ACTA ARITHMETICA
103.1 (2002)

Réalisation de produits en couronne comme groupe de Galois de polynômes réciproques et construction de polynômes génériques

par

Franck Lalande (Paris)

Introduction. Soit K un corps de nombres de degré $2n$ qui n'est pas de type CM et de clôture galoisienne L. Pour que K soit engendré par un entier réciproque, il faut et il suffit que $\mathrm{Gal}(L/\mathbb{Q})$ soit inclus dans le produit en couronne $C_2 \wr S_n$ ou autrement dit que K possède un automorphisme d'ordre 2 (*cf.* [L1] si K admet un plongement réel et l'appendice pour le cas général). À ce point, il est naturel de demander si un sous-groupe de $C_2 \wr S_n$ peut être réalisé comme groupe de Galois du polynôme minimal d'un nombre réciproque et plus précisément, du polynôme minimal d'un nombre de Salem.

Le travail qui suit s'intéresse à cette question et se décompose en deux parties. Dans la première, on réalise explicitement le produit en couronne $C_2 \wr H$ (H sous-groupe transitif de S_n) comme groupe de Galois sur $\mathbb{Q}$ d'un polynôme irréductible g en supposant H réalisé par un polynôme f. C'est donc un problème de plongement bien connu mais la résolution explicite que nous donnons permet de choisir g réciproque et même polynôme minimal d'un nombre de Salem si le polynôme f est totalement réel.

Rappelons, avant de poursuivre, quelques définitions. Un corps K est dit de *type CM* s'il possède un automorphisme c d'ordre 2 tel que pour tout plongement σ de K dans $\mathbb{C}$, $\sigma \circ c = \overline{\sigma}$. Un *polynôme réciproque* est un polynôme P vérifiant $P(X) = X^d P(1/X)$ (d étant le degré de P), un *entier réciproque* est un entier algébrique dont le polynôme minimal est réciproque (*i.e.* un entier algébrique conjugué à son inverse), et un *nombre de Salem* est un entier algébrique réciproque, réel, strictement supérieur à 1, dont tous les autres conjugués ont un module inférieur ou égal à 1 avec au moins un conjugué de module 1. Le *produit en couronne* $C_2 \wr S_n$ est le stabilisateur du polynôme $X_1X_2 + X_3X_4 + \ldots + X_{2n-1}X_{2n}$ sous l'action du

2000 *Mathematics Subject Classification*: 11R06, 12F12.

groupe symétrique S_{2n}. C'est le produit semi-direct de $(C_2)^n$ par S_n pour l'action

$$S_n \times (C_2)^n \to (C_2)^n, \quad (h, (\sigma_1, \ldots, \sigma_n)) \mapsto (\sigma_{h^{-1}(1)}, \ldots, \sigma_{h^{-1}(n)}).$$

On définit de même le produit en couronne $C_2 \wr H$ pour tout sous-groupe H de S_n. Les résultats de cette première partie ont été annoncés dans [L2].

Dans la seconde partie, nous résolvons le problème de Noether pour le groupe $C_2 \wr S_n$. L'idée du programme d'Emmy Noether est la suivante. Si G est un groupe fini plongé dans le groupe symétrique S_n et k un corps de caractéristique nulle, le corps $E = k(X_1, \ldots, X_n)$ est naturellement muni d'une G-action et d'après un théorème d'Artin, l'extension E/E^G est galoisienne de groupe de Galois G (*cf.* [B, p. 64]). Il s'agit ensuite de pouvoir redescendre sur le corps k, ce que permet dans certains cas le théorème d'irréductibilité de Hilbert (*cf.* [S1]). Ce programme s'applique très bien au produit en couronne $G = C_2 \wr S_n$ et l'obtention d'une base de transcendance du corps E^G des invariants de E sous l'action de G permet de déterminer un polynôme générique pour le groupe $C_2 \wr S_n$. On montre également dans cette partie que le polynôme réciproque

