TD1

September 29, 2019

0.1 Introduction rapide à Jupyter

Utilisation comme calculatrice

```
In [11]: 2+5
```

```
Out[11]: 7
```

```
In [12]: 1932 % 3
```

```
Out[12]: 0
```

On peut écrire du texte stylisé.
Ce texte est en italics.
Ce texte est en gras
On peut écrire du *latex*.
$\sum_{i=0}^{n} x^i$

0.2 Quelques rappels de Sage

Sage est un langage de programmation mathématique qui est basé sur Python.

On peut manipuler des entiers, des chaînes de caractères, des listes mais surtout des objects mathématiques plus complèxes.

```
In [13]: if 4 % 2 == 0 :
             print '4 est pair'
```

```
4 est pair
```

Une caractèristique particulière de Sage est qu'une variable n'est pas typée et son type peut changer en cours d'execution sans besoin de définir son type.

```
In [14]: a = 5
         print a
         type(a)
```

```
5
```

```
Out[14]: <type 'sage.rings.integer.Integer'>

In [15]: a = [3,5,1]
         print a
         type(a)

[3, 5, 1]


Out[15]: <type 'list'>

In [16]: a = (5 == 3)
         type(a)

Out[16]: <type 'bool'>
```

On va travailler avec des structures de données

```
In [17]: RR

Out[17]: Real Field with 53 bits of precision

In [18]: QQ

Out[18]: Rational Field

In [19]: ZZ

Out[19]: Integer Ring

In [20]: GF(2)

Out[20]: Finite Field of size 2

In [21]: Zmod(13)

Out[21]: Ring of integers modulo 13
```

On peut tester l'appartenance à un ensemble

```
In [22]: 2 in ZZ

Out[22]: True

In [23]: 1/2 in ZZ

Out[23]: False

In [24]: 1/2 in QQ

Out[24]: True
```

La variable x est une variable symbolique prédéfinie dans le *Symbolic Ring*.

```
In [25]: x

Out[25]: x

In [26]: x.parent()

Out[26]: Symbolic Ring

In [27]: y



        NameErrorTraceback (most recent call last)

        <ipython-input-27-9063a9f0e032> in <module>()
    ----> 1 y


        NameError: name 'y' is not defined
```

Si on le souhaite on peut définir y ou une autre variable symbolique avec la fonction **var**.

```
In [28]: var('y')

Out[28]: y

In [29]: (x+y)*(x-y)

Out[29]: (x + y)*(x - y)
```

Polynômes

À la place de travailler avec les polynômes symboliques, il est mieux de travailler directement avec les classes spécialisés de polynômes en Sage et profiter de toutes les fonctionnalités de traîtement de polynômes.

Il existe plusieurs façons pour définir un anneau de polynômes à variables dans un corps.

```
In [30]: A.<x> = QQ[]

In [31]: A

Out[31]: Univariate Polynomial Ring in x over Rational Field
```

De cette façon x est directement associé au générateur de A. Il existe d'autres façons de faire la même chose.

```
In [32]: A = QQ['x']
         x = A.gen()
```

```
In [33]: A.<x> = PolynomialRing(QQ)

In [34]: A

Out[34]: Univariate Polynomial Ring in x over Rational Field
```

En travaillant dans une classe spécialisée de polynômes, on ne fait plus de calculs symboliques. Tout calcul est effectué immédiatement.

```
In [35]: (x^2 + 1)*(x^4 + 3*x^2 + 2)

Out[35]: x^6 + 4*x^4 + 5*x^2 + 2
```

Affichage latex

```
In [36]: P = x^6 + 5*x^3 + 1

In [37]: P

Out[37]: x^6 + 5*x^3 + 1

In [38]: %display latex

In [39]: P

Out[39]: x^6 + 5*x^3 + 1

In [40]: %display plain

In [41]: P

Out[41]: x^6 + 5*x^3 + 1
```

0.2.1 Exercice 1.1

```
In [42]: A.<x> = QQ[]

In [44]: P1 = x^6 + 2*x^5 - 2*x^4 + 2*x^2 - 2*x - 1
         P2 = x^5 + x^4 - 2*x^3 + x^2 + x - 2

In [45]: P = P1*P2

In [46]: %display latex

In [47]: P

Out[47]: x^11 + 3*x^10 - 2*x^9 - 5*x^8 + 9*x^7 - 2*x^6 - 13*x^5 + 9*x^4 + 2*x^3 - 7*x^2 + 3*x

In [48]: %display plain

In [49]: P.degree()
```

```
Out[49]: 11

In [50]: P.leading_coefficient()

Out[50]: 1

In [51]: P.list()

Out[51]: [2, 3, -7, 2, 9, -13, -2, 9, -5, -2, 3, 1]

In [52]: P1 // P2

Out[52]: x + 1

In [53]: P1 % P2

Out[53]: -x^4 + x^3 - x + 1
```

