Sém. Th. Nombres Bordeaux **4** (1992), 24-30.

Polynômes à groupe de Galois diédral

Dominique Martinais et Leila Schneps

Résumé

Soit K un corps et K_1 une extension quadratique de K. Etant donné un polynôme P de $K_1[X]$ à groupe de Galois cyclique, nous donnons une méthode pour construire un polynôme Q de $K[X]$ à groupe de Galois diédral, à partir des racines de P. Cette méthode est tout à fait explicite: nous donnons de nombreux exemples de polynômes à groupe de Galois diédral sur le corps $\mathbb{Q}$.

*

§1. Le problème inverse de la théorie de Galois

Soit K un corps de caractéristique nulle et G un groupe fini. Le problème inverse de la théorie de Galois pour G sur K est de savoir si G se réalise comme groupe de Galois d'une extension de K. Si c'est le cas, l'étape suivante est de chercher à construire explicitement une extension galoisienne de K, de groupe de Galois G. Il est souvent utile d'avoir de telles réalisations explicites, entre autres pour étudier le problème inverse de la théorie de Galois lui-même pour des groupes plus grands. En effet, si $\tilde{G}$ est un groupe fini dont G est un quotient et si L/K est une extension galoisienne de groupe de Galois G, on se demande si L peut être plongé dans un corps M tel que M/K soit une extension galoisienne de K de groupe de Galois $\tilde{G}$. Si l'on connaît explicitement L, on pourra essayer de calculer l'obstruction. Si l'on arrive à choisir le corps L de telle façon que cette obstruction soit nulle, alors on saura que $\tilde{G}$ se réalise comme groupe de Galois sur K.

Dans cet article, nous avons voulu montrer comment obtenir explicitement des polynômes sur $\mathbb{Q}$, à groupe de Galois D_n, le groupe diédral d'ordre $2n$. Il est connu depuis longtemps (voir par exemple [M]) que les groupes D_n se réalisent comme groupes de Galois

sur $\mathbb{Q}$ et même comme groupes de Galois d'extensions régulières de $\mathbb{Q}(T)$, car D_n est le produit semi-direct de deux groupes abéliens, précisément de C_n par C_2. Mais ce raisonnement ne fournit pas directement de polynômes explicites. En utilisant la théorie du corps de classes de Hilbert, on peut réaliser quelques exemples explicites de polynômes de groupe de Galois D_p pour p premier: Hilbert lui-même l'a fait pour $p = 3$ et 5. Mais il faut chercher un corps quadratique imaginaire de nombre de classes égal à p, et les calculs deviennent très rapidement inabordables. Dans leurs travaux, Jensen et Yui [JY] donnent des conditions nécéssaires et suffisantes pour qu'un polynôme défini sur $\mathbb{Q}$ ait comme groupe de Galois D_p, où p est un nombre premier. Ils ne donnent dans leur article qu'une famille paramétrée ayant D_5 comme groupe de Galois, et un polynôme très grand de groupe de Galois D_7, obtenu par la méthode des corps de classes de Hilbert. Dans [M], Mestre donne une autre méthode qui fournit des polynômes en un paramètre de groupe de Galois D_5 ou D_7. A. Brumer [B] a trouvé un polynôme générique à deux paramètres à groupe de Galois D_5 que nous donnons dans le §4: nous le remercions de nous l'avoir communiqué.

Notre méthode est basée sur deux choses:

(1) la connaissance de familles de polynômes à groupe de Galois cyclique d'ordre n; Smith [Sm] en a donné lorsque n est impair, ses travaux étant basés sur des idées de Saltman [S];

(2) la structure du groupe diédral comme quotient du produit en couronne $C_n \wr C_2$ par son sous-groupe isomorphe à la diagonale de $C_n \times C_n$.

Nous traduisons ces deux idées en termes de corps: autrement dit, nous cherchons à réaliser le groupe diédral comme groupe de Galois d'un corps L/K, où $L \subset M$ et où M/K est galoisienne de groupe de Galois un sous-groupe de $C_n \wr C_2$. Cette extension M sera construite grâce aux polynômes cycliques.

§2. Construction théorique d'extensions diédrales

Fixons un entier n au moins égal à 2. Soit K un corps de caractéristique nulle. Choisissons une clôture algébrique de K que nous notons $\bar{K}$. Dans les constructions que nous allons faire, tous les corps considérés seront des sous-corps de $\bar{K}$. Nous supposons dans toute cette partie que le corps K satisfait aux conditions suivantes:

(i) Il existe $d \in K^* - (K^*)^2$. Soit $\alpha \in \bar{K}$ tel que $\alpha^2 = d$, et soit $K_1 = K(\alpha)$.

(ii) Il existe une extension galoisienne L_1 de K_1 telle que $\mathrm{Gal}(L_1/K_1)$ soit cyclique

d'ordre n.

Dans ce paragraphe nous montrons comment obtenir des extensions diédrales de K.

