corrigé de l'examen final du lundi 8 juin 2015

Exercice 1 Soit G le groupe de Galois de $X^4 - X - 1$. Modulo 7 : $X^4 - X - 1 = (X-3)(X^3+3X^2+2X-2)$. Le polynôme X^3+3X^2+2X-2 ne s'annule pas en $0, \pm 1, \pm 2, \pm 3$ donc est irréductible sur $\mathbb{Z}/7\mathbb{Z}$.

Donc si $X^4 - X - 1$ est réductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$, un de ses facteurs irréductibles est de degré 3. Donc $X^4 - X - 1$ a une racine dans $\mathbb{Z}$ qui divise le coefficient constant -1. Donc $X^4 - X - 1$aurait ± 1 comme racine. Absurde ! donc $X^4 - X - 1$ est irréductible sur $\mathbb{Q}$.

On a aussi que G contient un $3-$cycle.

Modulo 17 : $X^4 - X - 1 = (X+2)(X+5)(X^2-7X+5)$. Or le discriminant de $X^2 - 7X + 5$ est -5 qui n'est pas un carré dans $\mathbb{Z}/17\mathbb{Z}$. Donc $X^2 - 7X + 5$ est irréductible. Donc G contient une transposition. Comme $X^4 - X - 1$, G est un sous-groupe transitif de $\mathfrak{S}_4$. Donc son ordre est un multiple de 4. C'est aussi un multiple de 3 vu que G contient un $3-$cycle. Donc $12||G|$. D'où $G = \mathfrak{A}_4$ ou $\mathfrak{S}_4$. Comme G contient une transposition, $G = \mathfrak{S}_4$.

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 $G_d := \mathrm{Gal}(L_d/\mathbb{Q})$.

a) Comme $f_d(\theta_d) = 0$, $[K_d : \mathbb{Q}] \leq \deg f_d = 2 \deg g_d = 6$.

b) Le polynôme g_d est irréductible sur $\mathbb{Q}$ si et seulement s'il l'est sur $\mathbb{Z}$. Or g_d n'a pas de racine dans $\mathbb{Z}$ car une telle racine diviserait le coefficient constant : -1. Mais ± 1 ne sont pas racines :

$$g_d(1) = 4d + 1 \neq 0 \neq -1 = g_d(-1) \ .$$

Donc g_d est irréductible sur $\mathbb{Q}$.

c) Pour le discriminant, on sait que $\mathrm{disc}(a_0X^3 + a_1X^2 + a_2X + a_3) = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3$. Donc :

$$\mathrm{disc}(g_d) = (2d+2)^2(2d-1)^2 - 4(2d-1)^3 + 4(2d+2)^3 - 27 - 18(2d+2)(2d-1)$$
$$= (4d^2 + 2d + 7)^2 \ .$$

Donc le groupe de Galois de g_d est dans $\mathfrak{A}_3$. Donc $\mathrm{Gal}(g_d)$ est d'ordre 3 et forcément, le corps de décomposition de g_d est de degré 3 sur $\mathbb{Q}$. C'est donc $\mathbb{Q}(\theta_d^2) = C_d$. Donc C_d est une extension galoisienne de $\mathbb{Q}$ de degré 3 cyclique.

d) Notons x_1, x_2, x_3 de g_d. On a $L_d = \mathbb{Q}(\sqrt{x_1}, \sqrt{x_2}, \sqrt{x_3}) = \mathbb{Q}(\sqrt{x_1}, \sqrt{x_2})$ car $-(\sqrt{x_1}\sqrt{x_2}\sqrt{x_3})^2 = -1 \Rightarrow \sqrt{x_3} = \pm\frac{1}{\sqrt{x_1}\sqrt{x_2}}$. Or $\sqrt{x_1}, \sqrt{x_2}$ sont de degré au plus 2 sur $\mathbb{Q}(x_1, x_2, x_3) = C_d$. Donc :

$$[L_d : \mathbb{Q}] = [L_d : C_d][C_d : \mathbb{Q}] = 3[L_d : C_d] \leq 4 \times 3 = 12 \ .$$

e) Soit P le polynôme minimal de θ_d sur $\mathbb{Q}$. Comme $K_d \geq C_d$, $3|[K_d : \mathbb{Q}] \leq 6$ donc $[K_d : \mathbb{Q}] = 3$ ou 6. Si f_d est réductible sur $\mathbb{Q}$ alors c'est 3. Donc qu'il existe $a, b, c \in \mathbb{Z}$ tels que $h(X) := X^3 + aX^2 + bX + c$ est le polynôme minimal de θ_d sur $\mathbb{Q}$. On a $f_d(-\theta_d) = g_d(\theta_d^2) = f_d(\theta_d) = 0$. Or $-h(-X)$ est le polynôme minimal de $-\theta_d$ sur $\mathbb{Q}$. Comme $-h(-X) \neq h(X)$ (coefficient constant non nul !), ils sont premiers entre eux etles deux divisent $f_d(X) = f_d(-X)$. Donc pour des raisons de degrés : $f_d(X) = -h(X)h(-X)$ *i.e.*

$$X^6 + 2d + 2X^4 + (2d-1)X^2 - 1 = X^6 + (2b - a^2)X^4 + (b^2 - 2ac)X^2 - c^2$$

. D'où :