On peut effectuer ces deux étapes en une.

```
In [54]: P1.quo_rem(P2)

Out[54]: (x + 1, -x^4 + x^3 - x + 1)

In [55]: Q = gcd(P1,P2)

In [56]: Q

Out[56]: x^4 - x^3 + x - 1

In [57]: P1.gcd(P2)

Out[57]: x^4 - x^3 + x - 1

In [58]: P.factor()

Out[58]: (x + 2) * (x - 1)^2 * (x + 1)^2 * (x^2 + 3*x + 1) * (x^2 - x + 1)^2

In [59]: P(2)

Out[59]: 3564
```

0.2.2 Exercice 1.2

```
In [61]: A.<x> = ZZ[]

In [62]: A

Out[62]: Univariate Polynomial Ring in x over Integer Ring

In [63]: P = x^11 + x^10 + x^9 + 2*x^8 + 2*x^6 + 2*x^4 + x^3 + x^2 + x
```

```
In [64]: P.parent()
Out[64]: Univariate Polynomial Ring in x over Integer Ring
In [65]: P.factor()
Out[65]: x * (x^2 + 1) * (x^2 + x + 1) * (x^6 - x^4 + 2*x^3 - x^2 + 1)
In [66]: B.<x> = ZZ[i][]
In [67]: B
Out[67]: Univariate Polynomial Ring in x over Order in Number Field in I with defining polynom
In [68]: P1 = B(P)
In [69]: P1.parent()
Out[69]: Univariate Polynomial Ring in x over Order in Number Field in I with defining polynom
In [70]: P1.factor()



        NotImplementedErrorTraceback (most recent call last)

        <ipython-input-70-f8a86c9bd1b7> in <module>()
    ----> 1 P1.factor()


        sage/rings/polynomial/polynomial_element.pyx in sage.rings.polynomial.polynomial_elemen


        sage/rings/ring.pyx in sage.rings.ring.Ring.is_finite (build/cythonized/sage/rings/ring


        NotImplementedError:
```

Cette fonctionnalité n'est pas implementée pour l'anneau $\mathbb{ZZ}[i]$.

```
In [71]: P2 = P.change_ring(QQ[i])
In [72]: P2.parent()
Out[72]: Univariate Polynomial Ring in x over Number Field in I with defining polynomial x^2 +
In [73]: P2.factor()
Out[73]: (x - I) * x * (x + I) * (x^2 + x + 1) * (x^6 - x^4 + 2*x^3 - x^2 + 1)
In [74]: P.change_ring(GF(2)).factor()
Out[74]: x * (x + 1)^8 * (x^2 + x + 1)
In [75]: P.change_ring(GF(4)).factor()
Out[75]: x * (x + z2) * (x + z2 + 1) * (x + 1)^8
```

0.2.3 Exercice 1.3

```
In [76]: A.<x> = QQ[]
         P = x^7 + x^5 + 2*x^3 + 2*x^2 + 3*x + 2

In [77]: P.change_ring(GF(2)).factor()

Out[77]: x * (x^3 + x^2 + 1)^2

In [78]: P.change_ring(GF(7)).factor()

Out[78]: (x + 4) * (x^6 + 3*x^5 + 3*x^4 + 2*x^3 + x^2 + 5*x + 4)
```

On suppose que P n'est pas irréductible, alors $P = fh$ avec $1 \leq \deg(f), \deg(h) \leq 6$. Soit $\tilde{P}$ le polynôme P dans $\mathbb{F}_2$ et $\bar{P}$ le polynôme P dans $\mathbb{F}_7$.

$$\tilde{P} = \tilde{f}\tilde{h} = x(x^3 + x^2 + 1)^2 \tag{1}$$
$$\bar{P} = \bar{f}\bar{h} = (x - 3)Q. \tag{2}$$

Donc soit P est irréductible soit il a une racine $r \equiv 10 \mod 14$ (puisque P a une racine $r \equiv 0 \mod 2$ et $r \equiv 4 \mod 7$ et on utilise le théorème des restes chinois). Mais

$$P(r) = 0 \tag{3}$$
$$\Leftrightarrow r^7 + r^5 + 2r^3 + 2r^2 + 3r + 2 = 0 \tag{4}$$
$$\Leftrightarrow r(r^6 + r^4 + 2r^2 + 2r + 3) = -2 \tag{5}$$

De la dernière équation r doit diviser -2, ce qui implique que $r = \pm 1, \pm 2$ ce qui est impossible car toutes ces valeurs ne sont pas congrues à 10 modulo 14. On conclue alors que P est irréductible dans $\mathbb{Z}[x]$.