Pour tout sous-corps K' de $\bar{K}$ et pour tout polynôme U de $K'[X]$, on note $D_{K'}(U)$ le corps de décomposition de U, c'est-à-dire le plus petit sous-corps de $\bar{K}$ contenant K' et les racines de U. Soit P un polynôme unitaire de $K_1[X]$, de degré n, irréductible et tel que $L_1 = D_{K_1}(P)$. Appelons la conjugaison l'unique élément d'ordre 2 de $\mathrm{Gal}(K_1/K)$ et pour tout élément de K_1, appelons son conjugué son image par la conjugaison. Introduisons alors le polynôme $\bar{P}$ de $K_1[X]$ dont les coefficients sont les conjugués de ceux de P. Considérons l'extension L_2 de K_1 définie par $L_2 = D_{K_1}(\bar{P})$. Le groupe de Galois $\mathrm{Gal}(L_2/K_1)$ est cyclique d'ordre n. En effet, si $u : L_1 \to L_2$ est un isomorphisme de corps qui prolonge la conjugaison de K_1, on a alors $\mathrm{Gal}(L_2/K_1) = u\mathrm{Gal}(L_1/K_1)u^{-1}$.

Soit $M = L_1L_2$. L'extension M/K_1 est galoisienne et l'homomorphisme

$$\mathrm{Gal}(M/K_1) \to \mathrm{Gal}(L_1/K_1) \times \mathrm{Gal}(L_2/K_1)$$

$$\sigma \qquad \mapsto \qquad (\sigma|_{L_1}, \sigma|_{L_2})$$

est injectif. De plus, c'est un isomorphisme si et seulement si $L_1 \cap L_2 = K_1$. Puisque $P\bar{P} \in K[X]$, on a $M = D_K\big(P\bar{P}(X^2 - d)\big)$, donc en particulier M est une extension galoisienne de K et on a la suite exacte suivante:

$$1 \to \mathrm{Gal}(M/K_1) \to \mathrm{Gal}(M/K) \to \mathrm{Gal}(K_1/K) \to 1.$$

Dans toute la suite, écrivons $P = \prod_{i \in \mathbb{Z}/n\mathbb{Z}}(X - r_i)$ où les racines de P sont numérotées de telle façon que l'application $r_i \mapsto r_{i+1}$ définisse un générateur de $\mathrm{Gal}(L_1/K_1)$. Nous dirons dans ce cas que les racines de P sont *bien numérotées.*

Proposition 2.1: *Supposons qu'il existe* $\tau \in \mathrm{Gal}(M/K)$ *tel que* $\tau^2 = \mathrm{id}_M$ *et* $\tau|_{K_1}$ *soit la conjugaison de* K_1. *Alors* $\mathrm{Gal}(M/K)$ *est isomorphe à un sous-groupe du produit en couronne* $C_n \wr C_2$. *Plus précisément, il existe un sous-groupe* A *de* $C_n \times C_n$, *symétrique par rapport à la diagonale et tel que* $\mathrm{Gal}(M/K)$ *soit isomorphe au produit semi-direct* $A \rtimes C_2$, *où l'élément non-trivial de* C_2 *opère sur* A *par permutation des facteurs.*

Démonstration: On a $\tau(L_1) = L_2$. On a donc un monomorphisme $\phi : \mathrm{Gal}(M/K_1) \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ où $\phi(\sigma) = (j,k)$ si $\sigma(r_i) = r_{i+j}$ et $\sigma(\tau(r_i)) = \tau(r_{i+k})$ pour tout $i \in \mathbb{Z}/n\mathbb{Z}$. Si (j,k) est dans l'image de ϕ, notons $\sigma_{j,k}$ l'élément $\phi^{-1}(j,k)$. D'autre part, $\mathrm{Gal}(M/K_1)$ est un sous-groupe distingué de $\mathrm{Gal}(M/K)$ et $\mathrm{Gal}(M/K) = \mathrm{Gal}(M/K_1) \cdot \{\mathrm{id}_M, \tau\}$, donc le groupe $\mathrm{Gal}(M/K)$ est produit semi-direct de $\{\mathrm{id}_M, \tau\}$ par $\mathrm{Gal}(M/K_1)$; il est immédiat de voir que τ opère sur $\mathrm{Gal}(M/K_1)$ par $\tau\sigma_{j,k}\tau^{-1} = \sigma_{k,j}$ pour tout $(j,k) \in \mathrm{Im}(\phi)$, d'où la proposition.

$\diamondsuit$

Enonçons maintenant le théorème principal.

Théorème 2.2: *Supposons que l'entier n soit au moins égal à 3 et qu'il existe $\tau \in \mathrm{Gal}(M/K)$ tel que $\tau^2 = \mathrm{id}_M$ et $\tau|_{K_1}$ soit la conjugaison de K_1. Soit pour tout k dans $\mathbb{Z}/n\mathbb{Z}$, s_k défini par*

$$s_k = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} r_i \tau(r_{i+k}),$$

et soit Q le polynôme de $M[X]$ défini par

$$Q = \prod_{k \in \mathbb{Z}/n\mathbb{Z}} (X - s_k).$$

On a alors

(i) le polynôme Q est à coefficients dans K;

(ii) supposons que Q n'ait que des racines simples et posons $L = D_K(Q)$. Alors le groupe de Galois $\mathrm{Gal}(L/K)$ est isomorphe à un sous-groupe du groupe diédral D_n. De plus, il est isomorphe à D_n si et seulement s'il contient un élément d'ordre n.

