Faculté des Sciences
Aix*Marseille Université

Master de mathématiques, 1re année

Quatrième TP

vendredi 7 décembre 2015
B. Cadorel, T. Coulbois

Polynômes

1 Domaines de calcul

1. Comment expliquez-vous la différence entre
```
sage: var('x')
sage: p=(x-2)*(x+3)
sage: p
```
et
```
sage: x=QQ['x'].gen()
sage: p=(x-2)(x+3)
sage: p
```
?

Vous pouvez par exemple utiliser `x.parent(), p.parent()`. Comment représenter un polynôme dans un ordinateur ? Qu'est-ce qu'une forme normale ?

2. Pour $n = 1, \dots, 20$ donnez les facteurs irréductibles (sur $\mathbb{Q}$) des polynômes $\Phi_n(X) = X^n - 1$. `p.factor()`

3. Vérifier que les racines de $X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ sont les racines primitives 15^{e} de l'unité `p.roots(QQbar)`.

4. Comparer
```
sage: var('x')
sage: p=x^3-6x^2+9x-1
sage: solve(p,x)
```
et
```
sage: x=QQ['x'].gen()
sage: p=x^3-6x^2+9x-1
sage: rts=p.roots(QQbar)
sage: x0=rts[0][0]
sage: x0.radical_expression()
```
.

5. Donner le discrimant du polynôme $ax^3 + bx^2 + cx + d$. Sous quelle forme connait-on en général le discriminant des polynômes de degré 3 ?

Pour répondre à la question précédente, vous devrez réfléchir à ce qu'est un discrimant et au domaine de calcul que vous devez indiquer à Sage. La réflexion sur le domaine de calcul est importante pour la suite de ce TP.

2 Corps de nombres

```
QQ[sqrt(3)], NumberField(x^2-3,'xbar'), F.quotient(x^2-3), x.minpoly(),
F.primitive_element()
```

6. Définir le corps de nombre $\mathbb{Q}[\sqrt{2}]$ (en mathématiques et dans Sage). Caculer $\frac{1}{3-\sqrt{2}}$.

7. Donner le polynôme minimal (sur $\mathbb{Q}$) de $\sqrt{2} + \sqrt{3}$.

8. Définir le corps $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

9. Montrer que $\sqrt{2} + \sqrt{3}$ est un élément primitif de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

10. Donner un élément primitif de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

11. Donner le polynôme minimal de $5^{1/7}.3^{1/5} + 2^{1/3}$

12. Définir $L = \mathbb{Q}[x]/x^3 - 6x^2 + 9x - 1$. Vérifier que $[L : \mathbb{Q}]$ est une extension galoisienne. En déduire son groupe de Galois.

13. Vérifier que $\mathbb{Q}[x]/x^3 - x + 1$ n'est pas une extension galoisienne de $\mathbb{Q}$. Donner sa clôture galoisienne avec son groupe de Galois

2.1 Groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$

```
Z32=Integers(32), Z32.unit_group(), Z32.unit_gens(),...
```

Le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^\times$ est constitué des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

14. Décrire les groupes $\mathbb{Z}/17\mathbb{Z}^\times$, $\mathbb{Z}/103\mathbb{Z}^\times$,

15. Donner un générateur de $\mathbb{Z}/17\mathbb{Z}$ et un générateur de $\mathbb{Z}/103\mathbb{Z}$.

16. Décrire les groupes $\mathbb{Z}/4\mathbb{Z}^\times$, $\mathbb{Z}/8\mathbb{Z}^\times$, $\mathbb{Z}/16\mathbb{Z}^\times$, $\mathbb{Z}/32\mathbb{Z}^\times$, $\mathbb{Z}/64\mathbb{Z}^\times$ et $\mathbb{Z}/9\mathbb{Z}^\times$, $\mathbb{Z}/27\mathbb{Z}^\times$, $\mathbb{Z}/81\mathbb{Z}^\times$.