On vérifie que P est en effet irréductible.

```
In [79]: P.is_irreducible()

Out[79]: True
```

0.2.4 Exercice 1.4

```
In [80]: p = 2
         k = GF(p)
         A.<x> = k[]

In [81]: for c in k :
             g = x^p - x + c
             print g.factor()

x * (x + 1)
x^2 + x + 1
```

On regarde ce qu'il se passe pour d'autres valeurs de p.

```
In [82]: for p in [3,5,7] :
             print "p = ", p
             k = GF(p)
             A.<x> = k[]
             for c in k :
                 g = x^p - x + c
                 print g.factor()
             print " "
```

```
p =  3
x * (x + 1) * (x + 2)
x^3 + 2*x + 1
x^3 + 2*x + 2

p =  5
x * (x + 1) * (x + 2) * (x + 3) * (x + 4)
x^5 + 4*x + 1
x^5 + 4*x + 2
x^5 + 4*x + 3
x^5 + 4*x + 4

p =  7
x * (x + 1) * (x + 2) * (x + 3) * (x + 4) * (x + 5) * (x + 6)
x^7 + 6*x + 1
x^7 + 6*x + 2
x^7 + 6*x + 3
x^7 + 6*x + 4
x^7 + 6*x + 5
x^7 + 6*x + 6
```

On conjecture que $P = x^p - x + c$ est scindé pour $c = 0$ (décomposable en facteurs de degré 1 sur $\mathbb{F}_p[x]$) et irréductible pour $c \neq 0$. Nous allons maintenant démontrer ces deux conjectures.

Cas $c = 0$ Dans ce cas on a que $P = x^p - x$. Par le Petit Théorème de Fermat on a que $a^p \equiv a$ pour tout $a \in \mathbb{F}_p$. Par conséquent tout a est une racine et donc P s'écrit comme

$$P(x) = x(x-1)(x-2)\cdots(x-(p-1)).$$

Cas $c \neq 0$ Soit a une racine de $P = x^p - x + c$ et soit $a_i = a + i$ pour tout $0 \leq i < p$. On a

$$\begin{aligned}
P(a_i) &= a_i^p - a_i + c && (6)\\
&= (a+i)^p - (a+i) + c && (7)\\
&= a^p + i^p - a - i + c, \text{ (car en } \mathbb{F}_p, (a+b)^p = a^p + b^p) && (8)\\
&= (a^p - a + c) + (i^p + i) && (9)\\
&= a^p - a + c \text{ (par le Petit Théorème de Fermat) .} && (10)\\
&= 0 \text{ (car } a \text{ racine).} && (11)
\end{aligned}$$

Donc $a, a+1, \ldots, a+(p-1)$ sont toutes racines de P dans $\mathbb{F}_p$. On a p racines, par conséquent, tout élément de $\mathbb{F}_p$ est une racine de P et donc 0 est une racine de P. Ceci implique que $0^p - 0 + c \equiv 0 \mod p$ et que donc $c = 0$. On conclue que dans ce cas P n'a pas de racines dans $\mathbb{F}_p$. Cependant comme le degré de P est supérieur à 3 on ne peut pas directement conclure qu'il est irréductible.

On suppose que P n'est pas irréductible, donc $P = gh$ avec $deg(h) = k$ et $1 \leq k < p-1$. Soit $\{r_1, \ldots, r_k\}$ les racines de g qui n'appartiennent pas forcément dans $\mathbb{F}_p$.

Le polynôme g est de la forme :

$$g = x^k + a_{k-1}x^{k-1} + \cdots + a_1x_1 + a_0, \text{ avec } a_i \in \mathbb{F}_p.$$

Par la formule de Vieta on a que $-a_{k-1} = r_1 + \cdots + r_k$. Puisque $\{r_1, \ldots, r_k\}$ sont des racines de g elles sont forcément des racines de P. On a montré avant que si a est une racine de P alors $a+i$ l'est également pour tout i. Donc on a la correspondance $r_1 = r, r_2 = r + b_1, \ldots, r_k = r + b_{k-1}$ pour certains b_i dans $\mathbb{F}_p$. On a maintenant que

$$\begin{aligned} r_1 + \cdots + r_k &= kr + (b_1 + \cdots + b_{k-1}) && (12) \\ &= -a_{k-1}. && (13) \end{aligned}$$

Comme $a_{k-1}, (b_1 + \cdots + b_{k-1}) \in \mathbb{F}_p$ on obtient que $kr = \alpha \in \mathbb{F}_p$. Maintenant $k \in \{1, \ldots, p-1\}$ et comme $k \neq 0 \mod p$, il existe k^{-1}. Donc $r = k^{-1}\alpha \in \mathbb{F}_p$.