Démonstration: (i) Soit $\sigma_{i,j} \in \mathrm{Gal}(M/K_1)$; il est immédiat que l'on a $\sigma_{i,j}(s_k) = s_{k+j-i}$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$. Il vient donc $Q = \prod_{k \in \mathbb{Z}/n\mathbb{Z}}(X - \sigma_{i,j}(s_k))$. D'autre part, il est clair que l'on a $\tau(s_k) = s_{-k}$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$. Par suite on a $Q = \prod_{\mathbb{Z}/n\mathbb{Z}}(X - \tau(s_k))$. Les coefficients de Q sont donc invariants par $\mathrm{Gal}(M/K)$, donc dans K.

Le groupe $\mathrm{Gal}(L/K)$ est isomorphe au quotient $\mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$. Il faut donc calculer le groupe $\mathrm{Gal}(M/L)$. On a $\mathrm{Gal}(M/L) = \{\sigma \in \mathrm{Gal}(M/K) \mid \sigma|_L = \mathrm{id}_L\}$. Soit $\sigma_{i,j} \in \mathrm{Gal}(M/K_1)$; on a $\sigma_{i,j}(s_k) = s_{k+j-i}$ et $\tau\sigma_{i,j}(s_k) = s_{i-j-k}$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$. Les racines de Q étant simples, on a $\sigma_{i,j}(s_k) = s_k$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$ si et seulement si $i = j$. D'autre part, puisque $n \geq 3$, il existe $k \in \mathbb{Z}/n\mathbb{Z}$ tel que $2k \neq 0$. Par suite $\tau\sigma_{i,j} \notin \mathrm{Gal}(M/L)$. On a donc $\mathrm{Gal}(M/L) = \{\sigma_{i,i} \in \mathrm{Gal}(M/K_1)\}$. Rappelons que l'on a un monomorphisme $\mathrm{Gal}(M/K) \to C_n \wr C_2$ et donc un homomorphisme $\mathrm{Gal}(M/K) \to D_n$ dont le noyau est exactement $\mathrm{Gal}(M/L)$ d'après le calcul précédent. $\mathrm{Gal}(L/K)$ est donc isomorphe à un sous-groupe de D_n. Il est clair que si $\mathrm{Gal}(L/K)$ est isomorphe à D_n il contient un élément d'ordre n. Réciproquement, supposons que $\mathrm{Gal}(L/K)$ contient un élément d'ordre n. Cela veut dire qu'il existe $\sigma \in \mathrm{Gal}(M/K)$ tel que n soit le plus petit entier positif tel que $\sigma^n \in \mathrm{Gal}(M/L)$. Soit donc un tel σ. Pour tout élément $\sigma_{i,j}$ de $\mathrm{Gal}(M/K_1)$ on a $(\tau\sigma_{i,j})^2 = \sigma_{i+j,i+j}$ et donc $(\tau\sigma_{i,j})^2$ appartient à $\mathrm{Gal}(M/L)$. Par suite σ est nécéssairement dans $\mathrm{Gal}(M/K_1)$. Le groupe $\mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$ a donc au moins $2n$ éléments: les classes modulo $\mathrm{Gal}(M/L)$ de σ^k et de $\tau\sigma^k$ pour $k \in \{0, \ldots, n-1\}$. C'est donc D_n.

$\diamondsuit$

Etant donné un polynôme cyclique P défini sur K, notre construction repose sur l'existence d'un élément τ d'ordre 2 de $\mathrm{Gal}(M/K)$ qui prolonge la conjugaison de K_1. Voici alors quelques résultats théoriques sur l'existence d'un tel élément.

Lemme 2.3: *Si n est impair alors il existe un élément d'ordre 2 de* $\mathrm{Gal}(M/K)$ *qui prolonge la conjugaison de K_1.*

Démonstration: La suite

$$1 \to \mathrm{Gal}(M/K_1) \to \mathrm{Gal}(M/K) \to \mathrm{Gal}(K_1/K) \to 1$$

étant exacte, soit u un élément de $\mathrm{Gal}(M/K)$ qui prolonge la conjugaison de K_1. Puisque n est impair, u^n prolonge aussi la conjugaison. Montrons alors que u^n est d'ordre 2, c'est-à-dire que l'on a $u^{2n} = \mathrm{id}_M$. On a $u^2 \in \mathrm{Gal}(M/K_1)$, or $\mathrm{Gal}(M/K_1)$ est un sous-groupe de $C_n \times C_n$, groupe d'exposant n. Par suite on a $(u^2)^n = \mathrm{id}_M$, d'où le résultat.

$\diamondsuit$

Lemme 2.4: *Si on a $L_1 \cap L_2 = K_1$ alors il existe un élément d'ordre 2 de* $\mathrm{Gal}(M/K)$ *qui prolonge la conjugaison de K_1.*

Démonstration: Puisque l'on a $L_1 = D_{K_1}(P)$ et $L_2 = D_{K_1}(\bar{P})$, il existe un isomorphisme de corps $u : L_1 \to L_2$ qui prolonge la conjugaison de K_1. Comme on $L_1 \cap L_2 = K_1$, il vient $u|_{L_1 \cap L_2} = u^{-1}|_{L_1 \cap L_2}$. Soit alors $\tau : M \to M$ l'unique isomorphisme de corps tel que $\tau|_{L_1} = u$ et $\tau|_{L_2} = u^{-1}$. Il est clair que τ est un élément d'ordre 2 de $\mathrm{Gal}(M/K)$ et que τ prolonge la conjugaison de K_1.

