C. R. Acad. Sci. Paris, t. 308, Série I, p. 33-36, 1989

Algèbre/*Algebra*

$\tilde{D}_4$ et $\hat{D}_4$ comme groupes de Galois

Leila SCHNEPS

Résumé — On construit explicitement des corps ayant $\tilde{D}_4$ ou $\hat{D}_4$ comme groupe de Galois.

$\tilde{D}_4$ and $\hat{D}_4$ as Galois groups

Abstract — *Explicit fields having $\tilde{D}_4$ or $\hat{D}_4$ as Galois groups are constructed.*

Soit H un groupe fini, et soit G une extension centrale non scindée de H par C_2, le groupe multiplicatif $\{1, \omega\}$ d'ordre 2. Le groupe G satisfait $1 \to C_2 \to G \to H \to 1$. Soit F un corps de caractéristique différente de 2, et soit K une extension galoisienne de F telle que $\mathrm{Gal}(K/F) \cong H$. Soit $E(H, G, F, K)$ l'ensemble des corps L quadratiques sur K et galoisiens sur F tels que $\mathrm{Gal}(L/F) \cong G$ et que le diagramme
$$\begin{array}{ccc} \mathrm{Gal}(L/F) & \to & \mathrm{Gal}(K/F) \\ \downarrow & & \downarrow \\ G & \to & H \end{array}$$
commute. Dans ce qui suit, nous prenons $H = D_4$, le groupe diédral d'ordre 8 dont on fixe un plongement dans S_4, et G l'un des deux groupes $\tilde{D}_4$ et $\hat{D}_4$ qui apparaissent comme 2-sous-groupes de Sylow des groupes $\tilde{S}_4$ et $\hat{S}_4$ [1]. Nous donnons une description explicite de $E(D_4, \tilde{D}_4, F, K)$ et une description de $E(D_4, \hat{D}_4, F, K)$ dans le cas où F est un corps vérifiant certaines conditions, par exemple quand F est un corps global. Nous utilisons des méthodes basées sur des idées de Witt [2], que nous illustrons par des exemples d'extensions régulières de $\mathbf{Q}(t)$ de groupe de Galois $\tilde{D}_4$ et $\hat{D}_4$.

Nous tenons à remercier le Max-Planck Institut für Mathematik pour son hospitalité et son soutien financier pendant la préparation de cette Note.

1. LE THÉORÈME DE WITT POUR LE GROUPE DES QUATERNIONS H_8. — Soit $\Gamma = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et soit K une extension d'un corps R de caractéristique différente de 2, telle que $\mathrm{Gal}(K/R) \cong \Gamma$. Écrivons $\Gamma = \{1, \sigma_1, \sigma_2, \sigma_3\}$. Soit $\{\xi_\sigma \mid \sigma \in \Gamma\}$ une base de K sur R satisfaisant $\xi_1 = 1$, $\prod_\sigma \xi_\sigma = 1$, $\sigma(\xi_\sigma) = \xi_\sigma$ et $\xi_\sigma^2 \in R$. Posons $a_\sigma = \xi_\sigma^2$.

Witt s'intéresse au groupe des quaternions H_8, qui est une extension de Γ par C_2. Soit $\{h_\sigma \mid \sigma \in \Gamma\}$ un système de représentants de H_8/C_2. Pour $\sigma, \tau \in \Gamma$ on définit $\zeta_{\sigma,\tau} = h_\sigma h_\tau h_{\sigma\tau}^{-1}$, où $\zeta_{\sigma,\tau}$ est un élément de $C_2 = \{1, \omega\}$ que l'on identifie avec $\{1, -1\}$. Soit T le produit croisé $(K/R, \zeta_{\sigma,\tau})$. Rappelons que T est une algèbre centrale simple de dimension 16, contenant K. Soit $\{v_\sigma \mid \sigma \in \Gamma\}$ une base de T telle que $T = \sum_{\sigma \in \Gamma} K v_\sigma$ avec $v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau}$ et $v_\sigma \alpha = \sigma(\alpha) v_\sigma$ si $\alpha \in K$. Soit A la sous-algèbre de T engendrée par les v_σ pour $\sigma \in \Gamma$ et B celle engendrée par les $\xi_\sigma v_\sigma$ pour $\sigma \in \Gamma$. Les algèbres A et B sont isomorphes respectivement aux algèbres de quaternions $(-1, -1)$ et $(-a_{\sigma_1}, -a_{\sigma_2})$. On voit facilement que $T = A \otimes_R B$. Il est connu que $E(\Gamma, H_8, R, K)$ est non vide si et seulement si T est décomposée.

