Corrigé de l'examen de rattrapage de théorie de Galois du mercredi 26 juin 2013

Exercice 1 *a)* X^8-2 *a pour racines* $\zeta^i\sqrt[8]{2}$, $0\leq i\leq 7$, *où* $\zeta:=e^{2i\pi/8}=e^{i\pi/4}=\frac{1+i}{\sqrt{2}}$. *Donc* $K=\mathbb{Q}(\sqrt[8]{2},\zeta)=\mathbb{Q}(\sqrt[8]{2},i)$ *car* $\sqrt{2}=(\sqrt[8]{2})^4$. *On a :* $[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt[8]{2})(i):\mathbb{Q}(\sqrt[8]{2})][\mathbb{Q}(\sqrt[8]{2}):\mathbb{Q}]=2.8=16$ *car* $i\notin\mathbb{Q}(\sqrt[8]{2})$ *et* X^8-2 *est irréductible sur* $\mathbb{Q}$ *(par Eisenstein).*

b) On pose $\alpha:=\sqrt[8]{2}$. *Comme* $[K:K_1]=8$, *le polynôme* X^8-2 *est irréductible sur* K_1. *Il existe donc un* K_1-*automorphisme* $\sigma:K\to K$ *tel que* $\sigma(\alpha)=\zeta\alpha$. *Alors* $\sigma(\sqrt{2})=\sigma(\alpha^4)=(\zeta\alpha)^4=-\sqrt{2}$. *Donc* $\sigma(\zeta)=-\zeta$ *et par récurrence, pour tout* i, $\sigma^i(\alpha)=(-\zeta)^i\alpha$. *Donc* σ *est d'ordre* 8 *dans* $\mathrm{Gal}(K/K_1)$ *et* $\mathrm{Gal}(K/K_1)=\langle\sigma\rangle\simeq\mathbb{Z}/8\mathbb{Z}$.

Soit $c:z\mapsto\overline{z}$ *la conjugaison complexe. On a* $c\in\mathrm{Gal}(K/K_2)$. *Soit* $\sigma\in\mathrm{Gal}(K/K_1)$ *tel que* $\sigma(\alpha)=\zeta^2\alpha=i\alpha$. *Alors,* $\sigma(\sqrt{2})=\sigma(\alpha^4)=(i\alpha)^4=\sqrt{2}$. *Donc* $\sigma\in\mathrm{Gal}(K/K_2)$. *On a :* $\sigma^j(\alpha)=i^j\alpha$ *pour tout* j. *Donc* σ *est d'ordre* 4 *dans* $\mathrm{Gal}(K/K_2)$. *On a* $c^2=1$ *dans* $\mathrm{Gal}(K/K_2)$. *On a aussi* $c\sigma c^{-1}(\alpha)=-i\alpha=\sigma^3(\alpha)$, $c\sigma c^{-1}(i)=\sigma^3(i)=i$ *donc* $c\sigma c^{-1}=sigma^{-1}$ *dans* $\mathrm{Gal}(K/K_2)$. *De plus,* $c\notin\langle\sigma\rangle$ *(par exemple, parce que* $c(i)=-i$ *et* $\sigma(i)=i$*). Donc* $\langle c,\sigma\rangle$ *est d'ordre* >4 *et* $\mathrm{Gal}(K/K_2)=\langle c,\sigma\rangle$.

Or le groupe D_8 *a une présentation de la forme :*

$$D_8=\langle a,b\ :\ a^4=b^2=1,\ bab^{-1}=a^{-1}\rangle\ .$$

Il existe donc un morphisme de groupes : $D_8\to\mathrm{Gal}(K/K_2)$, $a\mapsto\sigma$, $b\mapsto c$. *Ce morphisme est surjectif donc c'est un isomorphisme car* $|D_8|=|\mathrm{Gal}(K/K_2)=8$.

