,8,6]),Vecsmall([4,6,7,1,8,2,3,5])]
```

Let gal be a galoisinit output :

- all subgroups of gal :

```
? L = galoissubgroups(gal);
? vector(#L, i, galoisisabelian(L[i],1))
% = [1, 1, 1, 1, 1, 1, 1, 1]
? vector(#L, i, galoisidentify(L[i])) \\ GAP4 Small Group 1
% = [[8, 2], [4, 1], [4, 2], [4, 1], [2, 1], [2, 1], [2, 1],
? [a,b]=%[1]; galoisgetname(a,b) \\ GAP4(8,2)="C4 x C2"
% = "C4 x C2"
```

Let gal be a galoisinit output :

- field fixed by a given subgroup :

```
? galoisfixedfield(gal,L[1])  
% = [x, Mod(0, x^8 - 7*x^6 + 14*x^4 - 8*x^2 + 1)]  
? galoisfixedfield(gal,L[2])  
% = [x^2 - 15, Mod(4*x^7 - 27*x^5 + ... + 1)]
```

The subfield of K fixed by gal is \mathbb{Q} .

- all subfields of K :

```
? galoissubfields(gal);  
? vector(#%, i, %[i][1])  
% = [x, x^2 - 15, x^2 - 14*x + 44, x^2 - 3,  
      x^4 - 9*x^2 + 9, x^4 - 5*x^2 + 5,  
      x^4 - 14*x^3 + 56*x^2 - 64*x + 16,  
      x^8 - 7*x^6 + 14*x^4 - 8*x^2 + 1]
```