Remarque 2.5: Ce dernier lemme est impraticable, c'est- à-dire que pour un polynôme P donné on n'a généralement pas de critère simple pour tester si les extensions L_1 et L_2 sont disjointes ou non. Par contre, lorsque $n = 2$, ce n'est pas difficile de choisir P pour que les extensions L_1 et L_2 soient disjointes.

Pour construire des polynômes diédraux pour n quelconque, nous procédons en "mettant ensemble" les différents morceaux provenant des puissances de premier divisant n, selon la méthode de la proposition 2.6. Avant d'énoncer cette proposition, fixons quelques notations. Soient n_1 et n_2 deux entiers premiers entre eux et soit $n = n_1 n_2$. Soit $P_1 = \prod_{i \in \mathbb{Z}/n_1\mathbb{Z}}(X - \alpha_i)$ (resp. $P_2 = \prod_{i \in \mathbb{Z}/n_2\mathbb{Z}}(X - \beta_i)$) un polynôme irréductible de $K_1[X]$ tel que le groupe de Galois de $D_{K_1}(P_1)$ sur K_1 (resp. de $D_{K_1}(P_2)$ sur K_1) soit cyclique d'ordre n_1 (resp. n_2). De plus, supposons que les racines de P_1 (resp. P_2) sont bien numérotées. Soient les extensions $M_1 = D_K\big(P_1\bar{P}-1(X^2-d)\big)$ et $M_2 = D_K\big(P_2\bar{P}_2(X^2-d)\big)$, et posons $M = M_1M_2$. Dans la proposition 2.6 nous construisons un polynôme $P \in K_1[X]$,

irréductible de degré n, tel que $D_{K_1}(P) = D_{K_1}(P_1)D_{K_1}(P_2)$ et dont le groupe de Galois est cyclique d'ordre n. Smith [Sm] a énoncé cette construction sans la démontrer. De plus, nous allons indiquer comment l'existence d'un τ sur M se ramène à l'existence d'un τ_1 sur M_1 et d'un τ_2 sur M_2. Notons ϕ_1 et ϕ_2 les surjections canoniques $\phi_1 : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z}$ et $\phi_2 : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_2\mathbb{Z}$.

Proposition 2.6: *Pour tout $i \in \mathbb{Z}/n\mathbb{Z}$, soit $\delta_i \in M$ défini par $\delta_i = \alpha_{\phi_1(i)} + \beta_{\phi_2(i)}$. Soit P le polynôme de $M[X]$ défini par $P = \prod_{i \in \mathbb{Z}/n\mathbb{Z}}(X - \delta_i)$.*

(i) Le polynôme P est un polynôme irréductible de $K_1[X]$, on a $M = D_K\big(P\bar{P}(X^2 - d)\big)$, et le groupe $\mathrm{Gal}(D_{K_1}(P)/K_1)$ est cyclique d'ordre n. De plus les racines de P sont bien numérotées.

(ii) Supposons qu'il existe $\tau_1 \in \mathrm{Gal}(M_1/K)$ et $\tau_2 \in \mathrm{Gal}(M_2/K)$ d'ordre 2 et prolongeant la conjugaison de K_1. Alors il existe un unique τ de $\mathrm{Gal}(M/K)$ qui prolonge τ_1 et τ_2, et τ est d'ordre 2.

Démonstration: (i) Puisque n_1 et n_2 sont premiers entre eux, on a $D_{K_1}(P_1) \cap D_{K_1}(P_2) = K_1$ et donc $\mathrm{Gal}\big(D_{K_1}(P_1)D_{K_1}(P_2)/K_1\big)$ est isomorphe au produit $\mathrm{Gal}\big(D_{K_1}(P_1)/K_1\big) \times \mathrm{Gal}\big(D_{K_1}(P_2)/K_1\big)$ qui est cyclique d'ordre n. Les racines de P sont donc permutées transitivement par le groupe $\mathrm{Gal}\big(D_{K_1}(P_1)D_{K_1}(P_2)/K_1\big)$. Pour démontrer que le polynôme P est irréductible sur K_1, il suffit donc de démontrer que ses racines sont simples. Soient alors i et j tels que $\delta_i = \delta_j$. Puisque $D_{K_1}(P_1) \cap D_{K_1}(P_2) = K_1$, on a donc $a_{\phi_1(i)} - \alpha_{\phi_1(j)} \in K_1$. Par suite $\alpha_{\phi_1(i)+k} - \alpha_{\phi_1(i)+k} = \alpha_{\phi_1(i)} - \alpha_{\phi_1(j)}$ pour tout $k \in \mathbb{Z}/n_1\mathbb{Z}$. Si l'on somme ces n_1 égalités, on trouve alors, puisque l'on est en caractéristique 0, que $\alpha_{\phi_1(i)} = \alpha_{\phi_1(j)}$, par suite $\phi_1(i) = \phi_1(j)$. De même on a $\phi_2(i) = \phi_2(j)$ et donc $i = j$. Le polynôme P est un polynôme irréductible de $K_1[X]$ donc $D_{K_1}(P) = D_{K_1}(P_1)D_{K_1}(P_2)$ soit $D_{K_1}(P) = D_{K_1}(P_1P_2)$. Par suite on a $M = D_K\big(P\bar{P}(X^2 - d)\big)$. Il est clair que les racines de P sont alors bien numérotées.

