Université Paris-Sud
Mathématiques générales (algèbre).
D4M4U9, 2008/2009

Feuille de TD numéro 2.

1. Soient K un corps, L une extension de K de degré m et P un polynôme irréductible de degré n dans $K[X]$.

a) On suppose que P s'écrit $P = QR$ avec Q, R dans $L[X]$ et Q irréductible dans $L[X]$. Soit F un corps de rupture de Q sur L. Montrer que n divise $[F : K]$.

b) En déduire que si m et n sont premiers entre eux, alors P est irréductible sur L.

2. Soit K un corps de caractéristique 0. On considère une extension L de K de la forme $L = K[x, y]$. On appelle P et Q les polynômes minimaux de x, y sur K, et on note M un corps de décomposition de PQ sur K. On pose

$$P = (X - x)\prod_{i=2}^{n}(X - x_i)$$

$$Q = (X - y)\prod_{j=2}^{m}(X - y_j)$$

avec les x_i et les y_j dans M.

a) Montrer que pour tous indices i, j, on a $x \neq x_i$ et $y \neq y_j$.

b) Montrer qu'il existe $t \in K^*$ tel que pour tous indices i, j, on ait $x + ty \neq x_i + ty_j$.

c) Soit alors $z = x + ty$ et $K' = K[z]$. On pose $F(X) = P(z - tX)$. Montrer que le polynôme F est dans $K'[X]$, et que $(X - y)$ est le pgcd de F et Q.

d) En déduire que $y \in K'$, puis que $L = K'$.

e) Soit F une extension finie de K. Montrer qu'il existe $\alpha \in F$ tel que $F = K[\alpha]$ (théorème de *l'élément primitif*).

3. Soit $\mathbf{F}_q$ le corps fini à q éléments (où q est une puissance d'un nombre premier p). Soit $n > 0$; on note $I(n, q)$ le nombre de polynômes irréductibles unitaires de degré n de $\mathbf{F}_q[X]$.

Soit Q le polynôme

$$Q = X^{q^n} - X$$

de $\mathbf{F}_q[X]$.

1. Montrer que dans la décomposition

$$Q = P_1^{\alpha_1} ... P_r^{\alpha_r}$$

de Q en produits de facteurs irréductibles (où les P_i sont unitaires, irréductibles, deux à deux premiers entre eux et $\alpha_i \geq 1$), tous les α_i sont égaux à 1. On écrit désormais

$$Q = P_1 ... P_r$$

avec P_i unitaire irréductible et P_i premier avec P_j si $i \neq j$.

2. Soit P un polynôme irréductible de degré d dans $\mathbf{F}_q[X]$, avec d divisant n.

a) Soit x une racine de P dans un corps de rupture de P sur $\mathbf{F}_q$. Montrer que $Q(x) = 0$.

b) En déduire que P divise Q.

3. Soit réciproquement F un polynôme irréductible de degré s tel que F divise Q. Soit K un corps de décomposition de Q sur $\mathbf{F}_q$.

a) Montrer que le cardinal de K est q^n.

b) Montrer que K contient un corps de rupture de F sur $\mathbf{F}_q$.

c) En déduire que s divise n.

4. En utilisant 2. et 3., montrer que les P_i sont exactement les polynômes irréductibles unitaires de $\mathbf{F}_q[X]$ dont le degré divise n.

5. Montrer que

$$q^n = \sum_{d|n} dI(d, q)$$