Université Claude Bernard Lyon I — 2nd semestre 2014/2015
M1 — Théorie de Galois

Examen final,
lundi 8 juin 2015,
9h-12h

---

5 { 1 · **Exercice 1** Factoriser au maximum le polynôme $X^4 - X - 1$ modulo 7 et
+1,5 modulo 17 (*indication : -2 et -5 sont racines modulo* 17). En déduire que
+2,5 le polynôme $X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ et que son groupe de Galois sur $\mathbb{Q}$ contient une transposition et un 3−cycle. En déduire que le groupe de Galois sur $\mathbb{Q}$ de $X^4 - X - 1$ est $\mathfrak{S}_4$.

Exercice 2 Soit $d \in \mathbb{Z}$; on pose $g_d(X) := X^3 + (2d+2)X^2 + (2d-1)X - 1 \in \mathbb{Z}[X]$ et $f_d(X) := g_d(X^2)$. On note θ_d une racine de f_d dans $\mathbb{C}$, $K_d := \mathbb{Q}(\theta_d)$, $C_d := \mathbb{Q}(\theta_d^2)$ et L_d le corps de décomposition de f_d dans $\mathbb{C}$. Enfin, on pose $G_d := \mathrm{Gal}(L_d/\mathbb{Q})$.

$$\begin{array}{c} L_d \\ | \\ K_d \\ | \\ C_d \\ | \\ \mathbb{Q} \end{array}$$

0,5 a) Montrer que $[K_d : \mathbb{Q}] \leq 6$.

1 b) Montrer que g_d est irréductible sur $\mathbb{Q}$.

c) **On admet que :**

1
$$\mathrm{disc}(g_d) = (4d^2 + 2d + 7)^2 \ .$$

En déduire que $C_d = \mathbb{Q}(\theta_d^2)$ est une extension cyclique de degré 3 de $\mathbb{Q}$.

1 d) Montrer que G_d est d'ordre ≤ 12.

3,5 { 1 e) Supposons que f_d est réductible sur $\mathbb{Q}$. Montrer qu'il existe $a, b, c \in \mathbb{Z}$
tels que $h(X) := X^3 + aX^2 + bX + c$ annule θ_d. Montrer qu'alors $f_d(X) =$
+0,5 $-h(X)h(-X)$. En déduire que :

+1

$$\begin{cases} c = \pm 1 \\ 2d + 2 = -a^2 + 2b \\ 2d - 1 = b^2 - 2ac \end{cases} .$$

+1

En déduire une contradiction ! *Donc f_d est irréductible sur $\mathbb{Q}$.*

0,5 f) Déterminer $[K_d : \mathbb{Q}]$ et montrer que $[L_d : \mathbb{Q}] = 6$ ou 12.

1 g) Montrer que $N := \mathrm{Gal}(L_d/C_d)$ est l'unique 2−Sylow de G_d.

1,5 h) Montrer que $\mathrm{disc}(f_d) = 2^6 \mathrm{disc}(g_d)^2$. En déduire que $G_d \leq \mathfrak{A}_6$.

1 i) Montrer qu'il n'y a pas d'éléments d'ordre 6 dans $\mathfrak{A}_6$. En déduire qu'il existe un sous-groupe H de G_d d'ordre 3 qui n'est pas distingué dans G_d.

j) Montrer que L_d^H n'est pas galoisienne sur $\mathbb{Q}$. En déduire que $[L_d : \mathbb{Q}] =$
2 12. Soit $x \in L_d$ tel que $L_d^H = \mathbb{Q}(x)$. Soit P le polynôme minimal de x sur $\mathbb{Q}$. Montrer que L_d est le corps de décomposition de P sur $\mathbb{Q}$.

k) En déduire que $G_d \simeq \mathfrak{A}_4$. En déduire que C_d est l'unique corps compris
2 strictement entre $\mathbb{Q}$ et K_d.

Exercice 3 Si $n \geq 1$, on pose $\zeta_n := e^{2i\pi/n}$.

1,5 a) Soient $m, n \geq 1$. Montrer que $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{\mathrm{ppcm}(m,n)})$.

b) Montrer que le morphisme :

2,5

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n)/\mathbb{Q}(\zeta_n)) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)),\ \sigma \to \sigma\big|_{\mathbb{Q}(\zeta_m)}$$

est injectif. On note I son image. Montrer que $\mathbb{Q}(\zeta_m)^I = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. En déduire la surjectivité du morphisme ci-dessus.

3 c) Montrer que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\mathrm{pgcd}(m,n)})$.

0,5 d) Soient p un nombre premier et $r \geq 1$. On pose $\zeta := \zeta_{p^r}$, $K := \mathbb{Q}(\zeta)$ et $A := \mathbb{Z}[\zeta]$. Montrer que $A \leq \mathcal{O}_K$, anneau des éléments de K entiers sur $\mathbb{Z}$.

2+ 2 e) Montrer que $N_{K/\mathbb{Q}}(1 - \zeta) = p$. En déduire que $1 - \zeta$ n'est pas inversible dans $\mathcal{O}_K$ et que $\mathcal{O}_K(1 - \zeta) \cap \mathbb{Z} = p\mathbb{Z}$.