(ii) Puisque les ordres des groupes $\mathrm{Gal}(M_1/K_1)$ et $\mathrm{Gal}(M_2/K_1)$ sont premiers entre eux, on a $M_1 \cap M_2 = K_1$, l'existence de τ est donc clair puisque l'on a $M = M_1M_2$.

$\diamondsuit$

Remarque 2.7: Dans la pratique, nous avons besoin de décrire explicitement l'élément τ. Nous ne savons pas le faire quand $n = 2^m$, $m > 1$, ni même donner des polynômes cycliques sur K_1 quand $m > 3$. La remarque 2.5 et la proposition 2.6 nous permettent donc de traiter les cas des groupes diédraux D_n et D_{2n} avec n impair.

§3. Application à la construction de polynômes diédraux sur $\mathbf{Q}$.

Le but de ce paragraphe est de rendre explicite la construction de polynômes diédraux donnée dans le §2, en donnant notre manière de calculer les polynômes cycliques et l'élément τ de la proposition 2.6. Pour éviter des calculs trop compliqués nous nous restreignons au cas $K = \mathbb{Q}$. Nous commençons par rappeler la construction de Smith (cf. [Sm]) d'un polynôme cyclique d'ordre n sur tout corps K_1 de caractéristique ne divisant pas n: dans notre construction de polynômes diédraux sur $\mathbb{Q}$, K_1 sera une extension quadratique de $\mathbb{Q}$.

Plaçons-nous d'abord dans le cas où n est la puissance d'un nombre premier impair. Soit ζ une racine primitive n-ième de l'unité. Soient $t_0, \ldots, t_{\phi(n)-1} \in K_1$ et définissons, pour tout $i \in (\mathbb{Z}/n\mathbb{Z})^*$, les nombres complexes b_i, c_i et e_i par:

$$b_i = \sum_{j=0}^{\phi(n)-1} t_j \zeta^{ij}, \qquad c_i^n = b_i \quad \text{et} \quad e_i = \prod_{j \in (\mathbb{Z}/n\mathbb{Z})^*} c_j^{\langle i/j \rangle},$$

où $\langle x \rangle$ désigne l'entier compris entre 0 et $n-1$ dont la classe modulo n est égale à x. Remarquons que c_i est défini à une puissance de ζ près, dont nous fixons un choix. Pour tout $i \in \mathbb{Z}/n\mathbb{Z}$, soit $r_i \in \mathbb{C}$ défini par:

$$r_i = \sum_{j \in (\mathbb{Z}/n\mathbb{Z})^*} e_j \zeta^{ij}.$$

Soit P le polynôme défini par

$$P(X) = \prod_{i \in \mathbb{Z}/n\mathbb{Z}} (X - r_i).$$

Alors $P \in K_1[X]$ et s'il est à racines simples, son groupe de Galois est cyclique d'ordre divisant n. Si P est irréductible ses racines sont bien numérotées et son groupe de Galois est isomorphe à C_n: s'il ne l'est pas, il existe $j \in \mathbb{Z}/n\mathbb{Z}$ tel que l'application $r_i \mapsto r_{i+j}$ définisse un générateur de $\mathrm{Gal}(L_1/K_1)$.

Posons maintenant $K = \mathbb{Q}$ et passons à la construction de polynômes diédraux. On traite d'abord le cas où n est une puissance de premier impair. Rappelons que ζ est une racine primitive n-ième de l'unité.

Hypothèse 1: Soit d un entier au moins égal à 2, sans facteurs carrés et tel que $\sqrt{d} \notin \mathbb{Q}(\zeta)$, autrement dit tel que $\mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$.

Posons $K_1 = \mathbb{Q}(\sqrt{d})$, et si $x \in K_1$, notons $\bar{x}$ son conjugué.

Lemme 3.1: *Soient $t_0, \ldots, t_{\phi(n)-1} \in K_1$ des paramètres et soient $\bar{t}_0, \ldots, \bar{t}_{\phi(n)-1}$ leurs conjugués. Par la méthode de Smith décrite ci-dessus, on associe des nombres r_i aux t_i et des nombres $\bar{r}_i$ aux $\bar{t}_i$. Posons*

$$P = \prod_{i \in \mathbb{Z}/n\mathbb{Z}} (X - r_i) \quad \text{et} \quad \tilde{P} = \prod_{i \in \mathbb{Z}/n\mathbb{Z}} (X - \bar{r}_i).$$

Alors le polynôme $\tilde{P}$ est égal à $\bar{P}$, le conjugué de P dans $K_1[X]$.

