Introduction à la théorie de Galois
Contrôle de connaissances

26 juin 2002

Durée : 1h30. Les exercices sont indépendants. En revanche, les réponses aux questions du problème pourront faire appel aux résultats des questions précédentes. Le nombre d'étoiles (*) est une mesure approximative de la difficulté des questions. Le sujet étant assez long, il ne sera probablement pas nécessaire de tout faire pour avoir le maximum des points.

Exercice 1 () *Résoudre par radicaux l'équation (à coefficients rationnels)*

$$X^2 = X + 1.$$

Exercice 2 (*) *Donner une expression par radicaux aussi simple que possible des solutions de l'équation*

$$X^4 - 6X^2 + 1 = 0.$$

Exercice 3 (*) *Quelle est l'aire d'un triangle rectangle dont l'hypothénuse est de longueur* 130 *et le périmètre de longueur* 308 *?*

Exercice 4 (**) *Soit* $P(X) \in \mathbb{Q}[X]$ *un polynôme de degré* 3 *à coefficients rationnels. On suppose que* P *a une racine double dans* $\mathbb{C}$. *Montrer que toutes les racines de* P *sont dans* $\mathbb{Q}$.

Problème 5 *Dans ce problème on fixe* p *un nombre premier différent de* 2. *On se propose d'étudier le corps engendré sur* $\mathbb{Q}$ *par le nombre complexe* $\zeta_p = e^{\frac{2i\pi}{p}}$.

a) (**) *Soient* $P(X) \in \mathbb{Z}[X]$ *et* $Q(X) \in \mathbb{Z}[X]$ *deux polynômes à coefficients entiers. Montrer que le p.g.c.d. des coefficients du polynôme produit* $P(X)Q(X)$ *est égal au produit du p.g.c.d. des coefficients de* $P(X)$

et du p.g.c.d. des coefficients de $Q(X)$ (indication : on pourra se ramener au cas où ces deux derniers p.g.c.d. sont tous deux égaux à 1, et par l'absurde supposer qu'il existe un nombre premier q divisant le p.g.c.d. des coefficients de $P(X)Q(X)$).

b) (*) *Soit* $P(X) \in \mathbb{Z}[X]$ *un polynôme à coefficients entiers. On suppose que* $P(X)$ *est produit de deux polynômes non constants à coefficients rationnels. Montrer qu'alors* $P(X)$ *est produit de deux polynômes non constants à coefficients entiers.*

c) (**) *Soit* $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ *un polynôme unitaire à coefficients entiers. On suppose que les entiers* $a_0, a_1, \ldots, a_{n-1}$ *sont tous divisibles par le nombre premier* p*, mais que* a_0 *n'est pas divisible par* p^2*. Montrer qu'alors* $P(X)$ *n'est pas produit de deux polynômes non constants à coefficients entiers.*

d) (**) *Montrer que le polynôme* $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ *est irréductible sur* $\mathbb{Q}$ (indication : on pourra considérer le polynôme $\Phi_p(X+1)$).

e) (*) *Montrer que le corps* $\mathbb{Q}(\zeta_p)$ *est une extension finie et normale de* $\mathbb{Q}$.

f) (*) *Montrer que le groupe de Galois de* $\mathbb{Q}(\zeta_p)$ *sur* $\mathbb{Q}$ *s'identifie naturellement au groupe multiplicatif* $(\mathbb{Z}/p\mathbb{Z})^\times$ *(formé des éléments non nuls du corps fini* $\mathbb{Z}/p\mathbb{Z}$*).*

g) (*) *Montrer qu'il existe un unique corps* F *de degré* 2 *sur* $\mathbb{Q}$ *inclus dans* $\mathbb{Q}[\zeta_p]$.

h) (***) *Montrer qu'on a* $F = \mathbb{Q}[\sqrt{p}]$ *si* p *est de la forme* $4k+1$ *et* $F = \mathbb{Q}[i\sqrt{p}]$ *si* p *est de la forme* $4k+3$ (indication : on pourra construire un élément α dans $\mathbb{Q}(\zeta_p)$ dont les images sous l'action du groupe de Galois sont $\pm\alpha$).