Examen 2019/2020 - Correction
4M002 - Algèbre et théorie de Galois
Anna Cadoret

Exercice 1.

(1) Par le lemme Chinois on a

$$\begin{aligned}\mathbb{Z}/4\oplus\mathbb{Z}/6\oplus\mathbb{Z}/18\oplus\mathbb{Z}/21 &\simeq (\mathbb{Z}/2)^2\times\mathbb{Z}/4\times(\mathbb{Z}/3)^2\times\mathbb{Z}/3^2\times\mathbb{Z}/7\\ &\simeq (\mathbb{Z}/2\times\mathbb{Z}/3)\times(\mathbb{Z}/2\times\mathbb{Z}/3)\times(\mathbb{Z}/4\times\mathbb{Z}/3^2\times\mathbb{Z}/7)\\ &\simeq \mathbb{Z}/2\times\mathbb{Z}/6\times\mathbb{Z}/6\times\mathbb{Z}/252\end{aligned}$$

avec $6|6|252$.

(2) (a) Soit u un k-endomorphisme de V ayant pour polynôme caractéristique P. Si on munit V de la structure de $k[T]$-module V_u définie par $T\cdot v = u(v)$, on sait par le théorème de structure que V_u s'écrit de façon unique sous la forme

$$V_u \simeq \bigoplus_{1\leq i\leq s_u} k[T]/D_{u,i}$$

avec les $D_{u,i}$, $i=1,\dots,s_u$ des polynômes unitaires dans $k[T]$ tels que $D_{u,1}|D_{u,2}|\cdots|D_{u,s_u}$. De plus, deux k-endomorphismes u,v de V sont semblables si et seulement si $s := s_u = s_v$ et $D_{u,i} = D_{v,i}$, $i=1,\dots,s$. Comme l'action de u sur V_u correspond à la translation par T, le polynôme caractéristique de u vaut $\chi_u = D_{u,1}D_{u,2}\cdots D_{u,s_u}$. La question est donc de déterminer le nombre de suite $D_1,\dots,D_s$ de polynômes unitaires de $k[T]$ telles que $D_1|D_2|\cdots|D_s$ et $P = D_1D_2\cdots D_s$. Par factorialité de $k[T]$, la condition $P = D_1D_2\cdots D_s$ impose que les facteurs irréductibles de $D_1, D_2, \dots, D_s$ soient parmi les $P_1,\dots,P_r$. Ecrivons donc $D_i = P_1^{\alpha_{i,1}}\cdots P_r^{\alpha_{i,r}}$. La condition $D_1|D_2|\cdots|D_s$ impose $\alpha_{1,j}\leq\cdots\leq\alpha_{s,j}$, $j=1,\dots,r$ et la condition $P = D_1D_2\cdots D_s$ impose $\alpha_{1,j}+\cdots+\alpha_{s,j} = \alpha_j$, $j=1,\dots,r$. Autrement dit, les suites $\alpha_{1,j}\leq\cdots\leq\alpha_{s,j}$ possibles sont en bijection avec les partitions de α_j, $j=1,\dots,r$. On en déduit que le nombre de classes de similitude de k-endomorphismes de V ayant pour polynôme caractéristique P est $p(\alpha_1)\cdots p(\alpha_r)$.

(b) Pour $k=\mathbb{Q}$ et $P = T^2(T-1)^3(T+1)$, on a donc $p(2)p(3)p(1) = 2\times 3\times 1 = 6$ classes de similitude de k-endomorphismes de V ayant pour polynôme caractéristique P.

Exercice 2.

(1) D'après le cours (produit tensoriel et somme directe commutent) $T^n(V)$ est de k-dimension d^n.

(2) Par n-k-linéarité du produit tensoriel, l'application $V^n\to T^n(V)$, $(v_1,\cdots,v_n)\to v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(n)}$ est n-k-linéaire donc, par propriété universelle du produit tensoriel, se factorise en un unique morphisme de k-espaces vectoriels $\sigma\cdot : T^n(V)\to T^n(V)$ tel que $\sigma\cdot v_1\otimes\cdots\otimes v_n = v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(n)}$. C'est en fait un isomorphisme, d'inverse $\sigma^{-1}\cdot$.

