ENS Lyon 2011 - 2012
MASTER 1

Algèbre Approfondie

20.09.2011

TD 1

Exercice 1. Critère d'Eisenstein.

1. Soit A un anneau factoriel, on note K son corps de fractions. Soit $P = a_n X^n + ... + a_0$ un polynôme de $A[X]$. On suppose qu'il existe un élément irréductible $p \in A$ tel que :

$$\begin{cases} p & \not| \quad a_n \\ p & | \quad a_i \text{ pour } 0 \leq i \leq n-1 \\ p^2 & \not| \quad a_0. \end{cases}$$

Montrer que P est irréductible dans $K[X]$. L'est-il aussi dans $A[X]$?

2. Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$.
   Indication : on pourra effectuer le changement de variable $Y = X + 1$.
3. Montrer que le polynôme $X^6 + 3$ est irréductible sur le corps $\mathbb{Q}(i)$, avec $i^2 = -1$.
   Indication : on rappelle que $\mathbb{Q}(i)$ *est le corps des fractions de l'anneau des entiers de Gauss* $\mathbb{Z}[i]$ *et que cet anneau est factoriel.*
4. Soit p un nombre premier. Montrer que le polynôme $1 + X + ... + X^{p-1}$ est irréductible sur $\mathbb{Q}$.

Exercice 2. Réduction modulo p.

Soit P un polynôme de degré n à coefficients dans $\mathbb{Z}$. Soit p un nombre premier. On note $\bar{P}$ la réduction de P modulo p, $\bar{P}$ est un polynôme de $\mathbb{F}_p[X]$.

1. Montrer que si $\deg(\bar{P}) = \deg(P)$ et si $\bar{P}$ est irréductible, alors le polynôme P est irréductible sur $\mathbb{Q}$. L'est-il nécessairement sur $\mathbb{Z}$?
2. Montrer que les polynômes $X^4 - 15X^3 + 7$ et $X^5 - 7$ sont irréductibles sur $\mathbb{Q}$.

Exercice 3.

Soit K un corps, soit P un polynôme de $K[X]$.

1. On suppose que le polynôme P est irréductible sur K. On appelle corps de rupture de P sur K une extension M de K dans laquelle P a au moins une racine qui engendre M sur K. Précisément, il existe $\alpha \in M$ tel que $M = K(\alpha)$ et $P(\alpha) = 0$.
   (a) Montrer que le quotient $M = K[X]/(P)$ est un corps de rupture de P sur K.
   (b) Montrer que si M' est un autre corps de rupture de P sur K, alors les corps M et M' sont isomorphes.
2. Maintenant, P est un polynôme quelconque. On appelle corps de décomposition de P sur K une extension L de K dans laquelle P est scindé et qui est engendrée par les racines de P.
   (a) On suppose que P est de degré n. Montrer que P admet au moins un corps de décomposition sur K, noté L, et que l'on a $[L : K] \leq n!$.
   (b) Si de plus P est irréductible, montrer que n divise $[L : K]$.
   (c) Vérifier que le polynôme $P(X) = X^4 - 7$ est irréductible sur $\mathbb{Q}$, puis donner "le" corps de décomposition de P sur $\mathbb{Q}$.

(d) Quel est le corps de décomposition du polynôme $Q(X) = (X^3 - 2)(X^2 - 2)$ sur $\mathbb{Q}$?

Exercice 4.

Soit K un corps. On fixe une clôture algébrique $\bar{K}$ de K. Soit $a \in \bar{K}$ de degré n sur K et de polynôme minimal P sur K. Soit $b \in \bar{K}$ de degré m sur K. On suppose que les entiers n et m sont premiers entre eux.

1. Montre que le polynôme P est irréductible sur $K(b)$.
2. Montrer : $K(a) \cap K(b) = K$.

Exercice 5.

1. Soit p un nombre premier. Quel est le degré de l'extension $K = \mathbb{Q}(3^{1/p})$ sur $\mathbb{Q}$? Quels sont les sous-corps de K ?
2. Déterminer le degré des extensions suivantes :
   (a) $\mathbb{Q}(2^{1/3}, \sqrt{2})$ sur $\mathbb{Q}(2^{1/3})$, puis sur $\mathbb{Q}$.
   (b) $\bar{\mathbb{Q}}$ sur $\mathbb{Q}$.
   (c) $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$ sur $\mathbb{Q}$ pour tout $n \geq 1$, où p_1,...,p_n sont des nombres premiers distincts.
3. Trouver le polynôme minimal sur $\mathbb{Q}$ de $a + \sqrt{2}$, où $a \in \mathbb{C}$ est racine du polynôme $X^2 + X - 1$.

Exercice 6.

Soit p un nombre premier impair. On pose $a = z + 1/z$, avec $z = \exp(2i\pi/p)$.

1. Montrer que z est algébrique de degré 2 sur $\mathbb{Q}(a)$.
2. En déduire que a est algébrique de degré $(p-1)/2$.
3. Déterminer le polynôme minimal de a lorsque $p = 5$, puis $p = 7$.

Exercice 7. **Caractérisation des extensions monogènes finies.**

1. Soit L/K une extension de corps telle que l'ensemble des sous-corps de L contenant K est fini. Montrer que l'extension L/K est monogène.

   On pourra d'abord montrer que cette extension est finie.
2. Réciproquement, soit L/K une extension finie monogène. Soit $\alpha \in L$ un élément tel que $L = K(\alpha)$.
   (a) Soit M une extension intermédiaire, c'est-à-dire $K \subset M \subset L$. Montrer que M est le sous-corps de$L$ engendré sur K par les coefficients du polynôme minimal de α sur M.
   (b) En déduire que l'ensemble des sous-corps de L contenant K est fini.