ENS Lyon **Algèbre approfondie**
M1 **2008-2009**

FEUILLE 11

Exercice 1 — Soit $f \in \mathbb{Z}[\mathrm{T}]$ un polynôme unitaire de degré n. On suppose qu'il existe trois nombres premiers $p_1,\ p_2$ et p_3 tels que

(i) le polynôme $f \pmod{p_1}$ soit irréductible ;

(ii) le polynôme $f \pmod{p_2}$ soit le produit d'un facteur irréductible de degré 2 et d'un ou de deux facteur(s) irréductible(s) de degré impair dans $\mathbb{F}_{p_2}[\mathrm{T}]$;

(iii) le polynôme $f \pmod{p_3}$ soit le produit d'un facteur linéaire et d'un facteur irréductible dans $\mathbb{F}_{p_3}[\mathrm{T}]$.

1. Démontrer que le groupe de Galois G d'un corps de décomposition de f au-dessus de $\mathbb{Q}$ est un sous-groupe transitif de $\mathfrak{S}_n$ contenant une transposition et un cycle de longueurs $n-1$; en déduire que $\mathrm{G} = \mathfrak{S}_n$.

2. Lorsque n est un nombre premier, montrer que les conditions (i) et (ii) suffisent à garantir $\mathrm{G} = \mathfrak{S}_n$.

3. Déterminer les groupes de Galois des polynômes $\mathrm{T}^5 - \mathrm{T} - 1$ et $\mathrm{T}^7 - \mathrm{T} - 1$.

Exercice 2 (*L'ubiquité des groupes symétriques comme groupes de Galois sur* $\mathbb{Q}$) — Soit $n \geq 2$ un entier naturel. Étant donné un entier naturel $\mathrm{N} \geq 1$, on note $\sigma_n(\mathrm{N})$ le nombre des polynômes unitaires $f \in \mathbb{Z}[\mathrm{T}]$ de degré n dont les coefficients sont majorés par N en valeur absolue et dont le groupe de Galois est $\mathfrak{S}_n$.

Suivant B.L. van der Waerden (*Die Seltenheit der Gleichungen mit Affekt*, Mathematische Annalen **109** (1934)), cet exercice a pour objet d'établir que la proportion $(2\mathrm{N}+1)^{-n}\sigma_n(\mathrm{N})$ de ces polynômes tend vers 1 lorsque N tend vers $+\infty$.

1. Étant donné un nombre premier $p \geq 3$, dénombrer les polynômes unitaires de degré n dans $\mathbb{F}_p[\mathrm{T}]$ qui sont soit irréductibles (*type 1*), soit le produit d'un facteur irréductible de degré 2 et d'un ou de deux facteur(s) irréductible(s) de degré impair (*type 2*), soit le produit d'un facteur linéaire et d'un facteur irréductible (*type 3*). Dans chaque cas de figure, vérifier qu'il y a au moins $p^n/k(n)$ tels polynômes, où $k(n) = 8(n-2)$.

2. Soit $p_1, \ldots, p_r$ des nombres premiers et $\mathrm{P} = p_1 \ldots p_r$. Quel que soit $i \in \{1, 2, 3\}$, vérifier qu'il y a au plus

$$\left(1 - \frac{1}{k(n)}\right)^r \mathrm{P}^n$$

polynômes unitaires et de degré n dans $\mathbb{Z}/\mathrm{P}\mathbb{Z}[\mathrm{T}]$ dont la réduction modulo chacun des nombres premiers $p_1, \ldots, p_r$ ne soit pas de type i.

3. On ordonne les nombres premiers $(p_i)_{i \geqslant 1}$ par ordre croissant et on note $r(\mathrm{N})$ le plus grand entier tel que $p_1 \ldots p_r \leqslant 2\mathrm{N}+1$.

(i) Majorer le nombre de polynômes unitaires de degré n dont les coefficients sont majorés par N et dont la réduction modulo P est fixée.

(ii) Démontrer la minoration

$$\frac{\sigma_n(\mathrm{N})}{(2N+1)^n} \geq 1 - 3 \cdot 2^n \left(1 - \frac{1}{k(n)}\right)^{r(\mathrm{N})}$$

et en déduire

$$\lim_{\mathrm{N}} \frac{\sigma_n(\mathrm{N})}{(2\mathrm{N}+1)^n} = 1.$$