Licence STS Mention MATH L3 - ATN
Anneaux

1 Anneaux de polynômes univariés

Pour utiliser des polynômes, il faut tout d'abord définir :

1. l'anneau ou corps de base (ZZ l'anneau $\mathbb{Z}$, QQ le corps $\mathbb{Q}$, $GF(p)$ le corps fini $\mathbb{F}_p$ sont prédéfinis)
2. l' (ou les) indéterminée(s)

```
sage: X = polygen(ZZ,'X')
sage: f = 6*X^4 - 3*X^3 + 6*X^2 + 7*X - 5
sage: f
6*X^4 - 3*X^3 + 6*X^2 + 7*X - 5
sage: parent(f)
Univariate Polynomial Ring in X over Integer Ring
sage: (U,V) = polygens(GF(5),'U,V')
sage: F = (U + V)^10
sage: F
U^10 + 2*U^5*V^5 + V^10
sage: parent(F)
Multivariate Polynomial Ring in U, V over Finite Field of size 5
sage: phi = F.polynomial(U)
sage: parent(phi)
Univariate Polynomial Ring in U over
Univariate Polynomial Ring in V over Finite Field of size 5
```

On peut aussi définir globalement des anneaux de polynômes :

```
sage: A = PolynomialRing(ZZ,'X')
sage: A
Univariate Polynomial Ring in X over Integer Ring
sage: X = A.gen()
sage: A.base_ring()
Integer Ring
sage: R = A.base_extend(QQ)
sage: R
Univariate Polynomial Ring in X over Rational Field
sage: R.base_ring()
Rational Field
```

les commandes $A.<tab>$ et $f.<tab>$ donnent la liste des attributs et des méthodes qui s'appliquent à A et f. Voici quelques exemples :

```
sage: f.args()
(X,)
sage: f(X=5)
3555
sage: f.base_ring()
Integer Ring
sage: f.coefficients()
[-5, 7, 6, -3, 6]
sage: f.exponents()
[0, 1, 2, 3, 4]
sage: sum(c*X^e for (c,e) in zip(f.coefficients(),f.exponents()))
6*X^4 - 3*X^3 + 6*X^2 + 7*X - 5
sage: f.degree()
4
sage: f.leading_coefficient()
6
sage: f.constant_coefficient()
-5
sage: f.valuation()
0
sage: f.content()
1
```

On peut calculer dérivées et primitives de polynômes :

```
sage: f.derivative()
24*X^3 - 9*X^2 + 12*X + 7
sage: g = f.integral()
sage: g
6/5*X^5 - 3/4*X^4 + 2*X^3 + 7/2*X^2 - 5*X
sage: g in R
True
```

Les fonctions prennent en compte l'anneau de base du polynôme auquel on les applique :

```
sage: f.is_irreducible()
False
sage: f.factor()
(2*X - 1) * (3*X^3 + 3*X + 5)
sage: fQ = f.base_extend(QQ)
6*X^4 - 3*X^3 + 6*X^2 + 7*X - 5
sage: fQ.factor()
(6) * (X - 1/2) * (X^3 + X + 5/3)
sage: R(f)
6*X^4 - 3*X^3 + 6*X^2 + 7*X - 5
sage: R(f).base_ring()
Rational Field
sage: R(f).factor()
(6) * (X - 1/2) * (X^3 + X + 5/3)
```

Pour les polynômes à coefficients dans un corps on dispose de la division euclidienne, du pcdg et de la formule de Bezout :

```
sage: f = X^3+4*X^2+4*X+3
sage: f
X^3 + 4*X^2 + 4*X + 3
sage: g = X^3+5*X^2+8*X+6
sage: g
X^3 + 5*X^2 + 8*X + 6
sage: gcd(f,g)
X + 3
sage: rm = f.mod(g)
sage: rm
-X^2 - 4*X - 3
sage: (q,r) = f.quo_rem(g)
sage: q,r
(1, -X^2 - 4*X - 3)
sage: d,u,v = xgcd(f,g)
sage: d,u,v
(X + 3, X + 1, -X)
sage: d == u*f + v*g
True
```

2 Corps des fractions

On peut construire le corps des fractions d'un anneau intègre :

```
sage: A = PolynomialRing(QQ,'X')
sage: X = A.gen()
sage: K = FractionField(A)
sage: K
Fraction Field of Univariate Polynomial Ring in X over Rational Field
```

et calculer sur ses éléments :

```
sage: P = X^2 + 3*X + 2
sage: Q = X^4 - X^3 + X^2 - 3*X - 6
sage: P/Q
(X + 2)/(X^3 - 2*X^2 + 3*X - 6)
sage: from sage.rings.fraction_field_element import FractionFieldElement
sage: R = FractionFieldElement(K,P,Q,reduce=False)
sage: R
(X^2 + 3*X + 2)/(X^4 - X^3 + X^2 - 3*X - 6)
sage: R.reduce()
sage: R.numerator(),R.denominator()
(X + 2, X^3 - 2*X^2 + 3*X - 6)
sage: R.partial_fraction_decomposition()
(0, [4/7/(X - 2), (-4/7*X - 1/7)/(X^2 + 3)])
```