(3) L'unicité de $S^n(f) : S^n(V)\to W$ sous réserve de son existence résulte du fait que $S^n(f)(\pi_n(v_1\otimes\cdots\otimes v_n)) = f(v_1,\cdots,v_n)$ est uniquement déterminé par f et que $S^n(V)$ est engendré comme k-espace vectoriel par les $\pi_n(v_1\otimes\cdots\otimes v_n)$ puisque $T^n(V)$ l'est par les $v_1\otimes\cdots\otimes v_n$. Pour l'existence, si $f : V^n\to W$ est une application n-k-linéaire symmétrique, elle est en particulier n-k-linéaire donc, par propriété universelle du produit tensoriel, se factorise en un unique morphisme de k-espaces vectoriels $S_0^n(f) : T^n(V)\to W$ tel que $S_0^n(f)(v_1\otimes\cdots\otimes v_n) = f(v_1,\dots,v_n)$. De plus, comme $f : V^n\to W$ est symmétrique, pour tout $\sigma\in\mathcal{S}_n$, $f(\sigma\cdot(v_1,\dots,v_n) - f(v_1,\dots,v_n) = 0$. Mais $f(\sigma\cdot(v_1,\dots,v_n)) = f(v_{\sigma(1)},\dots,v_{\sigma(n)}) = S_0^n(f)(v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(n)}) = S_0^n(f)(\sigma\cdot v_1\otimes\cdots\otimes v_n)$. Autrement dit, $R^n(V)\subset\ker(S_0^n(f))$ et, en particulier, $S_0^n(f) : T^n(V)\to W$ se factorise en un unique morphisme de k-espaces vectoriels $S^n(f) : S^n(V)\to W$ tel que $S^n(f)\circ\pi_n = S_0^n(f)$.

(4) On procède exactement de la même façon en remplaçant $R^n(V)$ par le sous-k-espace vectoriel $R^n_\epsilon(V) \subset T^n(V)$ engendré par les éléments de la forme $\epsilon(\sigma)t - \sigma \cdot t$, $t \in T^n(V)$.

(5) C'est la propriété universelle de $p_n : V^n \to S^n(V)$. (Noter qu'on utilise que k est de caractéristique 0 pour inverser $n!$).

(6) C'est la propriété universelle de $p_n : V^n \to \bigwedge^n(V)$. (Noter qu'on utilise que k est de caractéristique 0 pour inverser $n!$).

(a) Si $e_1, \ldots, e_d$ est une k-base de V, $\underline{e}^{\underline{a}} = e_1^{a_1} \cdot \cdots \cdot e_d^{a_d}$, $a_1 + \cdots + a_d = n$ est une k-base de $S^n(V)$. En effet, la famille $\underline{e}^{\underline{a}}$ est k-génératrice car $S^n(V)$ est engendré par les $e_{i_1} \cdot \cdots \cdot e_{i_n}$, $1 \leq i_1, \ldots, i_n \leq d$ mais que par définition de $S^n(V)$, on a $e_{i_1} \cdot \cdots \cdot e_{i_n} = e_{\sigma(i_1)} \cdot \cdots \cdot e_{\sigma(i_n)}$, $\sigma \in \mathcal{S}_n$. La famille $\underline{e}^{\underline{a}}$, $a_1 + \cdots + a_d = n$ est k-libre car si on a une relation de dépendance k-linéaire

$$\sum_{\underline{a}} \lambda_{\underline{a}} \underline{e}^{\underline{a}} = 0$$

en appliquant s_n on a

$$(*) \quad \frac{1}{n!} \sum_{\underline{a}} \lambda_{\underline{a}} \sum_{\sigma \in \mathcal{S}_n} \sigma \cdot e_1^{\otimes a_1} \otimes \cdots e_d^{\otimes a_d} = 0$$

Mais comme le coefficient de $\underline{e}^{\otimes \underline{a}} := e_1^{\otimes a_1} \otimes \cdots \otimes e_d^{\otimes a_d}$ dans (*) écrit dans la k-base $e_{i_1} \otimes \cdots \otimes e_{i_n}$, $1 \leq i_1, \ldots, i_n \leq d$ de $T^n(V)$ est $\lambda_{\underline{a}}/n!$, on en déduit $\lambda_{\underline{a}} = 0$. Donc $dim_k(S^n(V))$ est le nombre de uplets $\underline{a} = (a_1, \ldots, a_d)$ d'entiers ≥ 0 tels que $a_1 + \cdots + a_d = n$. En développant

$$\frac{1}{(1-X)^d} = (\sum_{n \geq 0} X^n)^d,$$

on obtient l'égalité demandée.