Démonstration: Remarquons que par l'hypothèse 1, on a $\mathrm{Gal}(K_1(\zeta)/K_1) = (\mathbb{Z}/n\mathbb{Z})^*$. Pour tout $i \in (\mathbb{Z}/n\mathbb{Z})^*$ nous définissons $\gamma_i \in \mathrm{Gal}(K_1(\zeta)/K_1)$ par $\gamma_i(\zeta) = \zeta^i$: quelque soit $x \in K_1(\zeta)$, on a $x \in \mathbb{R} \Leftrightarrow \gamma_{n-1}(x) = x$, car γ_{n-1} est exactement la restriction de la conjugaison complexe à $K_1(\zeta)$.

Soit u l'unique automorphisme de $K_1(\zeta)$ qui prolonge la conjugaison de K_1 et qui vérifie $u(\zeta) = \zeta$ (u est défini par ces conditions). On voit alors que $\gamma_{n-1} \circ u = u \circ \gamma_{n-1}$, car l'hypothèse $d \geq 2$ implique que $K_1 \subset \mathbb{R}$, et ces deux automorphismes de $K_1(\zeta)$ coïncident donc sur K_1 et sur ζ. Pour chaque $i \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $u(b_i) = \bar{b}_i$ où les b_i et les $\bar{b}_i$ correspondent aux $t_0, \ldots, t_{\phi(n)-1}$ et aux $\bar{t}_0, \ldots, \bar{t}_{\phi(n)-1}$ par la méthode de Smith: on voit donc que les coefficients de $\bar{P}$ sont les images par u de ceux de P.

$\diamondsuit$

Le but de ce qui suit est de donner des conditions suffisantes pour qu'il existe τ comme dans le théorème 2.2 et tel qu'en plus, on ait $\tau(r_i) = \bar{r}_i$.

Hypothèse 2: Choisissons les paramètres $t_0, \ldots, t_{\phi(n)-1}$ de telle façon que le nombre b_1 soit réel.

Ceci implique que tous les b_i et les $\bar{b}_i$ sont réels pour la raison suivante: pour tout i, on a $\gamma_{n-1}(b_1) = b_1$ et donc $\gamma_i\gamma_{n-1}(b_1) = \gamma_i(b_1) = b_i$. Puisque γ_{n-1} et γ_i commutent, on voit que $\gamma_{n-1}(b_i) = b_i$ et donc $b_i \in \mathbb{R}$. De plus $\bar{b}_i \in \mathbb{R}$ puisque $\bar{b}_i = u(b_i)$ et u commute avec γ_{n-1}.

Pour tout $i \in (\mathbb{Z}/n\mathbb{Z})^*$, nous choisissons pour c_i (resp. $\bar{c}_i$) l'unique racine réelle de b_i (resp. $\bar{b}_i$).

Proposition 3.2: *Soit N le plus petit sous-corps de $\mathbb{C}$ contenant $K_1(\zeta)$ et les c_i et les $\bar{c}_i$ pour tout $i \in (\mathbb{Z}/n\mathbb{Z})^*$. Il existe un unique automorphisme du corps N, que nous noterons v, tel que $v|_{K_1(\zeta)} = u$, $v(c_i) = \bar{c}_i$ et $v^2 = \mathrm{id}_N$.*

Démonstration: L'unicité est claire, démontrons l'existence. Puisque $c_1^n \in K_1(\zeta)$, le polynôme minimal de C_1 sur $K_1(\zeta)$ est de la forme $X^m - c_1^m$ avec m un diviseur de n. Le polynôme $X^m - c_1^m$ est donc un polynôme irréductible de $K_1(\zeta)[X]$. De plus, puisque $c_1^m \in \mathbb{R}$ on a $u(c_1^m) \in \mathbb{R}$. Or on a $\left(u(c_1^m)\right)^{n/m} = u(c_1^n) = u(b_1) = \bar{b}_1$ et $\bar{b}_1$ possède

une unique racine (n/m)-ième réelle, à savoir $\bar{c}_1^m$. Par suite $u(c_1^m) = \bar{c}_1^m$. On peut donc prolonger u en un isomorphisme de corps

$$u' : K_1(\zeta, c_1) \to K_1(\zeta, \bar{c}_1)$$

tel que $u'(c_1) = \bar{c}_1$. On constate que u' commute à la conjugaison complexe et donc envoie les réels de $K_1(\zeta, c_1)$ sur les réels de $K_1(\zeta, \bar{c}_1)$. On peut donc recommencer en adjoignant $\bar{c}_1$ à $K_1(\zeta, c_1)$. De proche en proche, on peut donc prolonger u en un automorphisme $v : N \to N$ tel que $v(c_i) = \bar{c}_i$ et $v(\bar{c}_i) = c_i$: cela est possible, car à chaque cran, l'isomorphisme construite commute à la conjugaison complexe et donc envoie les réels sur les réels.

$\diamondsuit$

Soit $M = D_{K_1}(P\bar{P})$. Voici le résultat essentiel de ce paragraphe:

Proposition 3.3: *L'automorphisme v de la proposition précédente vérifie $v(M) = M$. Si l'on pose $\tau = v|_M$, alors on a:*

(i) $\tau \in \mathrm{Gal}(M/K)$

(ii) $\tau^2 = \mathrm{id}_M$

(iii) $\tau|_{K_1}$ *est la conjugaison de* K_1

(iv) $\tau(r_i) = \bar{r}_i$ *pour tout* $i \in (\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration: Puisque v prolonge u, v prolonge la conjugaison de K_1. En particulier, on a $v|_K = \mathrm{id}_K$ et donc, puisque M est une extension galoisienne de K, on a $v(M) = M$. Puisque l'on a dejà $v^2 = \mathrm{id}_N$, on a certainement $\tau^2 = \mathrm{id}_M$. Le reste suit directement de la construction.

