Corrigé de l'examen final de Théorie de Galois du 27 mai

Exercice 1 *a)* $[\mathbb{F}_q(X):\mathbb{F}_q(X)^G]=|G|=|\mathbb{F}_q^\times||\mathbb{F}_q|=q(q-1)$.

b) *Le polynôme* $P(T)-P(X)\in\mathbb{F}_q(P)[T]$ *est de degré* $\deg P=q(q-1)$ *et annule* X *donc* $[\mathbb{F}_q(X):\mathbb{F}_q(P)]\leq q(q-1)$. *Or* $P(aX+b)=(a^qX^q+b^q-aX-b)^{q-1}=a^{q-1}(X^q-X)^{q-1}=P(X)$ *car* $a\in\mathbb{F}_q^\times\Rightarrow a^{q-1}=1$ *et* $b\in\mathbb{F}_q\Rightarrow b^q=b$. *Donc* $\mathbb{F}_q(P)\leq\mathbb{F}_q(X)^G\leq\mathbb{F}_q(X)$ *donc :*

$$q(q-1)\geq[\mathbb{F}_q(X):\mathbb{F}_q(P)]\geq[\mathbb{F}_q(X):\mathbb{F}_q(X)^G]=q(q-1)$$

et $[\mathbb{F}_q(X):\mathbb{F}_q(P)]=[\mathbb{F}_q(X):\mathbb{F}_q(X)^G]\Rightarrow\mathbb{F}_q(P)=\mathbb{F}_q(X)^G$.

c) *De même que précédemment :* $[\mathbb{F}_q(X):\mathbb{F}_q(X^q-X)]\leq q=|H|=[\mathbb{F}_q(X):\mathbb{F}_q(X)^H]$ *or,* $(X+b)^q-(X+b)=X^q-X\Rightarrow\mathbb{F}_q(X^q-X)\leq\mathbb{F}_q(X)^H\leq\mathbb{F}_q(X)\Rightarrow\mathbb{F}_q(X)^H=\mathbb{F}_q(X^q-X)$.

Exercice 2 *a)* *Comme* $\sqrt{2}^2\in\mathbb{Q},\sqrt{3}^2\in\mathbb{Q}$, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]\leq 4$. *Si* $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$, *alors* $\sqrt{3}=a+b\sqrt{2}$, $a,b\in\mathbb{Q}$. *Donc* $3=a^2+2\sqrt{2}ab+2b^2\Rightarrow ab=0$ *car* $\sqrt{}\notin\mathbb{Q}$. *Si* $b=0,\sqrt{3}\in\mathbb{Q}$ *absurde ! si* $a=0$, $\sqrt{3}/\sqrt{2}\in\mathbb{Q}$ *absurde ! Donc* $[\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}]=4$.

b) $N_{F/\mathbb{Q}(\sqrt{2})}(a)=(2+\sqrt{2})^2(3+\sqrt{3})(3-\sqrt{3})=6(2+\sqrt{2})^2=3\sqrt{2}^2(2+\sqrt{2})^2$ *qui n'est pas un carré dans* $\mathbb{Q}(\sqrt{2})$ *car* $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. *Si* a *est un carré dans* F, *alors* $a=\alpha^2$ *avec* $\alpha\in F$. *Mais alors* $N_{F/\mathbb{Q}(\sqrt{2})}(a)=N_{F/\mathbb{Q}(\sqrt{2})}(\alpha)^2$ *serait un carré dans* $\mathbb{Q}(\sqrt{2})$ *: absurde !*

c) $[E:\mathbb{Q}]=[F(\alpha):F][F:\mathbb{Q}]=4[F(\alpha):F]$ *; or,* $\alpha^2=a\in F$ *et* $\alpha\notin F$. *Donc* $[F(\alpha):F]=2$ *et* $[E:\mathbb{Q}]=8$. *Les racines du polynôme minimal de* α *sur* $\mathbb{Q}$ *sont les :*