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

on a donc $3 = (2d + 2 - (2d - 1)) = -a^2 - b^2 + 2b + 2ac = -(b-1)^2 - (a-c)^2 + 2 \Rightarrow (b-1)^2 + (a-c)^2 = -1$ absurde ! *Donc f_d est irréductible sur $\mathbb{Q}$.*

f) On a donc $[K_d : \mathbb{Q}] = 6$ et donc $[L_d : \mathbb{Q}] = 6$ ou 12 car $6|[L_d : \mathbb{Q}] \leq 12$.

g) On a $|G_d/N| = [C_d : \mathbb{Q}] = 3$ donc $|N|$ est bien la plus grande puissance de 2 qui divise $|G_d| = 6$ ou 12. D'où N est un $2-$Sylow. Comme $C_d/\mathbb{Q}$ est galoisienne, $N \triangleleft G_d$, c'est le seul.

h) Les racines de f_d sont $\pm\sqrt{x_i}$, $i = 1, 2, 3$. On a :

$$\begin{aligned} \mathrm{disc}(f_d) = &(\sqrt{x_1} - \sqrt{x_2})^2(\sqrt{x_1} + \sqrt{x_2})^2(-\sqrt{x_1} - \sqrt{x_2})^2(-\sqrt{x_1} + \sqrt{x_2})^2 \\ &(\sqrt{x_2} - \sqrt{x_3})^2(\sqrt{x_2} + \sqrt{x_3})^2(-\sqrt{x_2} - \sqrt{x_3})^2(-\sqrt{x_2} + \sqrt{x_3})^2 \\ &(\sqrt{x_1} - \sqrt{x_3})^2(\sqrt{x_1} + \sqrt{x_3})^2(-\sqrt{x_1} - \sqrt{x_3})^2(-\sqrt{x_1} + \sqrt{x_3})^2 \\ &(\sqrt{x_1} + \sqrt{x_1})^2(\sqrt{x_2} + \sqrt{x_2})^2(\sqrt{x_3} + \sqrt{x_3})^2 \\ = &\, 8^2 x_1 x_2 x_3 (x_1 - x_2)^4 (x_2 - x_3)^4 (x_1 - x_3)^4 = 8^2 \mathrm{disc}(g_d)^2 \ . \end{aligned}$$

Donc $G_d \leq \mathfrak{A}_6$.

i) Dans $\mathfrak{S}_6$ les éléments d'ordre 6 sont les $6-$cycles et les produits d'un $3-$cycle et d'une transposition à supports disjoints. Ces éléments ont -1 pour signature ! Donc s'il n'y a qu'un seul $3-$Sylow H dans G, on a $G_d = N \times H = N \times H$ et donc G_d a au moins un élément d'ordre 6 ce qui est absurde car $G_d \leq \mathfrak{A}_6$. Donc les $3-$Sylow de G_d (qui sont d'ordre 3 ne sont pas distingués dans G_d.

j) Si H n'est pas distingué, alors l'extension L_d^H n'est pas galoisienne sur $\mathbb{Q}$. Donc $[L_d : \mathbb{Q}] = \underbrace{[L_d : L_d^H]}_{=3}\underbrace{[L_d^H : \mathbb{Q}]}_{>2} = 12$. Soit $x \in L_d$ tel que $L_d^H = \mathbb{Q}(x)$. Soit P le polynôme minimal de x sur $\mathbb{Q}$. Soit M le corps de décomposition de P sur $\mathbb{Q}$. Puisque $\mathbb{Q}(x)/\mathbb{Q}$ n'est pas normale, on a : $\mathbb{Q} \leq \mathbb{Q}(x) < M \leq L_d$. Pour des raisons de degrés, $M = L_d$.

k) Donc G_d est d'ordre 12 isomorphe à un sous-groupe de $\mathfrak{S}_4$ (via son action sur les racines de $P(X)$) c'est donc $\mathfrak{A}_4$, seul sous-groupe de $\mathfrak{S}_4$ d'ordre 12. Si $\mathbb{Q} \leq C' \leq K_d$ est un corps intermédiaire strict, $[C' : \mathbb{Q}] = 2$ ou 3. Si c'est 3, $C' = C_d$, car $\mathrm{Gal}(L_d/C') = \mathrm{Gal}(L_d/C') =$ le seul sous-groupe d'ordre 4 de G_d. Si c'est 2, alors $\mathrm{Gal}(L_d : C')$ est un sous-groupe d'indice 2 dans $\mathfrak{A}_4$ ce qui n'existe pas !