$\diamondsuit$

Pour terminer ce paragraphe, expliquons comment pratiquement nous allons obtenir des polynômes définis sur $\mathbb{Q}$ et à groupe de Galois diédral D_n pour n impair ou $n = 2m$ avec m impair. Voici les choix et les tests successifs à effectuer:

(1) On décompose n en produit de facteurs premiers $n = \prod_{i=1}^r p_i^{\alpha_i}$.

(2) On choisit d entier positif sans facteur carré tel que $\mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\zeta_i) = \mathbb{Q}$ pour chaque $i \in \{1, \ldots, r\}$ lorsque ζ_i est une racine primitive $p_i^{\alpha_i}$-ième de l'unité.

(3) Pour chaque nombre premier p_i, on construit un polynôme cyclique $P_i \in \mathbb{Z}(\sqrt{d})[X]$, de degré $p_i^{\alpha_i}$, par la méthode de Smith en choisissant les paramètres $t_i \in \mathbb{Z}(\sqrt{d})$.

(4) Le seul test à effectuer sur P_i est de vérifier que ses racines sont simples car alors on a vu que son groupe de Galois est un sous-groupe du groupe cyclique d'ordre $p_i^{\alpha_i}$.

(5) On construit le polynôme P à coefficients dans $\mathbb{Z}(\sqrt{d})$ selon la méthode décrite dans la proposition 2.6. Le groupe de Galois de P sur $\mathbb{Q}(\sqrt{d})$ est alors un sous-groupe du groupe cyclique d'ordre n.

(6) On construit le polynôme Q à coefficients dans $\mathbb{Z}$ selon la méthode du théorème 2.2 et de la proposition 3.3.

(7) On vérifie que les racines de Q sont simples.

(8) En factorisant Q modulo quelques nombres premiers, on teste si le groupe de Galois de Q sur $\mathbb{Q}$ possède bien un élément d'ordre n. Si on en trouve un, on sait d'après le théorème 2.2 que le groupe de Galois est bien le groupe diédral D_n.

§4. Exemples de polynômes diédraux

Les polynômes donnés ici, tous définis sur $\mathbb{Q}$, ont été obtenus en suivant la méthode des deux paragraphes précédants. L'exemple de $n = 6$ a été simplifié via l'algorithme POLRED implanté dans le système PARI, qui enlève les facteurs parasites. A part l'utilisation de PARI (POLRED, BASE et DISCF pour l'exemple $n = 6$), tous les calculs ont été effectués avec Maple.

Nous nous bornons à donner un polynôme pour chaque n traité, sans explication: ils ont tous été obtenus en prenant, comme valeurs pour les paramètres de Smith, des nombres choisis au hasard dans $\mathbb{Q}(\sqrt{2})$.

Cas 1: n=5. Le cas $n = 5$ ayant été traité dans [RYZ] et [B], nous nous contentons de donner leur résultat ici. Soit Q le polynôme en deux paramètres donné par $Q(X) = X^5 + aX + b$ oú

$$a = \frac{3125ts^4}{(t-1)^4(t^2-6t+25)} \quad \text{et} \quad b = \frac{3125ts^5}{(t-1)^4(t^2-6t+25)}.$$

Alors (cf. [RYZ]) Q a groupe de Galois D_5 sur $\mathbb{Q}$ pour tout $t, s \in \mathbb{Q}$ tels que $t \neq 1$, $s \neq 0$, et $\mathrm{disc}(Q) = 4^4a^5 + 5^5b^4$ soit un carré.

D'autre part, soit $Q_{s,u}(X)$ donné par

$$X^5 + (s-3)X^4 + (u-s+3)X^3 + (s^2-s-2u-1)X^2 + uX + s.$$

D'après [B], ce polynôme est générique pour D_5, c'est-à-dire que si F est un corps contenant $\mathbb{Q}$ et K est une extension galoisienne de F de groupe de Galois D_5, alors K est le corps de décomposition d'un polynôme de la forme $Q_{s,u}(X)$ pour des valeurs de s et u dans F.

Cas 2: n=6.

$$Q = X^6 - 39X^4 + -78X^3 + 117X^2 + 234X - 52.$$

Le discriminant de ce polynôme est égal à $2^6 \cdot 3^6 \cdot 5^2 \cdot 13^5 \cdot 433^2$, mais le discriminant de son corps de décomposition est égal à $2^6 \cdot 3^6 \cdot 13^5$.