On vient de montrer que P a une racine dans $\mathbb{F}_p$. Absurde. Alors P irréductible.

0.2.5 Exercice 1.5

```
In [83]: P = cyclotomic_polynomial(1)

In [84]: P

Out[84]: x - 1

In [85]: for i in range(1,30) :
             print "i = ", i, ": ",
             P = cyclotomic_polynomial(i)
             print P

i =  1 :  x - 1
i =  2 :  x + 1
i =  3 :  x^2 + x + 1
i =  4 :  x^2 + 1
i =  5 :  x^4 + x^3 + x^2 + x + 1
i =  6 :  x^2 - x + 1
i =  7 :  x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
i =  8 :  x^4 + 1
i =  9 :  x^6 + x^3 + 1
i =  10 :  x^4 - x^3 + x^2 - x + 1
i =  11 :  x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
i =  12 :  x^4 - x^2 + 1
i =  13 :  x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
i =  14 :  x^6 - x^5 + x^4 - x^3 + x^2 - x + 1
```

```
i =  15 :  x^8 - x^7 + x^5 - x^4 + x^3 - x + 1
i =  16 :  x^8 + 1
i =  17 :  x^16 + x^15 + x^14 + x^13 + x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 +
i =  18 :  x^6 - x^3 + 1
i =  19 :  x^18 + x^17 + x^16 + x^15 + x^14 + x^13 + x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^
i =  20 :  x^8 - x^6 + x^4 - x^2 + 1
i =  21 :  x^12 - x^11 + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1
i =  22 :  x^10 - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1
i =  23 :  x^22 + x^21 + x^20 + x^19 + x^18 + x^17 + x^16 + x^15 + x^14 + x^13 + x^12 + x^11 +
i =  24 :  x^8 - x^4 + 1
i =  25 :  x^20 + x^15 + x^10 + x^5 + 1
i =  26 :  x^12 - x^11 + x^10 - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1
i =  27 :  x^18 + x^9 + 1
i =  28 :  x^12 - x^10 + x^8 - x^6 + x^4 - x^2 + 1
i =  29 :  x^28 + x^27 + x^26 + x^25 + x^24 + x^23 + x^22 + x^21 + x^20 + x^19 + x^18 + x^17 +
```

Pour rappel, tout polynôme cyclotomique est irréductible.

```
In [86]: A.<x> = ZZ[]

In [87]: for p in [2,3,5,7] :
             print "p = ", p
             h = x^(2*p) + x^p + 1
             print h.factor()

p =  2
(x^2 - x + 1) * (x^2 + x + 1)
p =  3
x^6 + x^3 + 1
p =  5
(x^2 + x + 1) * (x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)
p =  7
(x^2 + x + 1) * (x^12 - x^11 + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1)
```

Cas 1 : $p = 2 : P = x^4 + x^2 + 1 = \Phi(3)\Phi(6)$ produit de polynômes irréductibles.
Cas 2 : $p = 3 : P = x^6 + x^3 + 1 = \Phi(9)$ irréductible.

Cas 3 : $p > 3$: On calcule

$$\Phi_{3p}(x)\Phi_3(x) = \frac{x^{3p}-1}{\prod_{d|3p, d\neq 3p}\Phi_d(x)}\Phi_3(x) \tag{14}$$

$$= \frac{x^{3p}-1}{\Phi_1(x)\Phi_3(x)\Phi_p(x)}\Phi_3(x) \tag{15}$$

$$= \frac{x^{3p}-1}{\Phi_1(x)\Phi_p(x)} \tag{16}$$

$$= \frac{x^{3p}-1}{\Phi_1(x)\frac{x^p-1}{\Phi_1(x)}} = \frac{(x^p)^3-1^3}{x^p-1} \tag{17}$$

$$= \frac{(x^p-1)((x^p)^2+x^p+1)}{x^p-1} \tag{18}$$

$$= x^{2p}+x^p+1. \tag{19}$$

On conclue alors que

$$x^{2p}+x^p+1 = \Phi_{3p}(x)\Phi_3(x).$$