$$\sigma(\alpha)$$

où σ *décrit les morphismes de corps* $\sigma:E\to\mathbb{C}$. *Si* σ *est un tel morphisme,* $\sigma(\alpha)^2=\sigma(a)=(2+\sigma(\sqrt{2}))(3+\sigma(\sqrt{3}))=(2\pm\sqrt{2})(3\pm\sqrt{3})$. *D'où :* $\sigma(\alpha)=\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$ *ce qui fait au plus* 8 *valeurs distinctes.*
Or, α *est de degré* 8 *sur* $\mathbb{Q}$ *donc son polynôme minimal a exactement* 8 *racines ce sont donc les :*

$$\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}\ .$$

d) $\alpha\beta=\sqrt{(2-\sqrt{2})(2+\sqrt{2})(3+\sqrt{3})^2}=\sqrt{2}(3+\sqrt{3})\in F\leq E$ *donc* $\beta\in E$. *De même si on pose* $\gamma:=\sqrt{(2+\sqrt{2})(3-\sqrt{3})}$ *et* $\delta:=\sqrt{(2-\sqrt{2})(3-\sqrt{3})}$, *on trouve :* $\alpha\gamma=(2+\sqrt{2})\sqrt{6}\in F$, $\alpha\delta=2\sqrt{3}\in F$ *donc* $\pm\alpha,\pm\beta,\pm\gamma,\pm\delta\in E$ *et* E *est le corps de décomposition dans* $\mathbb{C}$ *du polynôme minimal de* α *sur* $\mathbb{Q}$. *Comme ce polynôme est séparable sur* $\mathbb{Q}$, *l'extension* $E/\mathbb{Q}$ *est galoisienne.*

e) *Il existe* $\sigma:E\to\mathbb{C}$ *un morphisme de corps tel que* $\sigma(\alpha)=\beta$ *car* β *est une racine du polynôme minimal de* α *sur* $\mathbb{Q}$. *Comme* $E/\mathbb{Q}$ *est galoisienne,* $\sigma(E)=E$ i.e. $\sigma\in G$. *On sait que* $\sigma(\sqrt{2})=\pm\sqrt{2}$, $\sigma(\sqrt{3})=\pm\sqrt{3}$ *et donc* $\sigma(\alpha^2)=(2\pm\sqrt{2})(3\pm\sqrt{3})=\sigma(\alpha)^2=\beta^2=(2-\sqrt{2})(3+\sqrt{3})$. *Or, les nombres*

$$(2\pm\sqrt{2})(3\pm\sqrt{3})$$

sont deux à deux distincts. La seule possibilité est donc : $\sigma(\sqrt{2})=-\sqrt{2}$ *et* $\sigma(\sqrt{3})=\sqrt{3}$. *D'où :* $\sigma(\alpha\beta)=\sigma(\sqrt{2}(3+\sqrt{3}))=-\sqrt{2}(3+\sqrt{3})\Rightarrow\sigma(\beta)=\frac{-\sqrt{2}(3+\sqrt{3})}{\beta}=-\frac{\sqrt{2}\sqrt{3+\sqrt{3}}}{\sqrt{2-\sqrt{2}}}=-\alpha$.

f) *De même il exite* $\tau \in G$ *tel que* $\tau(\alpha) = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$. *On a alors* $\tau(\sqrt{2}) = \sqrt{2}$ *et* $\tau(\sqrt{3}) = -\sqrt{3} \Rightarrow \tau^2(\alpha) = -\alpha$.
Donc $\sigma^2(\alpha) = \tau^2(\alpha) = -\alpha \Rightarrow \sigma^2 = \tau^2$ *dans* G *car* $E = \mathbb{Q}(\alpha)$.
D'un autre côté, on a :

$$\sigma\tau(\alpha) = \sigma\left(\sqrt{2+\sqrt{2}}\sqrt{3-\sqrt{3}}\right) = \frac{\sigma\left(\sqrt{2+\sqrt{2}}\sqrt{3-\sqrt{3}}\alpha\right)}{\sigma(\alpha)}$$

$$= \frac{(2-\sqrt{2})\sqrt{6}}{\sqrt{2-\sqrt{2}}\sqrt{3+\sqrt{3}}}$$

$$= \sqrt{2-\sqrt{2}}\sqrt{3-\sqrt{3}}\ .$$

Donc $(\sigma\tau)^2(\alpha) = \sigma\tau\left(\sqrt{2+\sqrt{2}}\sqrt{3-\sqrt{3}}\right)$

