Introduction à la théorie de Galois
Contrôle de connaissances

29 juin 2004

Durée : 1h30. Calculatrices et notes de cours sont autorisées. Une étoile (*) indique une question probablement un peu plus difficile.

Exercice 1 *a) Calculer* $(\sqrt{2}+\sqrt{5})^2$ *et* $(\sqrt{2}+\sqrt{5})^3$.

b) Montrer qu'on a $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{5})$.

c) Montrer que $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ *est une extension normale de* $\mathbb{Q}$.

d) Plus généralement, si p *et* q *sont deux nombres premiers distincts, montrer que* $\mathbb{Q}(\sqrt{p}+\sqrt{q})$ *est une extension normale de* $\mathbb{Q}$.

Exercice 2 *(*) Soit* G *un groupe fini. Montrer qu'il existe un corps* K *qui admet une extension galoisienne finie de groupe de Galois isomorphe à* G.

Problème 3 On se propose ici de montrer l'impossibilité de la résolution par radicaux de l'équation "universelle" de degré $n \geq 5$ suivant les preuves originales d'Abel et Ruffini, antérieures aux résultats plus généraux de Galois. On note

$$K = \mathbb{C}(x_1, \ldots, x_n)$$

le corps des fractions rationnelles en n indéterminées sur $\mathbb{C}$. Le groupe $\mathfrak{S}_n$ des permutations de $\{1, \ldots, n\}$ agit sur K de la façon suivante : pour $\sigma \in \mathfrak{S}_n$ et $f = f(x_1, \ldots, x_n) \in K$, on définit $A_\sigma(f) \in K$ par la formule

$$A_\sigma(f)(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

a) Vérifier que cette formule définit bien une action de groupe, en ce sens que pour tous $\sigma, \tau \in \mathfrak{S}_n$ *et* $f \in K$ *on a*

$$A_\sigma(A_\tau(f)) = A_{\sigma\circ\tau}(f).$$

b) Soient $f \in K$ *et* $k \geq 1$ *un entier. On suppose qu'il existe* $\sigma \in \mathfrak{S}_n$ *laissant* f^k *invariant. Montrer qu'il existe alors une racine* k*-ième de l'unité* ω *telle que*

$$A_\sigma(f) = \omega f.$$

c) *Avec les notations de la question précédente, montrer que ω est aussi une racine d-ième de l'unité, où d est l'ordre de σ.*

d) *On considère les cycles $c = (1\,2\,3)$ et $c' = (3\,4\,5)$, éléments de $\mathfrak{S}_n$. Calculer $c \circ c'$ et $c^2 \circ c'$.*

e) *Soient $f \in K$ et $k \geq 1$ un entier. On suppose que f^k est invariant sous c et sous c'. Montrer qu'alors il en est de même de f.*

f) *On note F le sous-corps de K formé des fractions rationnelles invariantes sous l'action de $\mathfrak{S}_n$, de sorte que $F = \mathbb{C}(s_1, \ldots, s_n)$ où les s_i sont les fonctions symétriques élémentaires en $x_1, \ldots, x_n$. Montrer qu'il n'existe pas de suite d'éléments $g_1, g_2, \ldots, g_N$ de K vérifiant les conditions suivantes :*
– *pour tout i, il existe un entier $k_i \geq 1$ tel que $g_i^{k_i} \in F(g_1, g_2, \ldots, g_{i-1})$;*
– *$x_1 \in F(g_1, \ldots, g_N)$.*

Le résultat de la question précédente, démontré pour la première fois par Ruffini en 1799 (et simplifié en 1813), peut s'interpréter comme suit : il est impossible de résoudre par radicaux l'équation universelle de degré $n \geq 5$, du moins sous la condition additionnelle que les quantités auxiliaires introduites ne sortent pas de $\mathbb{C}(x_1, \ldots, x_n)$ (i.e. les $g_1, \ldots, g_N$ restent dans K). Le "théorème des irrationalités naturelles" d'Abel (1824) montre que cette dernière condition n'est pas essentielle ; c'est ce que l'on va prouver dans les questions suivantes. Notons Ω une extension algébriquement close de K (et donc de F).

g) *(*) Soient p un nombre premier, W une extension de F incluse dans Ω, a un élément de W n'admettant pas de racine p-ième dans W, et α une racine p-ième de a dans Ω. Montrer que $X^p - a$ est irréductible sur W, et que $W(\alpha)$ est une extension normale de W de degré p.*

h) *(*) Sous les hypothèses de la question précédente, on suppose qu'il existe $f \in K$ tel que $f \in W(\alpha)$ mais $f \notin W$. Montrer qu'alors il existe $\alpha' \in W(\alpha) \cap K$ qui soit racine p-ième d'un élément de $W \cap K$ et tel que $f \in (W \cap K)(\alpha')$.*

i) *Montrer qu'il n'existe pas de suite d'éléments $h_1, h_2, \ldots, h_N$ de Ω vérifiant les conditions suivantes :*
– *pour tout i, il existe un entier $k_i \geq 1$ tel que $h_i^{k_i} \in F(h_1, h_2, \ldots, h_{i-1})$;*
– *$x_1 \in F(h_1, \ldots, h_N)$.*