THÉORÈME 1 (Witt [2]). — *Supposons que* T *soit décomposée, donc qu'il existe un isomorphisme d'algèbres* $g : A \xrightarrow{\cong} B$. *Pour un tel* g, *soit* $c_g \in A \otimes_R K$ *le quaternion* $c_g = \sum_{\tau \in \Gamma} v_\tau^{-1} \xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau)$. *Soit* $\gamma = N_A c_g$ *la norme de* c_g. *Alors les éléments de* $E(\Gamma, H_8, R, K)$ *sont les* $L_r = K(\sqrt{r\gamma})$, *où r parcourt* R^*.

Note présentée par Jean-Pierre SERRE.

0249-6291/89/03080033 \$ 2.00 © Académie des Sciences

2. Les groupes $\tilde{D}_4$ et $\hat{D}_4$. — Soit K une extension de F telle que $\mathrm{Gal}(K/F) \cong D_4$, que l'on plonge dans S_4 de la façon suivante : $D_4 = \{1, (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\}$. Le corps K est le corps de décomposition d'un polynôme de la forme $P(X) = X^4 + bX^2 + d$, $b, d \in F$. Notons α_1, α_2, α_3 et α_4 les racines de $P(X)$: on a $\alpha_1 + \alpha_3 = 0$. Soit G l'un des deux groupes $\tilde{D}_4$ ou $\hat{D}_4$. Posons $\varepsilon = 1$ si $G = \tilde{D}_4$ et $\varepsilon = \omega$ si $G = \hat{D}_4$, où ω est l'élément central d'ordre 2 de $\hat{D}_4$. Le groupe G est engendré par des éléments x et y tels que $x^4 = (xy)^2 = \omega$, $y^2 = \varepsilon$. Le groupe $\hat{D}_4$ est le groupe quaternionien d'ordre 16. Soit $\rho = (24) \in D_4$. L'élément $v_\rho \in G$ vérifie $v_\rho^2 = \varepsilon$. Soit $R = F(\sqrt{D}) = F(\sqrt{d})$, où $D = 16(b^2 - 4d)^2 d$ est le discriminant de $P(X)$. Alors $\mathrm{Gal}(K/R) \cong \Gamma$. On pose $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$ et $\sigma_3 = (14)(23)$. On prend comme base de K sur R : $\xi_1 = 1$, $\xi_{\sigma_1} = \alpha_1 + \alpha_2$, $\xi_{\sigma_3} = \alpha_1 + \alpha_4$ et $\xi_{\sigma_2} = (\xi_{\sigma_1} \xi_{\sigma_3})^{-1}$. Soit $\{h_\sigma \mid \sigma \in D_4\}$ un système de représentants de G/C_2 et $\zeta_{\sigma,\tau} = h_\sigma h_\tau h_{\sigma\tau}^{-1}$ pour $\sigma, \tau \in \Gamma$. Soit T le produit croisé $(K/F, \zeta_{\sigma,\tau})$ et soit $\{v_\sigma \mid \sigma \in D_4\}$ une base de T telle que $T = \sum_{\sigma \in D_4} K v_\sigma$, $v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau}$ et $v_\sigma \alpha = \sigma(\alpha) v_\sigma$ si $\alpha \in K$.