$$P(X, t_1, \ldots, t_n) = X^{2n} + \sum_{i=1}^{n-1} t_i (X^{2n-i} + X^i) + t_n X^n + 1$$

est générique pour le groupe $C_2 \wr S_n$. On rappelle enfin que si G est un groupe fini et k un corps de caractéristique nulle, un polynôme $P(X, n_1, \ldots, n_r)$ est un *polynôme générique* (*cf.* [Sm]) sur k pour G si, comme polynôme en X sur le corps $k(n_1, \ldots, n_r)$, le groupe de Galois de P est isomorphe à G et si, pour tout corps K contenant k et toute extension L/K galoisienne de groupe G, le corps L est un corps de décomposition du polynôme obtenu en spécialisant $P(X, n_1, \ldots, n_r)$ en des valeurs $n_i \in K$.

1. Réalisation du groupe $C_2 \wr H$. Soit H un sous-groupe transitif du groupe symétrique S_n. On commence dans cette partie par réaliser explicitement le produit en couronne $C_2 \wr H$ comme groupe de Galois d'un polynôme $g \in \mathbb{Q}[X]$ de degré $2n$ dès que H est réalisé par un polynôme $f \in \mathbb{Q}[X]$. Puisque $C_2 \wr H$ est un produit semi-direct à noyau abélien, ce problème de plongement admet des solutions (*cf.* [S2, p. 18], ou [Sa, th. 3.12] ou [MM, ch. 4, th. 2.4]). Si l'on note K et L ($K \subset L$) les corps de décomposition respectifs des polynômes f et g, d'après la théorie de Kummer, on a $L = K(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n})$ où les α_i appartiennent à K et sont tels que le groupe qu'ils engendrent dans K^*/K^{*2} soit isomorphe à $(C_2)^n$. Ajoutons que Gow [G] a déjà traité ce problème dans le cas où le polynôme f est totalement réel.

Soit K un corps de nombres. Nous commençons par montrer deux lemmes concernant le groupe multiplicatif K^*/K^{*2}. Dans toute la suite, on notera $\mathbb{Z}_K$ l'anneau des entiers algébriques de K.

LEMME 1. *Soit f un élément non carré de $\mathbb{Z}_K[X]$. Pour tout entier naturel n, il existe un idéal premier $\mathcal{P}$ de $\mathbb{Z}_K$ de norme supérieure à n et un entier rationnel t pour lesquels $f(t)$ n'est pas un carré dans $\mathbb{Z}_K/\mathcal{P}$.*

Preuve. Supposons que ce lemme soit inexact. Il existe alors un entier naturel n tel que pour tout idéal $\mathcal{P}$ de $\mathbb{Z}_K$ de norme $N(\mathcal{P}) > n$ et tout entier rationnel t, $f(t)$ soit un carré dans $\mathbb{Z}_K/\mathcal{P}$.