Il existe $\sigma_1\in\mathrm{Gal}(K/K_1)$ *tel que* $\sigma(\alpha)=i\alpha$. *On a alors* $\sigma(\sqrt{2})=\sqrt{2}$ *donc* $\sigma\in\mathrm{Gal}(K/K_3)$ *et dans* $\mathrm{Gal}(K/K_3)$, *on a :* $\sigma^2(\alpha)=-\alpha$ *et* $\sigma^2(i)=i$. *Il existe* $\sigma\in\mathrm{Gal}(K/K_1)$ *tel que* $\sigma(\alpha)=\zeta\alpha$. *On pose* $\sigma_2=\sigma c$. *On a* $\sigma_2(i\sqrt{2})=(-i)(-\sqrt{2})=i\sqrt{2}$. *Donc* $\sigma_2\in\mathrm{Gal}(K/K_3)$. *On a de plus,* $\sigma_2^2(i)=i$ *et* $\sigma_2^2(\alpha)=\sigma_2(\zeta\alpha)=\zeta^4\alpha=-\alpha$. *Donc* $\sigma_1^2=\sigma_2^2\in\mathrm{Gal}(K/K_3)$. *De plus,* $\sigma_1\sigma_2(\alpha)=\sigma_1(\zeta\alpha)=\zeta^3\alpha$ *et* $\sigma_1\sigma_2(\zeta)=\zeta^3$. *Donc* $(\sigma_1\sigma_2)^2(i)=\sigma_1\sigma_2(\zeta^6)=\zeta^{18}=\zeta^2=i$ *et* $(\sigma_1\sigma_2)^2(\alpha)=-\alpha$.
donc $(\sigma_1\sigma_2)^2=\sigma_1^2=\sigma_2^2$.
Il existe donc un morphisme de groupes $Q_8\to\mathrm{Gal}(K/K_3)$, $a\mapsto\sigma_1$, $b\mapsto\sigma_2$. *Or* σ_1 *est d'ordre* 4, σ_2 *aussi et* $\sigma_2\neq\sigma_1^{\pm1}$ *(car* $\sigma_1(\zeta)=\zeta$ *et* $\sigma_2(\zeta)=\zeta^3$*). Donc le groupe* $\langle\sigma_1,\sigma_2\rangle$ *est d'ordre* >4. *Comme* $\mathrm{Gal}(K/K_3)$ *est d'ordre* 8, $\mathrm{Gal}(K/K_3)=\langle\sigma_1,\sigma_2\rangle$ *et le morphisme ci-dessus est surjectif; c'est donc un isomorphisme*

Exercice 2 *Sur* $\mathbb{F}_2$ *les polynômes irréductibles de degré* ≤ 3 *sont :* $X, X+1, X^2+X+1, X^3+X+1, X^3+X^2+1$. *Donc* $X^8+X=X(X+1)(X^3+X+1)(X^3+X^2+1)$ *(une racine* x *de* X^3+X^2+1 *par exemple est dans* $\mathbb{F}_8$ *donc vérifie* $x^8+x=0$ *et donc* $X^3+X^2+1|X^8+X$ *sur* $\mathbb{F}_2$.

Exercice 3 *a) Un* $\mathbb{C}-$*automorphisme de* $\mathbb{C}(X)$ *est entièrement déterminé par son image de* X. *Il est clair que* $\sigma^3(X)=j^3X$ *et* $\tau^2(X)=X^{-1^{-1}}=X$. *De plus,* $\tau\sigma\tau^{-1}(X)=(jX^{-1})^{-1}=j^2X=\sigma^{-1}(X)$. *Or le groupe diédral d'ordre* 6 *a une présentation :*

$$D_6=\langle a,b\ :\ a^3=b^2=1,\ bab^{-1}=a^{-1}\rangle\ .$$

Il existe donc un morphisme surjectif $D_6 \to G$, $a \mapsto \sigma$, $b \mapsto \tau$. Comme $\tau \notin \langle\sigma\rangle$, l'ordre de G est ≥ 6. Donc le morphisme ci-dessus est un isomorphisme.

b) Le polynôme $T^6 - T^3(X^3 + X^{-3}) + 1 \in \mathbb{C}(X^3 + X^{-3})[T]$ annule X donc $[E : \mathbb{C}(X^3 + X^{-3})] = [\mathbb{C}(X^3 + X^{-3})(X) : \mathbb{C}(X^3 + X^{-3})] \leq 6$. Or, $\mathbb{C}(X^3 + X^{-3}) \leq E^G \leq E$ et $[E : E^G] = |G| = 6$. Donc $E^G = \mathbb{C}(X^3 + X^{-3})$.