Si T est décomposée, alors $E(D_4, G, F, K)$ est non vide. On note que dans ce cas, en considérant Γ et H_8 comme sous-groupes de D_4 et G respectivement, $E(\Gamma, H_8, R, K)$ contient $E(D_4, G, F, K)$. Le théorème de Witt nous permet de construire les éléments de $E(\Gamma, H_8, R, K)$: nous allons caractériser ceux qui sont dans $E(D_4, G, F, K)$.

Soient A l'algèbre $\sum_{\sigma \in \Gamma} R v_\sigma$ et B l'algèbre $\sum_{\sigma \in \Gamma} R \xi_\sigma v_\sigma$ comme dans le paragraphe 1. Soit $T' = A \otimes_R B = \sum_{\sigma \in \Gamma} K v_\sigma$. Notons ρ l'automorphisme semi-linéaire de T' donné par $x \mapsto v_\rho^{-1} x v_\rho$. Les algèbres A et B sont stables par ρ. Notons A^ρ (resp. B^ρ) l'ensemble des éléments de A (resp. B) invariants par ρ. Pour chaque isomorphisme g de A sur B, définissons un automorphisme f_g de A par $f_g(x) = \rho \circ g^{-1} \circ \rho^{-1} \circ g(x)$.

Théorème 2. — (i) $T = A \otimes_F B \otimes_F (\varepsilon, d) = (-2, -d) \otimes_F (2b, -d(b^2 - 4d)) \otimes_F (\varepsilon, d)$.

(ii) *Supposons que* T *soit décomposée. Alors si* $G = \tilde{D}_4$, *il existe un isomorphisme* $g : A \xrightarrow{\cong} B$ *tel que* f_g *soit l'identité, et si* $G = \hat{D}_4$ *et* F *est un corps global, il existe un isomorphisme* $g : A \xrightarrow{\cong} B$ *et un élément* $u \in A^*$ *tels que* $f_g(x) = u^{-1} x u$ *pour tout* $x \in A$ *et* $N_A u = d$. *Soit* c_g *le quaternion associé à un tel* g *comme dans le théorème* 1, *et soit* $\gamma = N_A c_g$. *Alors les éléments de* $E(D_4, G, F, K)$ *sont les* $K(\sqrt{r\gamma})$ *où* r *parcourt* F^*.

Démonstration. — (i) Le premier isomorphisme est clair, étant donné que (ε, d) est engendrée par v_ρ et $\sqrt{d}$. Le deuxième peut se voir en prenant $v_{\sigma_1} + v_{\sigma_3}$ et $\sqrt{d}.v_{\sigma_2}$ comme générateurs de A^ρ, et $\xi_{\sigma_1} v_{\sigma_1} + \xi_{\sigma_3} v_{\sigma_3}$ et $\sqrt{d}.v_{\sigma_2}(b^2 - 4d)$ comme générateurs de B^ρ.

(ii) *Cas* 1. — $G = \tilde{D}_4$. Dans ce cas $\varepsilon = 1$ et l'algèbre $(\varepsilon, d) = (1, d)$ est décomposée. Donc, si T est décomposée, il existe un isomorphisme $f : A^\rho \xrightarrow{\cong} B^\rho$. En étendant les scalaires à R, on obtient un isomorphisme $g : A \xrightarrow{\cong} B$. Mais il est clair qu'un g obtenu de cette façon commute avec ρ, et donc que f_g est l'identité.