Soit alors $\mathcal{P}$ un idéal premier de $\mathbb{Z}_K$ de norme $> n$, notons $K_\mathcal{P}$ le complété de K pour la valuation qu'il définit, $R_\mathcal{P}$ l'anneau de valuation de $K_\mathcal{P}$ et β son idéal de valuation (*i.e.* l'unique idéal maximal de $R_\mathcal{P}$). Le plongement $j : \mathbb{Z}_K \to R_\mathcal{P}$ induit par passage au quotient un homomorphisme $J : \mathbb{Z}_K/\mathcal{P} \to R_\mathcal{P}/\beta$ qui est en fait un isomorphisme (*cf.* [N, p. 89]), $f(t)$ est donc un carré dans $R_\mathcal{P}/\beta$ pour tout $t \in \mathbb{Z}$. Considérons alors le polynôme $g(X) = X^2 - f(t)$ appartenant à $\mathbb{Z}_K[X]$ et $\overline{g}(X) = X^2 - \overline{f(t)}$ son image dans $(R_\mathcal{P}/\beta)[X]$. La caractéristique étant différente de 2, seul le cas $\overline{f(t)} = 0$ peut permettre au polynôme $\overline{g}$ d'avoir une racine double. Ainsi, si t n'est pas une racine de f et si $f(t) \notin \mathcal{P}$, $f(t)$ est un carré non nul dans $\mathbb{Z}_K/\mathcal{P}$ et comme $\mathbb{Z}_K \cap \beta = \mathcal{P}$, $\overline{f(t)}$ est un carré non nul dans $R_\mathcal{P}/\beta$. Le polynôme $\overline{g}(X) = X^2 - \overline{f(t)}$ admet alors une racine simple dans $R_\mathcal{P}/\beta$ et d'après le lemme de Hensel (*cf.* [N, p. 211]), g admet une racine dans $R_\mathcal{P}$ et $f(t)$ est alors un carré dans $R_\mathcal{P}$. La finitude des idéaux contenant $f(t) \neq 0$, des idéaux de norme $N(\mathcal{P}) < n$ et des places archimédiennes de K permet d'affirmer que $f(t)$ est un carré dans presque tous les complétés de K. D'après [Om] (résultat 65.15), $f(t)$ est alors un carré dans K. Ceci contredit le théorème d'irréductibilité de Hilbert (*cf.* [S1]) car le polynôme f n'étant pas un carré dans $\mathbb{Z}_K[X]$, le polynôme $h(X, Y) = Y^2 - f(X)$ est irréductible dans $\mathbb{Z}_K[X, Y]$ et donc d'après ce théorème, il existe une infinité d'entiers rationnels t pour lesquels le polynôme $g(Y, t) = Y^2 - f(t)$ est irréductible dans $\mathbb{Z}_K[Y]$.

LEMME 2. *Soient K un corps de nombres et $\alpha_1, \ldots, \alpha_n$ des entiers de $\mathbb{Z}_K$ deux à deux distincts. Il existe un entier rationnel t pour lequel le sous-groupe multiplicatif de K^*/K^{*2} engendré par les $\alpha_i + t$, $1 \leq i \leq n$, est d'ordre 2^n.*

Preuve. Soient t un entier rationnel et G_t le sous-groupe multiplicatif de K^*/K^{*2} engendré par les $\alpha_i + t$, $1 \leq i \leq n$. Si l'ordre de G_t est strictement inférieur à 2^n, il existe une partie I non vide de $\{1, \ldots, n\}$ pour laquelle $\prod_{i \in I}(\alpha_i + t)$ est un carré dans K. Notons alors $I_1, \ldots, I_k$ les différentes parties non vides de $\{1, \ldots, n\}$ et considérons pour tout $j \in \{1, \ldots, k\}$ le polynôme P_j défini par $P_j(X) = \prod_{i \in I_j}(X + \alpha_i)$. Les polynômes P_j ne

sont pas des carrés dans $\mathbb{Z}_K[X]$, donc d'après le lemme 1, pour chaque $j \in \{1, \ldots, k\}$, il existe un idéal premier $\mathcal{P}_j$ de $\mathbb{Z}_K$ et un entier rationnel t_j pour lesquels $P_j(t_j)$ n'est pas un carré dans $\mathbb{Z}_K/\mathcal{P}_j$. Ces idéaux peuvent de plus être choisis de norme aussi grande qu'on le souhaite, ce qui permet de les supposer tous distincts. Le théorème chinois assure alors l'existence d'un entier rationnel t_0 congru à t_j modulo $\mathcal{P}_j$ pour tout j et par suite, $P_j(t_0) \equiv P_j(t_j) \pmod{\mathcal{P}_j}$, n'est pas un carré dans $\mathbb{Z}_K/\mathcal{P}_j$ et a fortiori dans $\mathbb{Z}_K$. Pour toute partie I de $\{1, \ldots, n\}$, $\prod_{i\in I}(\alpha_i + t_0)$ n'est alors pas un carré dans $\mathbb{Z}_K$ et G_{t_0} est un sous-groupe de K^*/K^{*2} d'ordre 2^n. Ceci achève la démonstration du lemme.