$$= \frac{\sigma\tau\left(\sqrt{2+\sqrt{2}}\sqrt{3-\sqrt{3}}\alpha\right)}{\sigma\tau(\alpha)}$$

$$= \frac{\sigma\tau\left(\sqrt{2}\sqrt{6}\right)}{\sqrt{2-\sqrt{2}}\sqrt{3-\sqrt{3}}}$$

$$= \frac{-\sqrt{2}\sqrt{6}}{\sqrt{2-\sqrt{2}}\sqrt{3-\sqrt{3}}}$$

$$= -\sqrt{2+\sqrt{2}}\sqrt{3+\sqrt{3}} = -\alpha\ .$$

Donc $(\sigma\tau)^2 = \tau^2 = \sigma^2$ *dans* G.

g) *Il existe un morphisme de groupes* $\phi : Q_8 \to G$ *tel que* $\phi(a) = \sigma$, $\phi(b) = \tau$. *Or* $|Q_8| = [E : \mathbb{Q}] = |G| = 8$. *Donc pour montrer que* ϕ *est un isomorphisme, il suffit de montrer que* ϕ *est surjectif* i.e. *que* σ, τ *engendrent* G. *Or* σ *est d'ordre* 4 *et* $\tau \notin \langle\sigma\rangle$ *(car* $\sigma^3(\alpha) = -\sigma(\alpha) = -\beta \neq \tau(\alpha) \Rightarrow \langle\sigma, \tau\rangle = G$*)*

h) $\mathbb{Q}(\sqrt{2}) = E^{\langle\tau\rangle}$, $\mathbb{Q}(\sqrt{3}) = E^{\langle\sigma\rangle}$, $\mathbb{Q}(\sqrt{6}) = E^{\langle\sigma\tau\rangle}$, $F = \mathbb{Q}^{\langle\sigma^2\rangle}$ *(à chaque fois, il y a une inclusion évidente et égalité des degrés).*

Exercice 3 *a) Dans* $\mathbb{F}_2[X]$, *il y a* 4 *polynômes de degré* 2 *:* $X^2, X^2+1 = (X+1)^2, X^2+X = X(X+1), X^2+X+1$. *Seul* X^2+X+1 *est irréductible (car il n'a pas de racine dans* $\mathbb{F}_2$*). Si* X^4+X+1 *était réductible, il aurait une racine (ce qui n'est pas le cas) ou il serait de la forme* PQ *avec* P, Q *irréductibles de degré* 2. *Mais alors, on aurait* $P = Q = X^2+X+1 \Rightarrow X^4+X+1 = (X^2+X+1)^2 = X^4+X^2+1$ *absurde ! Donc* X^4+X+1 *est irréductible sur* $\mathbb{F}_2$ *donc sur* $\mathbb{Z}$, *donc sur* $\mathbb{Q}$. *Dans* $\mathbb{F}_3[X]$, *on a :*

$$X^4+X+1 = (X-1)(X^3+X^2+X-1)$$

où X^3+X^2+X-1 *est irréductible sur* $\mathbb{F}_3$ *car sans racine dans* $\mathbb{F}_3$. *Donc il existe dans le groupe de Galois* G *de* X^4+X+1 *sur* $\mathbb{Q}$, *vu comme sous-groupe de* $\mathfrak{S}_4$, *un* $3-$*cycle. Or le groupe de Galois* G *agit transitivement sur l'ensemble des* 4 *racines de* X^4+X+1. *Donc* $|G|$ *est un multiple de* 4 *et de* 3. *D'où :*

$$12 \ \Big|\ |G| \ \Big|\ 24 = |\mathfrak{S}_4|\ .$$

Mais alors, $G = \mathfrak{A}_4$ ou $\mathfrak{S}_4$. Or si on note Δ le discriminant de $P := X^4 + X + 1 = (X - x_1)(X - x_2)(X - x_3)(X - x_4)$ (x_1, x_2, x_3, x_4 sont les 4 racines de $X^4 + X + 1$ dans $\mathbb{C}$), on a :