Posons $L = K(\sqrt{\gamma})$. On sait par le théorème 1 que L est galoisien sur R : pour montrer que L est galoisien sur F il suffit de montrer que $\gamma^\rho \gamma^{-1}$ est un carré dans K. Pour cela, on montre que $c_g^\rho = v_\rho^{-1} c_g v_\rho = c_g$, et donc $\gamma^\rho = \gamma$. On a

$$c_g^\rho = \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} (\xi_{\rho\tau\rho}^{-1} v_\rho^{-1} g^{-1} (\xi_\tau v_\tau) v_\rho)$$
$$= \sum_{\tau \in \Gamma} v_{\rho\tau\rho}^{-1} \xi_{\rho\tau\rho}^{-1} g^{-1} (\xi_{\rho\tau\rho} v_{\rho\tau\rho}) = \sum_{\tau \in \Gamma} v_\tau^{-1} \xi_\tau^{-1} g^{-1} (\xi_\tau v_\tau) = c_g.$$

De plus, en posant $\delta_\sigma = v_\sigma c_g^\sigma c_g^{-1}$ pour $\sigma \in \Gamma$ et $\delta_{\rho\sigma} = \delta_\sigma^\rho \zeta_{\rho,\sigma}$, on constate que $\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}$ pour tout $\sigma, \tau \in D_4$ et donc que $\mathrm{Gal}(L/F)$ est bien $\tilde{D}_4$. On a donc montré que L est dans $E(D_4, \tilde{D}_4, F, K)$. Les autres éléments sont donnés par $K(\sqrt{r\gamma})$, $r \in F^*$.

Cas 2. — $G = \hat{D}_4$ et F est un corps global. Le fait que T est décomposée signifie que les algèbres $A_1 = A^\rho \otimes_F (-1, d)$ et $B_1 = B^\rho \otimes_F (1, d)$ sont isomorphes. L'algèbre A_1 est engendrée par A et un élément α tel que $\alpha^2 = -1$ et $\alpha^{-1} x \alpha = x^\rho$ pour tout $x \in A$. De même B_1 est engendrée par B et un élément β tel que $\beta^2 = 1$ et $\beta y \beta = y^\rho$ pour tout $y \in B$.

On a $A = A^\rho \otimes_F R$ et $B^\rho \otimes_F R$; comme $(-1, d)$ et $(1, d)$ sont décomposées sur R, l'hypothèse $A_1 \cong B_1$ entraîne $A \cong B$. D'après le théorème de Skolem-Noether, il existe un isomorphisme $h: A_1 \overset{\cong}{\to} B_1$ qui applique A sur B et est R-linéaire. A un tel h on associe un élément $\lambda(h)$ de B tel que $h(\sqrt{d}.\alpha) = \lambda(h)\beta$ (notons que, puisque $h(\sqrt{d}.\alpha)$ anticommute avec $\sqrt{d}$, il se trouve forcément dans $B\beta$). L'élément $\lambda(h)$ a les deux propriétés suivantes :

(i) $\lambda(h)\beta\lambda(h)\beta = \lambda(h)\lambda(h)^\rho = d$.

(ii) Pour $x \in A$, on a $(\lambda(h)\beta)^{-1} h(x)(\lambda(h)\beta) = h(x)$, autrement dit

$$\beta h(x)\beta = h(x)^\rho = \lambda(h)^{-1} h(x)\lambda(h).$$

LEMME. — *On peut choisir h de telle sorte que* $N_B \lambda(h) = d$.

Démonstration. — Choisissons un isomorphisme $h_0: A_1 \overset{\cong}{\to} B_1$ comme ci-dessus. Pour tout $q \in B^*$, $q^{-1} h_0 q$ est aussi un tel isomorphisme. Nous allons construire un $q \in B^*$ tel que $N_B(\lambda(q^{-1} h_0 q)) = d$. On commence par remarquer que

$$\lambda(q^{-1} h_0 q)\beta = q^{-1} h_0(\sqrt{d}.\alpha) q = q^{-1}\lambda(h_0)\beta q = q^{-1}\lambda(h_0) q^\rho \beta.$$