Exercice 4 *a) Dans A_5, il y a $6-$ $5-$Sylow ($n_5 = 1 \bmod 5$, $n_5|12$ et $n_5 > 1$ car $\mathfrak{A}_5$ est simple. L'ensemble des $5-$Sylow est une orbite pour l'action par conjugaison de $\mathfrak{A}_5$. Donc $n_5 = |\mathfrak{A}_5|/|N|$. Or, $|\mathfrak{A}_5| = 60$ donc $|N| = 10$. Soit $s := (12345)$ soit $t := (14)(23)$. On a $tst^{-1} = s^{-1}$ donc $t \in N$ et $N = \langle s, t\rangle$ pour des raisons de cardinaux.*

b) $P(X-2) = X^5 - 10X^4 + 40X^3 - 80X^2 + 75X - 10$ qui est irréductible sur $\mathbb{Q}$ par Eisenstein. Donc P aussi.

c) Dans $\mathbb{F}_3[X]$, on a : $P = X^5 + X = X(X^2 - X - 1)(X^2 + X - 1)$ où $X^2 \pm X - 1$ sont irréductibles sur $\mathbb{F}_3$. Donc G contient une double-transposition.

d) Soit Δ le discriminant de P :

$$\Delta = P'(x_1)P'(x_2)P'(x_3)P'(x_4)P'(x_5)$$

si les x_i sont les racines de P. Donc $\Delta = \prod_{i=1}^5 (5x_i^4 - 5) = 5^5 \prod_{i=1}^5 (x_i^4 - 1)$. Or, $x_i^4 - 1 = 4 - 12/x_i = (4/x_i)(x_i - 3)$. Donc $\Delta = \frac{-5^5 4^5 \prod_{i=1}^5 (3-x_i)}{\prod_{i=1}^5 x_i} = 5^5.4^5/12P(3) = 5^2.4^6$ qui est un carré dans $\mathbb{Q}$. Donc $G \leq \mathfrak{A}_5$.

e) Comme P est irréductible, G agit transitivement sur l'ensemble des racines de P et $5||G|$. Or G contient une double transposition donc $2|\,|G|$. Donc $10|\,|G|$ et $|G| = 10, 20, 30,$ ou 60 car $|G|\,|\,|\mathfrak{A}_5| = 60$.

f) Un sous-groupe d'indice 2 est distingué or $\mathfrak{A}_5$ est simple donc $|G| \neq 30$. Si $|G| \leq 20$, le nombre m de $5-$Sylow dans G vérifie : $m = 1 \bmod 5$ et $m|\,|G|/5 \leq 4$. Mais alors $m = 1$ donc l'unique $5-$Sylow de G est distingué dans G i.e. G est contenu dans le normalisateur (dans $\mathfrak{A}_5$) d'un $5-$Sylow. Or un tel normalisateur est d'ordre 10 donc $G \simeq N$. Or le groupe D_{10} a une présentation :

$$\langle a, b \,:\, a^5 = b^2 = 1,\, bab^{-1} = a^{-1}\rangle$$

et il existe un morphisme surjectif $D_{10} \to N$, $a \mapsto s$, $b \mapsto t$. C'est forcément un isomorphisme. Donc si $G \neq \mathfrak{A}_5$, $|G| = 10$ ou 20 et d'après ce qui précède $G \simeq N \simeq D_{10}$.

g) Les coefficients de R sont symétriques en les r_i donc s'expriment comme des polynômes (à coefficients entiers) en les polynômes symétriques élémentaires spécialisés en les r_i. Or, les polynômes symétriques élémentaires spécialisés en les r_i sont $\pm$ les coefficients de P. Donc les coefficients de R sont entiers. Le coefficient dominant est 1 et $\deg R = \binom{5}{2} = 10$. Les r_i sont deux à deux distinctes car P est irréductible sur $\mathbb{Q}$ donc séparable ($\mathrm{car}\mathbb{Q} = 0$).

h) Si $G = \mathfrak{A}_5$, alors l'action de G sur l'ensemble $\{r_i : 1 \leq i \leq 5\}$ est $2-$transitif. Or, si $\sigma \in G$, si $r_1 + r_2$, par exemple, est une racine de $X^5 - 5X^3 - 10X^2 + 30X - 36$, $r_{\sigma(1)} + r_{\sigma(2)}$ aussi donc l'action de G sur l'ensemble $\{r_i : 1 \leq i \leq 5\}$ n'est pas $2-$transitive. Donc $G \neq \mathfrak{A}_5$ et $G \simeq D_{10}$.