$$\Delta = \prod_{1 \leq i < j \leq 4} (x_i - x_j)^2 = P'(x_1)P'(x_2)P'(x_3)P'(x_4)$$

$$= (4x_1^3 + 1)(4x_2^3 + 1)(4x_3^3 + 1)(4x_4^3 + 1)$$

mais, on a : $\forall\, i$, $x_i^4 = -x_i - 1 \Rightarrow x_i^3 = -1 - x_i^{-1}$. D'où :

$$\Delta = \prod_{i=1}^{3}(-3 - 4x_i^{-1}) = 3^4(x_1x_2x_3x_4)^{-1} \prod_{i=1}^{4}(-4/3 - x_i)$$

$$= 3^4 P(-4/3) = 4^4 - 4.3^3 + 1 = 229$$

qui est un nombre premier. Donc Δ n'est pas un carré dans $\mathbb{Q}$ et $G \neq \mathfrak{A}_4 \Rightarrow G = \mathfrak{S}_4$.

b) Soit $P := X^4 + 8X + 12$. Soit Δ son discriminant. Comme dans la question précédente, on a :

$$\Delta = \prod_{i=1}^{4}(4(-6 - 12x_i^{-1})) = 4^4(x_1x_2x_3x_4)^{-1} \prod_{i=1}^{4}(-12 - 6x_i)$$

$$= 6^4.4^4/12P(-2) = 6^4.4^4 = (6^2.4^2)^2$$

qui est bien un carré dans $\mathbb{Q}$. Dans $\mathbb{F}_5[X]$, on a :

$$P = X^4 - 2X + 2 = (X + 1)(X^3 - X^2 + X + 2)$$

et $X^3 - X^2 + X + 2$ est irréductible sur $\mathbb{F}_5$ car $X^3 - X^2 + X + 2$ n'a pas de racines dans $\mathbb{F}_5$. Soit $P = P_1...P_r$ une décomposition de P en facteurs irréductibles unitaires dans $\mathbb{Q}[X]$. Forcément, les P_i sont dans $\mathbb{Z}[X]$. On a donc une décomposition :

$$\overline{P} = \overline{P_1}...\overline{P_r}$$

dans $\mathbb{F}_5[X]$. Nécessairement, il existe $1 \leq i, j \leq r$ tels que $X + 1 \mid \overline{P_i}$ et $X^3 - X^2 + X + 2 \mid \overline{P_j}$ dans $\mathbb{F}_5[X]$. Mais alors $r \leq 2$ et soit P est irréductible soit $r = 2$ et P a un facteur de degré 1 i.e. une racine dans $\mathbb{Q}$ (donc dans $\mathbb{Z}$). Si $a \in \mathbb{Z}$ est une racine de P, alors $a \mid 12$ donc $a = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6,$ ou ± 12. Mais aucun de ces nombres n'est racine de P. Donc P est irréductible sur $\mathbb{Q}$.

Soit G le groupe de Galois de P sur $\mathbb{Q}$, vu comme sous-groupe de $\mathfrak{S}_4$. Comme P est irréductible, $4 \mid |G|$. De plus G contient un $3-$cycle donc $12 \mid G$. Enfin $G \leq \mathfrak{A}_4$ donc $G = \mathfrak{A}_4$.

Exercice 4 *a) Si $\sigma : L_k \to \mathbb{C}$ est un morphisme de corps, alors $\sigma(\sqrt{a_i}) = \pm\sqrt{a_i}$ pour tout i donc $\sigma(L_k) = L_k$ pour tout k. L'extension $L_k/\mathbb{Q}$ est donc normale donc galoisienne.*

b) Pour tout i, si α est pair, $\sqrt{a_i}^\alpha \in \mathbb{Q}$, si α est impair, $\sqrt{a_i}^\alpha \in \mathbb{Q}\sqrt{a_i}$. Comme $L_k = \mathbb{Q}[\sqrt{a_1}, ..., \sqrt{a_k}]$, on en déduit que la famille

$$\sqrt{a_{i_1}...a_{i_r}} \ : \ 0 \leq r \leq k, \ 1 \leq i_1 < ... < i_r \leq k$$

est une famille génératrice de L_k comme $\mathbb{Q}-$espace vectoriel. Cette famille a $\sum_{r=0}^{k} \binom{r}{k} = 2^k = [L_k : \mathbb{Q}]$ éléments. C'est donc une base.

