141. Polynômes irréductibles, corps de rupture : questions

On pourra aussi reprendre l'exercice 3 de la feuille de questions relatives à la leçon 151.

1. Soit K un corps fini de cardinal q. Soit $d > 0$ un entier.

a) Montrer qu'il existe une extension de corps L de K de degré d, unique à isomorphisme près. Quel est le cardinal de L ?

b) On rappelle que le groupe multiplicatif L^* est cyclique. Soit α un générateur de ce groupe. Montrer que $L = K[\alpha]$.

c) En déduire qu'il existe un polynôme irréductible P dans $K[X]$, avec $\deg P = d$ (remarque : trouver explicitement un tel P est un problème algorithmique difficile !).

2. (Sorte de réciproque de l'exercice 1) . Soit K un corps fini de cardinal q. Soit $P \in K[X]$ un polynôme irréductible de degré d. Soit $L = K[\alpha]$ un corps de rupture de P.

a) Montrer que l'application $F : x \mapsto x^q$ est un automorphisme du corps L qui induit l'identité sur K. On note $F^m = F \circ F \circ ... \circ F$ le m-ième itéré de F.

b) Montrer que d est le plus petit entier $m > 0$ tel que $F^m(\alpha) = \alpha$ (raisonner par l'absurde, en montrant que si on avait $m < d$, alors α appartiendrait à une extension de corps de K strictement incluse dans L).

c) En déduire que L est aussi un corps de décomposition de P.

d) On pose $K = \mathbf{F}_4$ et $L = \mathbf{F}_{16}$, corps respectivement à 4 et à 16 éléments. Montrer que L est une extension de degré 2 de F qui peut s'écrire $L = K[\alpha]$, où α est un élément d'ordre 5 de L^* (ici α n'est donc pas un générateur de L^*).

3. Soit K un corps.

a) Montrer que si K est fini de caractéristique p, alors l'application $x \mapsto x^p$ de K dans K est bijective.

b) On suppose maintenant K de caractéristique zéro. Montrer que si $P \in K[X]$ est irréductible dans $K[X]$ et si L est une extension de corps de K, alors toute racine de P dans L est simple.

c) Montrer que b) reste vrai si K est un corps fini (utiliser a), mais qu'il est faux si $K = \mathbf{Z}/p\mathbf{Z}(T)$.

4. Soit $F \in \mathbf{Z}[X]$ un polynôme unitaire de degré au moins 1. Soit p un nombre premier. On note $\overline{F} \in \mathbf{Z}/p\mathbf{Z}[X]$ le polynôme obtenu en réduisant les coefficients de F modulo p.

a) On suppose que $\overline{F}$ est irréductible dans $\mathbf{Z}/p\mathbf{Z}[X]$. Montrer que F est irréductible.

b) La réciproque de a) est-elle vraie ?

c) Peut-on, dans a), remplacer l'hypothèse F unitaire par F primitif ?

5. Soit K un corps. Soit $P \in K[X]$ un polynôme de degré d. Soit L le corps de décomposition de P. Montrer que $[L : K] \leq d!$ (on pourra procéder par récurrence sur d, et utiliser la notion de corps de rupture). Donner un exemple avec $d = 3$ où on a $[L : K] = d!$.