(b) On vérifie immédiatement que $((1-X)^{-d})^{(n)} = d(d+1)\cdots(d+n-1)(1-X)^{-d-n}$. D'où la conclusion en identifiant avec l'égalité de la question précédente.

(7) Comme pour $S^n(V)$, on voit facilement que $\bigwedge^n V$ est engendré comme k-espace vectoriel par les $e_{i_1} \wedge \cdots \wedge e_{i_n}$, $1 \leq i_1 < \cdots < i_n \leq d$ (utiliser que s'il existe $1 \leq i \neq j \leq n$ tel que $v_i = v_j$ alors $v := v_1 \wedge \cdots \wedge v_n = 0$ car $-v = (i,j) \cdot v = v$ donc $2v = 0$ donc $v = 0$ car k est de caractéristique $\neq 2$).

(a) En particulier, si $n > d$, on a $\bigwedge^n V = 0$.

(b) On dispose du déterminant $det_{\underline{e}} : V^d \to k$ dans la base $\underline{e}$. Donc $\bigwedge^d V \neq 0$. Mais $\bigwedge^d V$ est de k-dimension ≤ 1 puisque engendré par $e_1 \wedge \cdots \wedge e_d$. On en déduit que $\bigwedge^d V$ est de k-dimension 1 avec pour k-base $e_1 \wedge \cdots \wedge e_d$.

(c) Il suffit de montrer que si $n < d$, $e_{i_1} \wedge \cdots \wedge e_{i_n}$, $1 \leq i_1 < \cdots < i_n \leq d$ est k-libre. Soit donc

$$\sum_{1 \leq i_1 < \cdots < i_n \leq d} \lambda_{\underline{i}} e_{i_1} \wedge \cdots \wedge e_{i_n} = 0$$

une relation de k-dépendance linéaire. Pour chaque $1 \leq i_1 < \cdots < i_n \leq d$, on note $1 \leq j_1 < \cdots < j_{d-n} \leq d$ l'unique $d-n$-uplet tel que $\{i_1, \ldots, i_n, j_1, \ldots, j_{d-n}\} = \{1, \ldots, d\}$. En appliquant $- \wedge e_{j_1} \wedge \cdots \wedge e_{j_{d-n}}$, on obtient

$$0 = \lambda_{\underline{i}} e_{i_1} \wedge \cdots \wedge e_{i_n} \wedge e_{j_1} \wedge \cdots \wedge e_{j_{d-n}} = \pm \lambda_{\underline{i}} e_1 \wedge \cdots \wedge e_d,$$

ce qui, d'après la question précédente, implique $\lambda_{\underline{i}} = 0$.

(8) L'existence de $s_n \oplus \wedge_n : S^n(V) \oplus \bigwedge^n(V) \hookrightarrow T^n(V)$ est la propriété universelle de la somme directe. De plus, $s_n \oplus \wedge_n(v \oplus w) = s_n(v) + \wedge_n(w) = 0$ si et seulement si $s_n(v) = - \wedge_n (w)$. Mais si $n \geq 2$, on dispose d'au moins une permutation τ de signature -1. En particulier, $- \wedge_n (w) = s_n(v) = \tau \cdot s_n(v) = -\tau \cdot \wedge_n(w) = \wedge_n(w)$ donc $\wedge_n(w) = s_n(v) = 0$ (on a encore utilisé que k est de caractéristique $\neq 2$). Mais $s_n : S^n(V) \to T^n(V)$ et $\wedge_n : \bigwedge^n(V) \to T^n(V)$ sont injectives à cause des relations $\pi_n \circ s_n = Id$,

$\pi_n \circ \wedge_n = Id$. Donc $v = 0$, $w = 0$. Pour $n = 2$, on a $d^2 = \binom{d+1}{2} + \binom{d}{2}$. (On peut vérifier, mais c'est un peu fastidieux, qu'on a toujours $d^n < \binom{d+n-1}{n} + \binom{d}{n}$ pour $3 \leq n < d$).

Problème.

