Introduction à la théorie de Galois
Contrôle de connaissances

21 juin 2005

Durée : 1h30. Calculatrices et notes de cours sont autorisées.

Exercice 1 *Le polynôme X^4+1 est-il irréductible sur $\mathbb{R}$? Décrire l'anneau quotient $\mathbb{R}[X]/X^4+1$.*

Problème 2 *a) Soient $p_1, \ldots, p_n$ des entiers naturels et $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Montrer que K est une extension normale de $\mathbb{Q}$ (donc galoisienne, puisque $\mathbb{Q}$ est de caractéristique nulle).*

b) Montrer qu'on a

$$[K : \mathbb{Q}] = 2^m$$

pour un certain entier $m \leq n$, avec en outre $m = n$ si et seulement si p_k n'est un carré dans $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$ pour aucun $k \leq n$.

c) On fait maintenant l'hypothèse supplémentaire que $p_1, \ldots, p_n$ sont des nombres premiers, deux à deux distincts. Soit $x \in K$ vérifiant $x^2 \in \mathbb{Q}$. Montrer qu'alors il existe $r \in \mathbb{Q}$ et $\epsilon_1, \ldots, \epsilon_n \in \{0, 1\}$ tels que

$$x^2 = r^2 p_1^{\epsilon_1} \ldots p_n^{\epsilon_n}$$

(on pourra raisonner par récurrence sur n, en montrant par la même occasion que $[K : \mathbb{Q}] = 2^n$).

d) Supposant toujours $p_1, \ldots, p_n$ premiers et deux à deux distincts, décrire le groupe de Galois de K sur $\mathbb{Q}$.

e) Soient a et b deux rationnels non nuls. Montrer que

$$\mathbb{Q}(a\sqrt{2} + b\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Plus généralement, $p_1, \ldots, p_n$ étant des nombres premiers deux à deux distincts, et $a_1, \ldots, a_n$ des rationnels, montrer que

$$\mathbb{Q}(a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$$

si et seulement si $a_1, \ldots, a_n$ sont tous non nuls.

Problème 3 Le but de ce problème est de donner une forme générale pour les extensions de groupe de Galois $\mathbb{Z}/3\mathbb{Z}$. On commence par quelques généralités sur les extensions cycliques de degré quelconque.

Soient n un entier naturel et L/K une extension de corps galoisienne de groupe de Galois G isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Plus précisément, choisissons un générateur σ de G, de sorte que $\sigma^n = 1$ et $G = \{1, \sigma, \ldots, \sigma^{n-1}\}$. On définit des opérateurs "norme" N et "trace" Tr par les formules

$$\mathrm{N}(x) = x\sigma(x)\ldots\sigma^{n-1}(x)$$

et

$$\mathrm{Tr}(x) = x + \sigma(x) + \cdots + \sigma^{n-1}(x)$$

pour $x \in L$.

a) *Montrer que* N *et* Tr *sont à valeurs dans* K.

b) *Soit* $b \in L$. *Montrer qu'il existe* $x \in L$ *tel que*

$$x + b\sigma(x) + b\sigma(b)\sigma^2(x) + \cdots + b\sigma(b)\ldots\sigma^{n-2}(b)\sigma^{n-1}(x) \neq 0.$$

c) *Montrer que* $b \in L$ *vérifie* $\mathrm{N}(b) = 1$ *si et seulement s'il existe* $a \in L^\times$ *tel que* $b = a/\sigma(a)$.

d) *De la même façon, montrer que* $b \in L$ *vérifie* $\mathrm{Tr}(b) = 0$ *si et seulement s'il existe* $a \in L$ *tel que* $b = a - \sigma(a)$.

e) *On suppose maintenant* $n = 3$, *de sorte que* $G = \{1, \sigma, \sigma^2\}$. *Supposons qu'il existe* $y \in L$ *vérifiant*

$$\sigma(y) = 1 - \frac{1}{y}.$$

Exprimer $\sigma^2(y)$ *en fonction de* y. *Montrer que* $\mathrm{N}(y) = -1$, *et que si l'on note* $t = \mathrm{Tr}(y)$, *alors* y *est racine du polynôme* $X^3 - tX^2 + (t-3)X + 1$.

f) *Soit* L/K *une extension galoisienne de groupe de Galois isomorphe à* $\mathbb{Z}/3\mathbb{Z}$. *Montrer qu'il existe* $t \in K$ *tel que le polynôme* $P_t(X) = X^3 - tX^2 + (t-3)X + 1$ *soit irréductible sur* K, *et que* L *soit isomorphe à l'anneau quotient* $K[X]/P_t(X)$.