X

Exercice 1 (Les sous-groupes transitifs et résolubles de S_p, p premier) Soit p un nombre premier.

a) Vérifier que Aff_p peut s'identifier à un sous-groupe transitif de S_p et plus précisément au normalisateur de $\langle(12...p)\rangle$.

b) Vérifier que si $\sigma \in \mathrm{Aff}_p$ fixe deux éléments de $\{1, ..., p\}$, alors σ est l'identité.

c) Montrer que tout sous-groupe transitif et résoluble de S_p est conjugué à un sous-groupe de Aff_p.

d) Déduire des questions précédentes que si f est un polynôme irréductible sur $\mathbb{Q}$ de degré p, alors sont équivalentes :

   i) l'équation $f = 0$ est résoluble par radicaux sur $\mathbb{Q}$.

   ii) Si x_1, x_2 sont des racines distinctes quelconques de f, alors $\mathbb{Q}(x_1, x_2)$ contient toutes les racines de f.

e) Montrer que si f est un polynôme irréductible sur $\mathbb{Q}$ de degré p premier avec une racine réelle qui peut s'exprimer avec des radicaux, alors f a toutes ses racines réelles ou une seule racine réelle.

Exercice 2 (Extensions cycliques en caractéristique p) Soit k un corps de caractéristique p. Soit F une extension galoisienne cyclique de degré p de k. Soit σ un générateur du groupe de Galois de F sur k.

a) Montrer que l'endomorphisme $k-$linéaire de F :

$$S : \alpha \mapsto \alpha - \sigma(\alpha)$$

est nilpotent.

b) Soit $\alpha \in \ker S^2 \setminus \ker S$. Montrer que $\beta := \frac{\alpha}{\sigma(\alpha)-\alpha}$ vérifie $\sigma(\beta) = \beta + 1$.

c) En déduire que β vérifie une équation de la forme $X^p - X - a = 0$.

Exercice 3 (Entiers des corps cyclotomiques) a) Montrer que le discriminant du polynôme $\Phi_n(X)$ est :

$$(-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod\limits_{\substack{p|n \\ p \text{ premier}}} p^{\frac{\varphi(n)}{p-1}}}$$

b) Soient p un nombre premier et z une racine primitive $p-$ième de l'unité. On note A l'anneau des entiers de $\mathbb{Q}(z)$. Montrer que :

$$p = (1-z)...(1-z^{p-1})$$

et en déduire que :

$$A(1-z) \cap \mathbb{Z} = p\mathbb{Z}$$

Montrer que pour tout $y \in A$, $\mathrm{tr}(y(1-z)) \in p\mathbb{Z}$.

On suppose que $x = a_0 + ... + a_{p-2}z^{p-2}$ est entier sur $\mathbb{Z}$ avec les $a_i \in \mathbb{Q}$. En calculant $\mathrm{tr}(x(1-z))$, montrer que $a_0 \in \mathbb{Z}$ puis que tous les a_i sont entiers (*indication : calculer d'abord* $\mathrm{tr}(z^j)$, $0 \leq j \leq p-1$). En déduire que $A = \mathbb{Z}[z]$.

c) Traiter le cas où z est une racine primitive p^r-ième de l'unité.

d) Traiter le cas général : montrer que si z est une racine primitive $n-$ième de l'unité, alors $\mathbb{Z}[z]$ est l'anneau des entiers de $\mathbb{Q}(z)$.