(1) L'extension K/k est galoisienne comme corps de décomposition sur k d'un polynôme séparable sur k. Comme P est à coefficient dans k, pour tout $\sigma \in Gal(K|k)$ on a $\sigma(Z_K(P)) = Z_K(P)$ d'où un morphisme de groupes bien défini $G \to \mathcal{S}(Z_K(P))$, $\sigma \to \sigma_{Z_K(P)} : Z_K(P) \tilde{\to} Z_K(P)$, qui est injectif puisque $K = k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

(2) Un calcul immédiat donne $a_1 - a_2 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$ $a_1 - a_3 = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$ $a_2 - a_3 = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$. Ces éléments sont tous non nuls puisque P est séparable.

(3) On considère l'action de $\mathcal{S}_4$ sur $\{a_1, a_2, a_3\}$ induite par celle de $\mathcal{S}_4$ sur $Z_K(P)$. Puisque $\mathcal{S}_4$ est engendré par $(1,2)$ et $(1,2,3,4)$, pour vérifier que cette action est bien définie, il suffit de vérifier que $(1,2)$ et $(1,2,3,4)$ stabilisent $\{a_1, a_2, a_3\}$. Or on a $(1,2) \cdot a_1 = a_1$, $(1,2,3,4) \cdot a_1 = a_3$, $(1,2) \cdot a_2 = a_3$, $(1,2,3,4) \cdot a_2 = a_2$, $(1,2) \cdot a_3 = a_2$, $(1,2,3,4) \cdot a_3 = a_1$. Cela montre aussi que l'action est transitive. En particulier $[\mathcal{S}_4 : S_i] = |\mathcal{S}_4 \cdot a_i| = 3$ donc $|S_i| = 8$. On vérifie immédiatement que $\tau_i, c_i \in S_i$ donc $D_i \subset S_i$. Par ailleurs, $\langle c_i \rangle \subset D_i$ est un sous-groupe de D_i, normal dans D_i car $\tau_i c_i \tau_i^{-1} = c_i^{-1}$ et distinct de D_i. Autrement dit on a une suite exacte

$$1 \to \langle c_i \rangle \to D_i \to D_i/\langle c_i \rangle \to 1.$$

Comme $\tau_i \notin \langle c_i \rangle$, on a nécessairement $[D_i : \langle c_i \rangle] \geq 2$ donc $|D_i| \geq 8$. D'où $|D_i| = |S_i|$ et $D_i = S_i$.

(4) On a $V_4 \subset S_i = D_i$, $i = 1,2,3$ donc $V_4 \subset D_1 \cap D_2 \cap D_3$. Puisque D_i est d'ordre 8 et $D_i \neq D_j$, $i \neq j$, on a nécessairement $|D_1 \cap D_2 \cap D_3| = 1, 2$ ou 4. Donc nécessairement, $V_4 = D_1 \cap D_2 \cap D_3$. Cela montre déjà que V_4 est un sous-groupe de $\mathcal{S}_4$ puisque c'est une intersection de sous-groupes. Il est contenu dans $\mathcal{A}_4 = \ker(\epsilon_4)$ puisque les transpositions sont de signature -1. Enfin V_4 est normal dans $\mathcal{S}_4$ puisque toute conjuguée d'une double transposition est encore une double transposition.

(5) Tout d'abord, puisque $\mathcal{S}_4$ stablilise $\{a_1, a_2, a_3\}$, $Gal(K|k)$ stabilise *a fortiori* $\{a_1, a_2, a_3\}$ donc K'/k est une sous-etension normale de K/k. Puisque K/k est séparable, K'/k est automatiquement séparable. Donc K'/k est galoisienne. De plus, pour tout $\sigma \in Gal(K|k) \subset \mathcal{S}_4$, $\sigma \in Gal(K|K')$ si et seulement si $\sigma a_i = a_i$, $i = 1,2,3$ *i.e.* si et seulement si $\sigma \in D_1 \cap D_2 \cap D_3 = V_4$. Donc $Gal(K|K') = G \cap V_4$. Par la correspondance de Galois, $K' = K^{G \cap V_4}$ et $G' := Gal(K'|k) = G/G \cap V_4$.

(6) Pour tout orbite $O \subset Z_K(P)$ de G le polynôme $P_O := \prod_{\alpha \in O}(T - \alpha)$ divise P dans $K[T]$ et est à coefficients dans $K^G = k$. Donc si $P \in k[T]$ est irréductible sur k, on a nécessairement $O = Z_K(P)$ puisque P est séparable.

