CORPS FINIS SOUS PARI/GP

BILL ALLOMBERT

Soit p un nombre premier et $n > 0$ un entier. On identifie le corps fini $\mathbb{F}_{p^n}$ avec le corps $\mathbb{F}_p[T]/(P)$ où P est un polynôme irréductible de $\mathbb{F}_p[X]$ de degré n.

PARI/GP permet de déterminer un tel polynôme avec la commande `P=ffinit(p,n)`.

```
? ffinit(2,2)
%1 = Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2)
? ffinit(2,8)
%2 = Mod(1, 2)*x^8 + Mod(1, 2)*x^6 + Mod(1, 2)*x^5 + Mod(1, 2)*x^4 + Mod(1, 2)*x^3
+ Mod(1, 2)*x + Mod(1, 2)
? ffinit(17,5)
%3 = Mod(1, 17)*x^5 + Mod(1, 17)*x^4 + Mod(13, 17)*x^3 + Mod(14, 17)*x^2
+ Mod(3, 17)*x + Mod(1, 17)
```

Nous contruisons un générateur a du corps fini à partir de P avec la commande `a=Mod('a*Mod(1,p),subst(P,x,'a))`. Nous exprimons les autres éléments comme polynômes en a.

```
? P=ffinit(2,4);
? a=Mod('a*Mod(1,2),subst(P,x,'a));
? b=a^3+a+1;
? c=a^2+1;
? b*c
%5 = Mod(Mod(1, 2)*a^2 + Mod(1, 2)*a, Mod(1, 2)*a^4 + Mod(1, 2)*a^3 + Mod(1, 2)*a^2
+ Mod(1, 2)*a + Mod(1, 2))
? lift(lift(b*c))
%6 = a^2 + a
```

Ici, la commande `lift(lift())` permet de supprimer les modulos pour l'affichage.

```
? P=ffinit(2,4);
? a=Mod('a*Mod(1,2),subst(P,x,'a));
? M=[a,a^2+a;a+1,a^3+1];
? lift(lift(matdet(M)))
%6 = a^2 + a + 1
```