Exercices - Feuille E 7 Avril 2004

Exercice E1. Soient p un nombre premier, f un entier ≥ 1 et F un corps ayant q éléments avec $q = p^f$. On désigne par $\mathbf{F}_p$ le sous-corps premier de F et par $G = \mathrm{Aut}F$ le groupe des automorphismes de F.
a) Montrer que si L est un sous-corps de F il existe un diviseur d de f tel que le nombre d'éléments de L soit p^d.
b) Inversement, soit d un diviseur de f. Montrer qu'il existe un unique sous-corps L de F ayant p^d éléments.
c) Montrer que l'application $\varphi : F \to F$, $\varphi(x) = x^p$ est un automorphisme de F. Quel est l'ordre de φ dans le groupe G?
d) Montrer que G est un groupe cyclique engendré par φ.
e) Quand H est un sous-groupe de G, on note

$$F^H = \{x \in F \ ; \ \psi(x) = x \ \text{ pour tout } \psi \in H\}.$$

Montrer que F^H est un sous-corps de F. Quel est le nombre d'éléments de F^H?
f) Quand L est un sous-corps de F, on note

$$G(F/L) = \{\psi \in G \ ; \ \psi(x) = x \ \text{ pour tout } x \in L\}.$$

Montrer que $G(F/L)$ est un sous-groupe de G. Vérifier que la restriction à L d'un automorphisme de F définit un morphisme de groupes de G sur $G(L/\mathbf{F}_p)$ de noyau $G(F/L)$. En déduire l'ordre du groupe $G(F/L)$.
g) Vérifier que $H \mapsto F^H$ et $L \mapsto G(F/L)$ sont des bijections réciproques de l'ensemble des sous-groupes de G sur l'ensemble des sous-corps de F.
h) Soit $\alpha \in F^\times$. On désigne par s le plus petit entier ≥ 1 tel que $\alpha^{p^s} = \alpha$. Montrer que α est de degré s sur $\mathbf{F}_p$ et que le polynôme irréductible de α sur $\mathbf{F}_p$ est

$$(X - \alpha)(X - \alpha^p) \cdots (X - \alpha^{p^{s-1}}).$$

Exercice E2. On désigne par Ω un corps algébriquement clos contenant $\mathbf{F}_p$ et on note $\overline{\mathbf{F}}_p$ l'ensemble des éléments de Ω algébriques sur $\mathbf{F}_p$ (on dit que $\overline{\mathbf{F}}_p$ est une *clôture algébrique de* $\mathbf{F}_p$). Montrer que pour chaque entier $n \geq 1$ il existe un unique sous-corps de $\overline{\mathbf{F}}_p$ ayant p^n éléments. On désigne ce sous-corps par $\mathbf{F}_{p^n}$. Montrer, pour n et m entiers ≥ 1, l'équivalence

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \ \text{ divise } m.$$

http://www.math.jussieu.fr/∼miw/enseignement.html