(7) D'après (*), si $G \cap V_4 = \{1\}$ G est soit trivial, soit engendré par une transposition, soit engendré par un 3-cycles. Dans chacun de ces trois cas il n'agit pas transitivement sur $\{1,2,3,4\}$.

(8) Comme $G \cap V_4 \neq \{1\}$, on a $|G \cap V_4| = 2, 4$. Si $|G \cap V_4| = 4$, $V_4 \subset G$ donc, toujours d'après (*), $G = \mathcal{S}_4$, $\mathcal{A}_4$, D_i, $i = 1,2,3$ ou V_4; les valeurs de $[G : G \cap V_4]$ correspondantes sont alors 6, 3, 2 et 1. Si $|G \cap V_4| = 2$ alors $G \cap V_4$ est engendré par une double transposition et, toujours d'après (*), $G = \langle c_i \rangle$, $i = 1,2,3$ ou G est engendré par deux transpositions à support disjoint. Mais dans ce dernier cas, G n'agit pas transitivement sur $\{1,2,3,4\}$. Donc $G = \langle c_i \rangle$, $i = 1,2,3$ et $[G : G \cap V_4] = 2$.

(9) D'après la question (3) $\mathcal{S}_4$ donc *a fortiori* G stabilise $\{a_1, a_2, a_3\}$ donc R est à coeffiients dans $K^G = k$. Par construction, K' est donc le corps de décomposition de R sur k.

(10) En développant $P = \prod_{1\leq i\leq 4}(T-\alpha_i)$, le coefficient de T^{4-j} dans P est $(-1)^j \sum_{1\leq i_1<\cdots<i_j\leq 4} \alpha_{i_1}\cdots\alpha_{i_j}$ et en développant $R = \prod_{1\leq i\leq 3}(T-a_i)$, le coefficient de T^{3-j} dans R est $(-1)^j \sum_{1\leq i_1<\cdots<i_j\leq 3} a_{i_1}\cdots a_{i_j}$. En exprimant les a_i en fonction des α_j, on vérifie les égalités demandées. Par exemple pour le coefficient T^2 dans R on a $-(a_1+a_2+a_3) = -(\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_1\alpha_3+\alpha_2\alpha_4+\alpha_1\alpha_4+\alpha_2\alpha_3) = -(-1)^2\sum_{1\leq i_1<<i_2\leq 4}\alpha_{i_1}\alpha_{i_2} = -b$ *etc.*

(11) (a) $P(T) = T^4 - 4T + 2$ est irréductible sur $\mathbb{Q}$ *e.g.* par Eisenstein avec $p = 2$, $R(T) = T^3 - 8T - 16$ est irréductible sur $\mathbb{Q}$ car sa réduction modulo 5 n'a pas de racine dans $\mathbb{F}_5$. Donc $Gal(K'|\mathbb{Q})$ contient un 3-cycle. En réduisant modulo 3, on a $\overline{R}(T) = (T+1)(T^2-T-1)$ avec T^2-T-1 irréductible car sans racine sur $\mathbb{F}_3$. Donc $Gal(K'|\mathbb{Q})$ contient une transposition; c'est donc $\mathcal{S}_3$. D'après la question (9), $G = \mathcal{S}_4$.

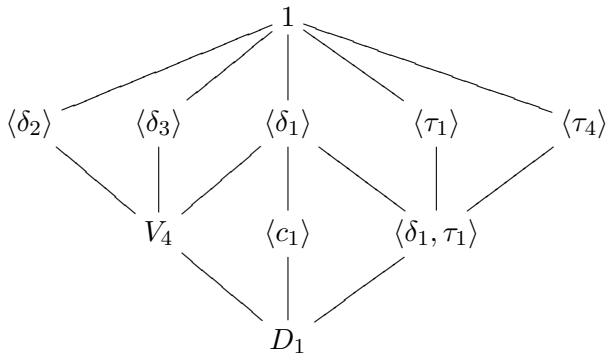
(b) $P(T) = T^4+4T^2+2$ est irréductible sur $\mathbb{Q}$ *e.g.* par Eisenstein avec $p = 2$, $R(T) = T^3-4T^2-8T+32$ a une racine évidente 4 donc se factorise en $R(T) = (T-4)(T^2-8)$ dans $\mathbb{Q}[T]$. Comme $Q(T) := (T^2-8)$ est irréductible de degré 2 sur $\mathbb{Q}$, on en déduit que $K' = \mathbb{Q}[T]/Q = \mathbb{Q}(\sqrt{2})$ est de degré 2 donc $[G : G\cap V_4] = 2$. D'après la question (9), cela correspond à $G \simeq D_i$ ou $G \simeq \mathbb{Z}/4$. Mais on a aussi $P(T) = (T^2)^2 + 4(T^2) + 2 = (T^2+2+\sqrt{2})(T^2+2-\sqrt{2})$ dans $K'[T]$ donc si on note α_1, α_2 les racines de $T^2+2+\sqrt{2}$, on a $Gal(K|K') = \{Id, (1,2)(3,4)\}$ donc $G \simeq \langle(1,2,3,4)\rangle \simeq \mathbb{Z}/4$.