c) Il existe $i_p \in \{i_1, ..., i_r\} \backslash \{j_1, ..., j_s\}$. Comme $[L_k : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a_j} : \substack{1 \leq j \leq k \\ j \neq i_p})(\sqrt{a_{i_p}}) : \mathbb{Q}(\sqrt{a_j} : \substack{1 \leq j \leq k \\ j \neq i_p})] = 2^k$, on a $\sqrt{a_{i_p}} \notin \mathbb{Q}(\sqrt{a_j} : \substack{1 \leq j \leq k \\ j \neq i_p})$. Il existe donc $\sigma : L_k \to \mathbb{C}$ un $\mathbb{Q}(\sqrt{a_j} : \substack{1 \leq j \leq k \\ j \neq i_p})-$morphisme de corps tel que $\sigma(\sqrt{a_{i_p}}) = -\sqrt{a_{i_p}}$. On a forcément : $\sigma(\sqrt{a_{i_1}...a_{i_r}}) = -\sqrt{a_{i_1}...a_{i_r}}$ et $\sigma(\sqrt{a_{j_1}...a_{j_s}}) = \sqrt{a_{j_1}...a_{j_s}}$.

d) Si $\alpha \in L_k$, on a :

$$\alpha = \sum_{r=0}^{k} \sum_{1 \leq i_1 < ... < i_r \leq k} t_{i_1,...,i_r} \sqrt{a_{i_1}...a_{i_r}}$$

pour certains coefficients $t_{i_1,...,i_r} \in \mathbb{Q}$. Si au moins 2 de ces coefficients sont son nuls alors il existe comme ci-dessus $0 \leq r, s \leq k$, $1 \leq i_1 < ... < i_r \leq k$, $1 \leq j_1 ... \leq j_s \leq k$, avec $\{i_1, ..., i_r\} \not\subseteq \{j_1, ..., j_s\}$, tels que :

$$t_{i_1,...,i_r}, t_{j_1,...,j_s} \neq 0 \ .$$

Choisissons σ comme ci-dessus, on trouve :

$$\alpha = ... + t_{j_1,...,j_s} \sqrt{a_{j_1}...a_{j_s}} + ... + t_{i_1,...,i_r} \sqrt{a_{i_1}...a_{i_s}} + ...$$

$$\sigma(\alpha) = ... + t_{j_1,...,j_s} \sqrt{a_{j_1}...a_{j_s}} + ... - t_{i_1,...,i_r} \sqrt{a_{i_1}...a_{i_s}} + ...$$

donc $\sigma(\alpha) \neq \pm\alpha$. En particulier, si on avait $\sqrt{a_{k+1}} \in L_k$, comme pour tout $\sigma \in \mathrm{Gal}(L_k/\mathbb{Q})$, $\sigma(\sqrt{a_{k+1}}) = \pm\sqrt{a_{k+1}}$, on aurait :

$$\sqrt{a_{k+1}} = t\sqrt{a_{i_1}...a_{i_r}}$$

pour un certain $t \in \mathbb{Q}$ et certains $1 \leq i_1 < ... < i_r \leq k$. En élevant au carré, $q^2 a_{k+1} = p^2 a_{i_1}...a_{i_r}$ pour certains entiers p, q premiers entre eux. Comme a_{k+1} est sans facteur carré, $p^2 = 1$ et $a_{k+1} \mid a_{i_1}...a_{i_r}$ ce qui est impossible car les a_i sont deux à deux premiers entre eux.

e) On a donc $[L_{k+1} : \mathbb{Q}] = [L_k(\sqrt{a_{k+1}}) : L_k][L_k : \mathbb{Q}] = 2^{k+1}$ car $1 < [L_k(\sqrt{a_{k+1}}) : L_k] \leq 2$.
On en déduit par récurrence que $[L_n : \mathbb{Q}] = 2^n$.