Donc $N_B \lambda(q^{-1} h_0 q) = (N_B \lambda(h_0))(N_B q)^\rho (N_B q)^{-1}$. Soit $z = N_B(\lambda(h_0))/d \in F(\sqrt{d})$. On a alors $zz^\rho = 1$ et donc par le théorème 90 de Hilbert, il existe $y \in F(\sqrt{d})$ tel que $z = y/y^\rho$. Donc $(N_B(\lambda(h_0))y^\rho/y = d$. On remarque qu'à chaque place réelle de $F(\sqrt{d})$ où $N_B x$ est définie positive, z est positif et donc y et y^ρ ont même signe : on peut donc rendre y positif à chacune de ces places en le multipliant par un élément convenable de F. Or, la norme d'un quaternion est une forme quadratique à 4 variables, donc par le théorème de Hasse-Minkowski, l'équation $N_B q = y$ a une solution dans B. On pose $h(x) = q^{-1} h_0(x) q$, ce qui permet de conclure.

Choisissons h comme dans le lemme, et soit g sa restriction à A, qui est un isomorphisme de A sur B. L'application $x \mapsto f_g(x) = \alpha^{-1} g^{-1}(\beta g(x)\beta)\alpha$ est un automorphisme de A. Il existe donc un élément $u \in A^*$ tel que $u^{-1} xu = \alpha^{-1} g^{-1}(\beta g(x)\beta)\alpha$ pour tout $x \in A$. Pour tout $x \in A$,

$$u^{-1} xu = \alpha^{-1} g^{-1}(\beta g(x)\beta)\alpha$$
$$= \alpha^{-1} g^{-1}(\lambda(h)^{-1} g(x)\lambda(h))\alpha = \alpha^{-1} g^{-1}(\lambda(h)^{-1})\alpha x \alpha^{-1} g^{-1}(\lambda(h))\alpha,$$

donc $u = \alpha^{-1} g^{-1}(\lambda(h))\alpha$. Ceci donne $N_A u = N_A(g^{-1}(\lambda(h))^\rho = N_A(\lambda(h))^\rho = d$ par le lemme.

Soit $\gamma = N_A c_g$ la norme du quaternion $c_g \in A \otimes_R K$ associé à g. Comme dans le cas $G = \tilde{D}_4$, pour montrer que L est galoisien sur F il suffit de montrer que $\gamma^\rho \gamma^{-1}$ est un carré dans K. Tout d'abord, on a

$$c_g = \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} (v_\rho^{-1} \xi_\tau^{-1} g^{-1}(\xi_\tau v_\tau) v_\rho)$$
$$= \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} \rho(\xi_\tau)^{-1} \alpha^{-1} g^{-1}(\xi_\tau v_\tau)\alpha$$
$$= \sum_{\tau \in \Gamma} (-v_{\rho\tau\rho})^{-1} \xi_{\rho\tau\rho}^{-1} u^{-1} g^{-1}(\beta\xi_\tau v_\tau \beta) u$$
$$= \sum_{\tau \in \Gamma} -v_{\rho\tau\rho}^{-1} \xi_{\rho\tau\rho}^{-1} u^{-1} g^{-1}(-\xi_{\rho\tau\rho} v_{\rho\tau\rho}) u = \sum_{\tau \in \Gamma} v_\tau^{-1} \xi_\tau^{-1} u^{-1} g^{-1}(\xi_\tau v_\tau) u.$$

On emploie alors l'identité suivante, facile à vérifier :

$$v_\tau^{-1} = c_g(\xi_{\sigma\tau}^{-1} g^{-1}(\xi_\tau v_\tau))\, c_g^{-1} = c_g^\rho(u^{-1}\xi_{\sigma\tau}^{-1} g^{-1}(\xi_\tau v_\tau) u)\,(c_g^\rho)^{-1}.$$