(c) $P(T) = T^4 - 10T^2 + 4$ est irréductible sur $\mathbb{Q}$ car il l'est sur $\mathbb{Z}$. En effet, il n'a pas de racine dans $\mathbb{Z}$ car il n'a pas de racine modulo 3. Si P n'est pas irréductible dans $\mathbb{Z}[T]$, il doit donc se factoriser sous la forme $P(T) = (T^2+aT+b)(T^2+cT+d)$ donc, en développant et en identifiant les coefficients, on devrait avoir $a = -c$, $a^2 = 1+d+b$, $a(d-b) = 0$, $bd = 1$. Donc $b = d = \pm 1$ et $a^2 = 3$ ou -1: contradiction. On a $R(T) = T^3 + 10T^2 - 16T - 160$ a une racine évidente -10 donc se factorise en $R(T) = (T+10)(T-4)(T+4)$ dans $\mathbb{Q}[T]$. En particulier, $[K' : \mathbb{Q}] = 1 = [G : V_4 \cap G]$. D'après la question (9), cela correspond à $G \simeq V_4$.

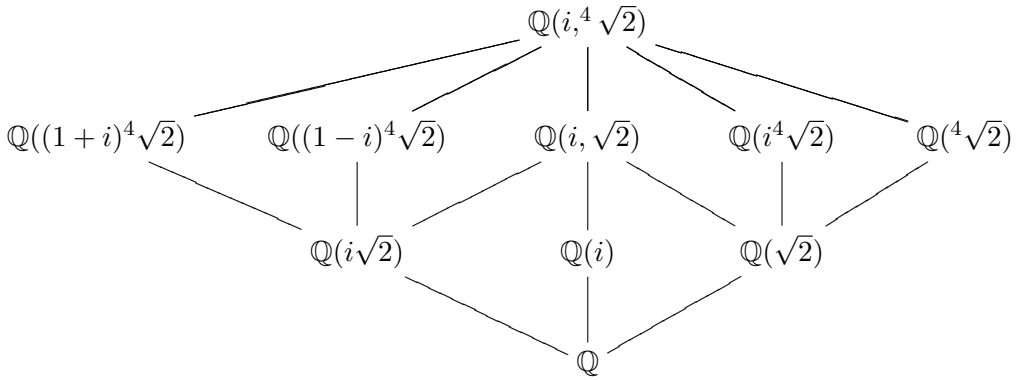
(d) $P(T) = T^4 - 2$ est irréductible sur $\mathbb{Q}$ *e.g.* par Eisenstein avec $p = 2$, $R(T) = T(T^2+8)$. Comme $Q(T) := (T^2+8)$ est irréductible de degré 2 sur $\mathbb{Q}$, on en déduit encore que $K' = \mathbb{Q}[T]/Q = \mathbb{Q}(i\sqrt{2})$ est de degré 2 donc $[G : G\cap V_4] = 2$. D'après la question (9), cela correspond encore à $G \simeq D_i$ ou $G \simeq \mathbb{Z}/4$. Mais cette fois-ci, on peut facilement calculer les racines de P - $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$ donc $K = \mathbb{Q}(i,\sqrt[4]{2})$ et $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \mathbb{Q}(\sqrt[4]{2})(i) : \mathbb{Q}(\sqrt[4]{2})]4 = 8$ puisque le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$ est T^4-2 et le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{2})$ est T^2+1 (qui n'a clairement pas de racines dans $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$).