3 Anneaux quotients

On peut calculer dans les anneaux quotients d'un anneau de polynômes univariés $A[X]$.

```
sage: A = PolynomialRing(ZZ,'X')
sage: X = A.gen()
sage: Q = A.quotient(X^2+1,'x')
sage: x = Q.gen()
sage: x^2
-1
sage: Q.characteristic()
0
sage: Q.degree()
2
sage: Q.discriminant()
-4
sage: Q.is_integral_domain()
True
sage: Q.is_field()
False
sage: y = x^5+2*x^3+1
sage: y
-x + 1
sage: y.norm()
2
sage: y.trace()
2
sage: y.charpoly('T')
T^2 - 2*T + 2
```

4 Exercices

Exercice 1.
Montrer que le polynôme $X^4 + 11X^3 + 42X^2 + 65X + 37$ est irréductible dans $\mathbb{Z}[X]$.
Former la liste des 20 premiers *entiers premiers* p pour lesquels $\overline{f}$ est irréductible dans $\mathbb{Z}/\mathbb{Z}p$.

Exercice 2.
Factoriser dans $\mathbb{F}_{13}$ le polynôme cyclotomique Φ_{15}. (`cyclotomic_polynomial()` construit les polynômes cyclotomiques)

Exercice 3.
Calculer le pgcd et les coefficients de la formule de Bezout des polynômes

$$f = 2X^8 + X^6 - 3/2X^4 - 3X^3 + 8X^2 + 2X - 5 \qquad g = 3X^6 + 5/4X^4 - 4X^2 - 9X + 21$$

Exercice 4.
Déterminer l'idéal de $\mathbb{Q}[X]$ engendré par les polynômes

$$f = X^3 + 3X^2 + 4X + 2 \qquad g = X^4 + 2X^3 + 3X^2 + 2X + 2$$

Exercice 5.
On considère le polynôme $f = X^4 + 3X^3 + 6X^2 + 3X + 1$.

1. Vérifier que f est un polynôme primitif irréductible de $\mathbb{Z}[X]$.
2. Vérifier que f est un polynôme *réciproque* (*i.e.* que $f = f_{\text{rec}}$ avec $f_{\text{rec}} = X^{\deg(f)} f(\frac{1}{X})$).

Exercice 6. On considère le polynôme

$$f = (t+1)\,X^4 + \left(t^4 - t^2 + t + 1\right) X^3 + \left(t^3 + 1\right) X^2 + \left(t^4 - t^2 + t + 1\right) X + t + 1$$

dans l'anneau $A[X]$ où $A = \mathbb{Z}[t]$.

1. Calculer le contenu c et la partie primitive p de f.
2. Vérifier que f est un polynôme réciproque dans $A[X]$.
3. Montrer que p est irréductible dans $A[X]$ (justifier le calcul effectué avec SAGE)

Exercice 7.
Soit $K = \mathbb{Q}(X)$ le corps des fractions rationnelles en une indéterminée X à coefficients dans $\mathbb{Q}$.

1. Construire la suite de polynômes $(T_j)_{0 \le j \le d-1}$ de $K[Y]$:
   a) $T_0 = Y$
   b) T_1 est le reste de la division euclidienne dans $K[Y]$ de $-U\dfrac{\partial P}{\partial X}$ par P où U et V sont les coefficients de la formule de Bezout $U\dfrac{\partial P}{\partial Y} + VP = 1$.
   c) T_j est le reste de la division euclidienne dans $K[Y]$ de $\dfrac{\partial T_{j-1}}{\partial X} + T_1 \dfrac{\partial T_{j-1}}{\partial Y}$ par P pour $2 \le j \le d-1$,
2. Former la matrice M, carrée d'ordre d dont les colonnes sont les coefficients des polynômes T_j ($M = (c_{i,j})_{0 \le i,j \le d-1}$ avec $T_j = \sum_{i=0}^{d-1} c_{i,j} Y^i$).
3. Calculer des éléments $K_j \in K$, $1 \le j \le d$, tels que l'on ait une combinaison linéaire *non triviale* $\sum_{j=1}^{d} K_j T_{j-1} = 0$.
4. Former l'équation différentielle $\sum_{j=1}^{d} K_j \dfrac{d^{j-1} f(X)}{dX^j}$ et vérifier que ϕ est une solution où $P(X, \phi) = 0$.