On en tire : $c_g^{-1} c_g^\rho u^{-1}(\xi_{\sigma\tau}^{-1} g^{-1}(\xi_\tau v_\tau)) = (\xi_{\sigma\tau}^{-1} g^{-1}(\xi_\tau v_\tau))\, c_g^{-1} c_g^\rho u^{-1}$, d'où le fait que $c_g^{-1} c_g^\rho u^{-1}$ est dans le centre de $A \otimes_R K$, donc dans K. Donc $N_A c_g = N_A c_g . N_A u$ modulo $(K^*)^2$. Mais par construction $N_A u = d$, qui est un carré dans K. On voit donc que $L = K(\sqrt{\gamma})$ est galoisien sur F. Pour vérifier que Gal(L/F) est bien $\hat{D}_4$, on remarque qu'en posant $\delta_\sigma = v_\sigma c_g^\sigma c_g^{-1}$ pour $\sigma \in \Gamma$ et $\delta_\rho = \sqrt{d} . c_g^{-1} c_g^\rho u^{-1}$ on a $\delta_\sigma \delta_\tau \delta_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}$ pour tout $\sigma, \tau \in D_4$. Donc $K(\sqrt{\gamma}) \in E(D_4, \hat{D}_4, F, K)$ et les autres éléments sont les $K(\sqrt{r\gamma})$ où r parcourt F^*.

Exemples. — Soit $P(X) = X^4 - X^2 + d$, où d, $1-4d$ et $d(1-4d)$ ne sont pas des carrés dans F, et soient α_1, α_2, α_3 et α_4 les racines de P(X) comme ci-dessus.

Cas 1. — $G = \tilde{D}_4$. On a $A^\rho = (-2, -d)$ et $B^\rho = (-2, -d(1-4d))$, donc si $A^\rho = B^\rho$ il existe u et $v \in F$ tels que $-2u^2 + (1-4d)v^2 = 1$. La méthode décrite ci-dessus donne

$$\gamma = 1 + \alpha_1 - \frac{1}{v\sqrt{1-4d}} - \frac{1}{v\sqrt{1-4d}}\alpha_1, \qquad \text{où} \qquad \sqrt{1-4d} = \frac{1}{2} - \alpha_1^2.$$

Soit Q(X) le polynôme minimal de γ. Alors le groupe de Galois de $Q(X^2)$ est $\tilde{D}_4$ et

$$Q(X^2) = X^8 - 4X^6 + \left(\frac{2v + 10u^2 v - 2 - 4u^2}{v(1+2u^2)}\right)X^4 - \left(\frac{4u^2(v-1)}{v(1+2u^2)}\right)X^2 + \left(\frac{4u^4 d}{(1+2u^2)^2}\right).$$

En prenant $v=2$, par exemple, et $u=t$, ce polynôme donne une extension régulière de $\mathbf{Q}(t)$ de groupe de Galois $\tilde{D}_4$.

Cas 2. — $G = \hat{D}_4$. On considère le cas où l'algèbre $(-1, d)$ est décomposée : dans ce cas on n'a pas besoin de supposer que F est un corps global. Si $(-1, d)$ est décomposée, il existe x et $y \in F$ tels que $-x^2 + dy^2 = 1$. On envoie A^ρ sur B^ρ comme dans le cas 1 et $\alpha \mapsto x\beta + y\beta\sqrt{d}$. Posons $\lambda = -yd + x\sqrt{d} \in F(\sqrt{d})$. Alors la méthode décrite ci-dessus permet de calculer

$$\gamma = (2yd\lambda)\left[1 + \alpha_1 - \frac{1}{v\sqrt{1-4d}} - \frac{1}{v\sqrt{1-4d}}\alpha_1\right].$$

On en déduit des extensions régulières de $\mathbf{Q}(t)$ à groupe de Galois le groupe quaternionien d'ordre 16.

Note remise le 21 novembre 1988, acceptée le 23 novembre 1988.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] I. SCHUR, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, *J. reine angew. Math.*, 139, 1911, p. 155-250 (*Ges. Abh.*, I, p. 346-441).

[2] E. WITT, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. reine angew. Math.*, 174, 1935, p. 237-245.

Max-Planck Institut für Mathematik,
Gottfried-Clarenstrasse 26, 5300 *Bonn* 3, *R.F.A.*