(12) On peut supposer $i = 1$. Comme D_1 est d'ordre 8, les sous-groupes non triviaux de D_1 sont d'ordre 2 ou 4. Le seul groupe d'ordre 2 est $\mathbb{Z}/2$ et les seuls groupes d'ordre 4 sont $\mathbb{Z}/4$ et $\mathbb{Z}/2\times\mathbb{Z}/2$ (un groupe d'ordre 4 est abélien car soit il est cyclique, soit tous ses éléments sont d'ordre divisant 2). Comme D_1 ne contient que deux éléments d'ordre 4 - c_1 et c_1^{-1}, le seul sous-groupe cyclique d'ordre 4 de D_1 est $\langle c_1\rangle$. Les éléments d'ordre 2 de D_1 sont $\tau_1 = (1,2)$, $\delta_1 = c_1^2 = (1,2)(3,4)$, qui est central puisqu'il commute avec τ_1, $\tau_1 c_1 = \delta_3 = (1,4)(2,3)$, $\tau_1\delta_1 = (3,4) =: \tau_4$, $\tau_1 c_1^{-1} = \delta_2 = (1,3)(2,4)$. On a donc
- 2 sous-groupes isomorphes à $\mathbb{Z}/2\times\mathbb{Z}/2$ - $\langle\delta_1,\tau_1\rangle$, V_4;
- 5 sous-groupes isomorphes à $\mathbb{Z}/2$ - $\langle\delta_1\rangle$, $\langle\delta_2\rangle$, $\langle\delta_3\rangle$, $\langle\tau_1\rangle$, $\langle\tau_4\rangle$.

Avec les relations d'inclusion



(13) Notons $\alpha_1 =^4 \sqrt{2}$, $\alpha_2 = -^4\sqrt{2}$, $\alpha_3 = i^4\sqrt{2}$, $\alpha_4 = -i^4\sqrt{2}$. On a déjà observé que $K' = K^{V_4} = \mathbb{Q}(i\sqrt{2})$. On a deux autres sous-extensions de $K = \mathbb{Q}(i,^4\sqrt{2})$ de degré 2 - $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, dont on vérifie immédiatement qu'elles correspondent respectivement à $\langle c_1\rangle$ et $\langle \delta_1, \tau_1\rangle$ (utiliser *e.g.* $i = \alpha_3/\alpha_1$, $\sqrt{2} = -\alpha_1\alpha_2$). L'extension $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$ est de degré 4 et contient $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$, donc c'est celle fixée par $\langle\delta_1\rangle$ (on peut aussi le vérifier à la main). Les racines de P nous donnent deux autres extensions de degré 4 - $\mathbb{Q}(^4\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(i^4\sqrt{2})/\mathbb{Q}$, dont on vérifie immédiatement qu'elles correspondent respectivement à $\langle\tau_4\rangle$ et $\langle\tau_1\rangle$. Enfin on a $\alpha_1 + \alpha_3 = (1+i)^4\sqrt{2}$ qui est fixé par δ_2 et de degré 4 donc $\mathbb{Q}((1+i)^4\sqrt{2})/\mathbb{Q}$ correspond à $\langle\delta_2\rangle$. De même, $\alpha_1 + \alpha_4 = (1-i)^4\sqrt{2}$ est fixé par δ_3 et de degré 4 donc $\mathbb{Q}((1-i)^4\sqrt{2})/\mathbb{Q}$ correspond à $\langle\delta_3\rangle$. Pour résumer, le diagramme dual obtenu par la correspondance de Galois est:



Les sous-groupes normaux de D_1 sont ceux d'indice 2 et $\langle\delta_1\rangle$; les sous-extensions galoisiennes de $\mathbb{Q}(i,^4\sqrt{2})$ sont donc $\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(i,\sqrt{2}/\mathbb{Q}$. Les éléments $i+\sqrt{2}$ et $i+^4\sqrt{2}$ sont respectivement de degré 4 et 8 (*e.g.* calculer leur orbite sous G) donc sont respectivement primitifs pour $\mathbb{Q}(i,\sqrt{2})$ et $\mathbb{Q}(i,^4\sqrt{2})$.

anna.cadoret@imj-prg.fr
IMJ-PRG- Sorbonne Université.