Exercice 5 *a)* $\Phi_{11}(X) = X^{10} + X^9 + ... + X + 1$. *Les racines de* Φ_{11} *dans* $\mathbb{C}$ *sont* $z, ..., z^{10}$. *Donc* $\mathbb{Q}(z)$ *est le corps de décomposition de* Φ_{11} *sur* $\mathbb{Q}$ *(dans* $\mathbb{C}$*). Donc* $\mathbb{Q}(z)/\mathbb{Q}$ *est galoisienne. De plus* $[\mathbb{Q}(z) : \mathbb{Q}] = \varphi(11) = 10$. *Le groupe de Galois est isomorphe à* $(\mathbb{Z}/11\mathbb{Z})^\times$, *cyclique car* 11 *est premier.*

b) *Comme* $z + z^{-1} = 2\cos(2\pi/11) \in \mathbb{R}$, *on a* $\mathbb{Q}(z + z^{-1}) \leq \mathbb{Q}(z) \cap \mathbb{R} \leq \mathbb{Q}(z)$. *Or,* z *est racine du polynôme* $(X - z)(X - z^{-1}) = X^2 - (z + z^{-1})X + 1 \in \mathbb{Q}(z + z^{-1})[X]$ *; donc* $[\mathbb{Q}(z) : \mathbb{Q}(z + z^{-1})] \leq 2$ *et* $[\mathbb{Q}(z) : \mathbb{Q}(z + z^{-1})] = 2$ *car* $\mathbb{Q}(z) \neq \mathbb{Q}(z + z^{-1})$. *On a donc forcément* $\mathbb{Q}(z + z^{-1}) = \mathbb{Q}(z) \cap \mathbb{R}$.

c) *On a* $z + z^{-1} = 2\cos(2\pi/11)$ *et* $[\mathbb{Q}(z + z^{-1}) : \mathbb{Q}] = [\mathbb{Q}(z) : Q]/[\mathbb{Q}(z) : \mathbb{Q}(z+z^{-1})] = 5$. *Soit* P *le polynôme minimal de* $z+z^{-1}$ *sur* $\mathbb{Q}$. *On a* $\deg P = [\mathbb{Q}(z + z^{-1}) : \mathbb{Q}] = 5$. *Or :*

$$1 + z + ... + z^{10} = 0 \Rightarrow z^{-5} + ... + 1 + ... + z^5 = 0$$

$$\Rightarrow 1 + (z + z^{-1}) + z^2 + z^{-2} + ... + z^5 + z^{-5} = 0 \ .$$

Or, si on pose $Z := z + z^{-1}$, $z^2 + z^{-2} = Z^2 - 2$, $z^3 + z^{-3} = Z^3 - 3Z$, *etc*
On a donc : $Z^5+Z^4-4Z^3-3Z^2+3Z+1 = 0$. *D'où :* $P = X^5+X^4-4X^3-3X^2+3X+1$. *L'extension* $\mathbb{Q}(z+z^{-1})/\mathbb{Q}$ *est galoisienne (car* $\mathbb{Q}(z)/\mathbb{Q}$ *est galoisienne cyclique (et donc* $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}(z + z^{-1}))$ *est distingué dans* $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$*) de groupe de Galois isomorphe à* $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}(z + z^{-1})) \simeq \mathbb{Z}/5\mathbb{Z}$. *Comme* $\mathbb{Q}(z+z^{-1})/\mathbb{Q}$ *est galoisienne,* $\mathbb{Q}(z+z^{-1})$ *est le corps de décomposition de* P *sur* $\mathbb{Q}$ *(dans* $\mathbb{C}$*). Donc* $\mathrm{Gal}_{\mathbb{Q}}(P) \simeq \mathbb{Z}/5\mathbb{Z}$.