Université Paris 7 **23 septembre 2016**
Algèbre

TD2 : polynômes

1 Polynômes

Exercice 1 :

Quels sont les polynômes irréductibles de $\mathbb{C}[x]$? de $\mathbb{R}[x]$?

Exercice 2 :

Montrer que deux polynômes de $K[x]$ sont premiers entre eux si et seulement si ils n'ont aucune racine commune dans tout corps L contenant K.

Exercice 3 :

1. Donner un exemple de polynôme irréductible de degré 5 sur $\mathbb{F}_2$.

2. Donner un exemple de polynôme irréductible de degré 10 sur $\mathbb{Q}$.

Exercice 4 :

Soit $K \subset L$ deux corps, et $P \in K[x]$ tel que P possède une racine dans L commune avec un polynôme Q de degré strictement inférieur. Montrer que P n'est pas irréductible.

Exercice 5 :

Montrer qu'un corps algébriquement clos est infini.

Exercice 6 :

1. Montrer que $x^4 + x + 1$ est irréductible sur $\mathbb{F}_2$.

2. $x^8 + x^2 + 1$ est-il irréductible sur $\mathbb{F}_2$?

3. Calculer l'inverse de $x^2 + x + 1$ dans $\mathbb{F}_2[x]/(x^8 + x^2 + 1)$ de trois manières différentes (effectuer réellement le calcul pour deux d'entre elles).

4. Quels sont les inversibles de $\mathbb{F}_2[x]/(x^8 + x^2 + 1)$? calculer leur nombre.

5. Proposer une quatrième manière pour calculer l'inverse de $x^2 + x + 1$ dans $\mathbb{F}_2[x]/(x^8 + x^2 + 1)$ (ne pas effectuer les calculs).

2 Irréductibles

Exercice 7 :

Soit $P \in \mathbb{Z}[x]$. Montrer que s'il existe p premier ne divisant pas le coefficient dominant de P et tel que P mod p est irréductible dans $\mathbb{F}_p[x]$, alors P est irréductible dans $\mathbb{Q}[x]$.

Exercice 8 : critère d'Eisenstein

1. Soit $P(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. On suppose qu'il existe p premier tel que
   — p ne divise pas a_n
   — p divise tous les autres a_i, $i = 0, \dots n-1$
   — p^2 ne divise pas a_0

   Montrer que P est irréductible.

2. Montrer que pour tout p premier, $x^{p-1} + x^{p-2} + \dots x + 1$ est irréductible dans $\mathbb{Z}[x]$.

3 Racines

Exercice 9 :

1. Soit $P(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. Montrer que si $\frac{p}{q} \in \mathbb{Q}$ est racine de P, alors $p \mid a_0$ et $q \mid a_n$.
2. $P(x) = x^3 - 4x^2 - 9/2x - 5/2$ est il irréductible sur $\mathbb{Q}$?

Exercice 10 :

Montrer que si $P \in \mathbb{Q}(x)$ est irréductible, alors P est à racines simples dans $\mathbb{C}$.

Exercice 11 :

On considère $a = x \bmod x^3 + x + 1 \in \mathbb{F}_2[x]/(x^3 + x + 1)$. Montrer que a^2 est racine de $x^3 + x + 1$, ainsi que a^4.

4 Corps finis

Exercice 12 :

1. Quels sont les polynômes irréductibles de degré 2 sur $\mathbb{F}_3$?
2. Construire explicitement deux corps K_1 et K_2 à 9 éléments.
3. Ecrire un isomorphisme entre ces deux corps.

Exercice 13 :

1. Montrer que les carrés de $\mathbb{F}_p^\times$ sont les racines de $x^{\frac{p-1}{2}} - 1$.
2. Montrer que $x^2 + 1$ est irréductible dans $\mathbb{F}_p$ si et seulement si $p \equiv 3 \bmod 4$.

Exercice 14 :

Soit p premier impair et α une racine de $x^4 + 1$ dans un corps L contenant $\mathbb{F}_p$. On pose $y = \alpha + \alpha^{-1}$.

1. Montrer que $y^2 = 2$.
2. Montrer que α est d'ordre 8 dans $L^\times$.
3. Montrer que $y^p = y$ si $p \equiv \pm 1 \bmod 8$.
4. Montrer que $y^p = -y$ si $p \equiv \pm 3 \bmod 8$.
5. En déduire que $x^2 - 2$ est irréductible dans $\mathbb{F}_p$ si et seulement si p est impair et $p \equiv \pm 3 \bmod 8$.

Exercice 15 :

1. Montrer que $x^4 + 1$ est irréductible dans $\mathbb{Z}[X]$
2. On introduit α comme dans l'exercice précédent, déterminer un annulateur de degré 2 de α dans $\mathbb{F}_p[x]$.
3. En déduire que la réciproque de l'exercice 7 est fausse. [1]

1. Du moins en degré 4. On déduit de la théorie de Galois que cette réciproque marche quand le degré est premier, tandis que tout degré pair $\geqslant 4$ fournit des contre-exemples.