Cas 3: n=7.

$$Q = X^7 - 559357197X^5 - 268864359358X^4 + 74420379522337639X^3 - 1297419289139035397 16X^2 - 2683887042758532537141243X + 90846839239542036055402086 74.$$

Cas 4: n=9.

$$Q = X^9 - 728745579X^7 - 1560973030218X^6 + 154761110107933392X^5 + 778006209242596580640X^4 - 8787884570607440698729920X^3 - 69629446396777895439430568832X^2 - 1145563971398178383851010623733 76X - 33382261688898167266516275698915328.$$

Cas 5: n=10.

$$Q = X^{10} - 2962000X^8 + 2601672700000X^6 - 708711964100000000X^4 + 633623458264865000000000X^2 - 1130121211600384160000000000.$$

Cas 6: n=11.

$$Q = X^{11} - 10789838015X^9 + 113513411853006X^8 + 31080623573769619586X^7 - 460532126300933651991576X^6 - 188552797194834715055402081 18X^5 + 135844709636442562738530359267412X^4 + 264820055020066378800404676560301577 3X^3 - 133105372984783675604219287700441475727 2X^2 - 851361999940575945347507538147387002670418 35X - 19726932973896710808945510590486864789411518 2450.$$

Cas 7: n=15.

$$Q = X^{15} - 168885X^{13} - 1039770X^{12} + 11335105575X^{11} + 118923545844X^{10} - 387032023092195X^9 - 5188105608866010X^8 + 709849596981231144 0X^7 + 1065319810459786843 20X^6 - 669991116639536207948 16X^5 - 1034895708437017368274560X^4 + 273352630140600591383930880X^3 + 427196274944186700324145152 0X^2 - 248968054795407596596772536320X - 399215410285529090487789630 2592.$$

Nous traitons maintenant un cas à part, celui de $n = 8$, par des méthodes permettant de donner un polynôme à 4 paramètres.

Cas 8: n=8.

Nous donnons un polynôme défini sur le corps $\mathbb{Q}(m, n, r, b)$ où n, m, r et b sont des indéterminées. Posons $d = m^2 - 2n^2$: pour des spécialisations de m, n, r et b à des valeurs dans un corps de nombres K, le polynôme aura groupe de Galois D_8 sur K à condition que d et $4r^4 - b^2d$ soient non-triviaux et indépendants dans $K^*/(K^*)^2$. On pose

$$Q = X^8 - 4mX^6 + (5m^2 - 3d + \tfrac{mdb}{r^2})X^4 + (2dm - 2m^3 + \tfrac{m^2db}{r^2})X^2 + \tfrac{1}{16r^4}(4r^4m^4 + 4r^4d^4 - 8r^4m^2d - d^3b^2 + 2d^2b^2m^2 - m^4b^2d).$$

La méthode employée étant différente de celle du théorème 2.2, on donne la démonstration. On considère les huit racines de Q, qui sont données par

$$\pm\sqrt{(m+\sqrt{d})\big(1 \pm \tfrac{1}{2r}\sqrt{2r^2 + b\sqrt{d}}\big)} \text{ et } \pm\sqrt{(m-\sqrt{d})\big(1 \pm \tfrac{1}{2r}\sqrt{2r^2 - b\sqrt{d}}\big)}.$$

La démonstration se fait alors en trois étapes.

(1) On remarque que le corps de décomposition L_1 de Q contient un sous-corps L de groupe de Galois D_4 sur le corps de base K, donné par $L = K(\sqrt{2r^2 + b\sqrt{d}}, \sqrt{2r^2 - b\sqrt{d}})$.

(2) On montre que montrer que L_1 est bien de degré 16 sur K, c'est-à-dire que c'est une extension quadratique de L. Notons $\lambda = (m+\sqrt{d})(1 - \frac{1}{2r}\sqrt{2r^2 + b\sqrt{d}})$ et λ_1,λ_2 et λ_3 ses trois conjugués sur K: il suffit de montrer que $\lambda\lambda_i$ est un carré dans L pour $i = 1, 2, 3$. On constate que

$$\lambda\lambda_1 = \frac{1}{4r^2}(2r^2 - b\sqrt{d}),$$

$$\lambda\lambda_2 = n^2\left(1 + \frac{1}{2r}\sqrt{4r^2 + 2\sqrt{4r^2 - b^2d}}\right)^2, \text{ et}$$

$$\lambda\lambda_3 = n^2\left(1 + \frac{1}{2r}\sqrt{4r^2 - 2\sqrt{4r^4 - b^2d}}\right)^2.$$

(3) Le groupe de Galois de Q est donc d'ordre 16 avec un quotient isomorphe à D_4: il n'y a que trois possibilités dont une seule, D_8, possède un sous-groupe également isomorphe à D_4. Or ici c'est le cas puisque l'on a $\mathrm{Gal}\big(L_1/K(\sqrt{d})\big) \simeq D_4$.

Références

[B] A. Brumer, Preprint.

[JY] C. Jensen et N. Yui, Polynomials with D_p as Galois Group, *Jour. Numb. Th.* **15** (1982), 347-375.

[M] B.H. Matzat, *Konstruktive Galoistheorie*, LNM 1284, Springer-Verlag.

[Me] J-F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. reine und angew. Math. **343** (1983), 23-35.

[RYZ] G. Roland, N. Yui et D. Zagier, A Parametric Family of Quintic Polynomials with Galois Group D_5, *Jour. Numb. Th.* **15** (1982), 137-142.

[S] D. Saltman, Generic Galois Extensions and Problems in Field Theory, *Adv. in Math.* **43** (1982), 250-283.

[Sm] G. Smith, Generic Cyclic Polynomials of Odd Degree, *Communications in Algebra* **19 (12)** (1991), 3367-3391.