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

a) Notons $p = \mathrm{ppcm}(m, n)$. on a : $\zeta_p^{p/m} = \zeta_m$. Donc $\zeta_m \in \mathbb{Q}(\zeta_p)$. De même $\zeta_n \in \mathbb{Q}(\zeta_p)$ donc $\mathbb{Q}(\zeta_m, \zeta_n) \leq \mathbb{Q}(\zeta_{\mathrm{ppcm}(m,n)})$. Réciproquement, comme p/m et p/n sont premiers entre eux, on peut trouver u, v entiers tels que :

$$up/m + vp/n = 1 \textit{i.e. } 1/p = u/m + v/n$$

d'où $\zeta_p = \zeta_m^u \zeta_n^v \in \mathbb{Q}(\zeta_m, \zeta_n)$ et $\mathbb{Q}(\zeta_m, \zeta_n) \leq \mathbb{Q}(\zeta_{\mathrm{ppcm}(m,n)})$.

b) Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n)/\mathbb{Q}(\zeta_n))$ est l'identité sur $\mathbb{Q}(\zeta_m)$, alors $\sigma(\zeta_m) = \zeta_m$ et $\sigma(\zeta_n) = \zeta_n$ donc $\sigma = 1$ et le noyau du morphisme est trivial ; d'où l'injectivité. Il est clair que $\mathbb{Q}(\zeta_m)^I \geq \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Si $x \in \mathbb{Q}(\zeta_m)^I$, alors pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n)/\mathbb{Q}(\zeta_n))$, $\sigma(x) = x$ donc $x \in \mathbb{Q}(\zeta_n) \Rightarrow x \in \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. On a donc bien $\mathbb{Q}(\zeta_m)^I = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Par la correspondance de Galois, on a :

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^I) = I = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$$

d'où la surjectivité.

c) Posons $d = \mathrm{pgcd}(m, n)$. On a $\zeta_d = \zeta_m^{m/d} = \zeta_n^{n/d} \in \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Donc $\mathbb{Q}(\zeta_d) \leq \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Or, d'une part :

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)] = \frac{[\mathbb{Q}(\zeta_m) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_d) : \mathbb{Q}]} = \frac{\varphi(m)}{\varphi(d)}$$

et d'autre part,

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_n)]$$

$$= \frac{\varphi(p)}{\varphi(n)} \ .$$

Il suffit donc de montrer que $\frac{\varphi(m)}{\varphi(d)} = \frac{\varphi(p)}{\varphi(n)}$ *i.e.* $\varphi(m)\varphi(n) = \varphi(p)\varphi(d)$.

Or, on a :

$$\varphi(m)\varphi(n) = m \prod_{\substack{q \text{ premier} \\ q|m}} (1-1/q).n \prod_{\substack{q \text{ premier} \\ q|n}} (1-1/q)$$

$$= mn \prod_{\substack{q \text{ premier} \\ q|m \text{ et } q|n}} (1-1/q)^2 \prod_{\substack{q \text{ premier} \\ q|m \text{ et } q\not|n \text{ ou } q|n \text{ et } q\not|m}} (1-1/q)$$

$$= pd \prod_{q|d} (1-1/q)^2 \prod_{\substack{q \text{ premier} \\ q|p \text{ et } q\not|d}} (1-1/q)$$

$$= \varphi(p)\varphi(d) \ .$$

d) Il est clair que ζ est entier sur $\mathbb{Z}$ car ζ est annulé par $X^{p^r} - 1$. Donc $\zeta \in \mathcal{O}_K \Rightarrow \mathbb{Z}[\zeta] \leq \mathcal{O}_K$.

e) Les conjugués de ζ (sur $\mathbb{Q}$) sont les ζ^i, $1 \leq i \leq p^r$, i premier à p. Donc $N_{K/\mathbb{Q}}(1-\zeta) = \prod_{\substack{i=1 \\ p\not|i}}^{p^r} (1-\zeta^i) = \Phi_{p^r}(1)$ où $\Phi_{p^r} = \prod_{\substack{i=1 \\ p\not|i}}^{p^r} (X-\zeta^i) \in \mathbb{Z}[X]$ est le polynôme minimal de ζ sur $\mathbb{Q}$. Or, x est une racine primitive p^r-ème de l'unité $\Leftrightarrow$ $x^{p^{r-1}}$ est une racine $p-$ème de l'unité. Donc $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$ (l'un divise l'autre et les degrés sont les mêmes !). Donc $N_{K/\mathbb{Q}}(1-\zeta) = \Phi_{p^r}(1) = p$. Comme la norme est multiplicative, si $1-\zeta$ était inversible dans $\mathcal{O}_K$, alors $N_{K/\mathbb{Q}}(1-\zeta)$ serait un entier inversible *i.e.* ± 1 et ce n'est pas le cas ! Donc l'idéal $(1-\zeta)$ de $\mathcal{O}_K$ est propre et $(1-\zeta) \cap \mathbb{Z}$ est un idéal propre de $\mathbb{Z}$ qui contient p. En effet, $p = (1-\zeta)\prod_{\substack{i=2 \\ p\not|i}}^{p^r} (1-\zeta^i)$. Comme l'idéal $p\mathbb{Z}$ est maximal dans $\mathbb{Z}$, on a $(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$.