Remarque. Tout entier $t \equiv t_0 \pmod{\mathcal{P}_1\mathcal{P}_2 \ldots \mathcal{P}_k}$ satisfait également le lemme 2. L'entier t peut donc être choisi aussi grand qu'on le souhaite.

Nous pouvons maintenant énoncer la solution du problème de plongement annoncé dans l'introduction, bien connue et déjà présente dans [Sa] et [MM].

Proposition 1. *Soit $f \in \mathbb{Z}[X]$ un polynôme irréductible, unitaire de degré n et de groupe de Galois H. Il existe alors $g \in \mathbb{Z}[X]$ irréductible, unitaire de degré $2n$ et dont le groupe de Galois est le produit en couronne $C_2 \wr H$. De plus, si K et L désignent les corps de décomposition respectifs des polynômes f et g, $K \subset L$ et $\mathrm{Gal}(L/K) = C_2^n$.*

Preuve. Notons $\alpha_1, \ldots, \alpha_n$ les racines de f. D'après le lemme 2, il existe un entier rationnel t pour lequel l'ordre du sous-groupe de K^*/K^{*2} engendré par les $\alpha_i + t$, $1 \leq i \leq n$, est 2^n. Considérons alors le polynôme g de $K[X]$ défini par $g(X) = \prod_{i=1}^{n}(X^2 - (\alpha_i + t))$. Ce polynôme est en fait à coefficients dans $\mathbb{Q}$ puisque $\sigma(g) = g$ pour tout $\sigma \in H$ et comme de plus $[\mathbb{Q}(\sqrt{\alpha_1 + t}) : \mathbb{Q}] = 2n$, il est irréductible. D'autre part, puisque le sous-groupe de K^*/K^{*2} engendré par les $\alpha_i + t$ est d'ordre 2^n, d'après la théorie de Kummer, $\mathrm{Gal}(L/K) = (C_2)^n$. Ainsi, $\mathrm{Gal}(L/\mathbb{Q})$ est une extension de H par $(C_2)^n$ incluse dans le produit en couronne $C_2 \wr H$, il lui est donc égal. Ceci achève cette démonstration.

Théorème 1. *Il existe un polynôme $h \in \mathbb{Z}[X]$ irréductible, unitaire de degré $2n$ et réciproque dont le corps de décomposition L satisfait le problème de plongement de la proposition* 1.

Preuve. D'après la proposition 1, on peut trouver un entier rationnel t tel que le polynôme $g(X) = \prod_{i=1}^{n}(X^2 - (\alpha_i + t))$ ait pour groupe de Galois le produit en couronne $C_2 \wr H$. L'entier t peut être choisi de telle sorte que le corps engendré par une racine de g ne soit pas de type CM. En effet, si f admet une racine réelle α, d'après la remarque qui suit le lemme 2, t peut être choisi suffisamment grand pour que $\alpha + t$ soit positif et g admet alors une racine réelle $\sqrt{\alpha + t}$. Plaçons nous maintenant dans le cas où f

est totalement imaginaire, notons a une racine de g et supposons que $\mathbb{Q}(a)$ soit de type CM. Soit $L = \mathbb{Q}(a_1, \ldots, a_{2n})$ le corps de décomposition de g. Le groupe de Galois de $L/\mathbb{Q}$ est alors inclus dans $C_2 \wr S_n$ où $\mathrm{Gal}(L/\mathbb{Q})$ est vu comme un groupe permutant les racines de g ordonnées de telle sorte que $a_{2k} = \overline{a}_{2k-1}$. Mais par construction, $\mathrm{Gal}(L/\mathbb{Q}) = C_2 \wr H$ est inclus dans $C_2 \wr S_n$ pour un ordre où une racine a_{2k} est couplée avec son opposé $a_{2k-1} = -a_{2k}$. Mais alors l'automorphisme de L qui échange a_1 et son opposé et laisse toutes les autres racines fixes (c'est l'élément $(1, 0, \ldots, 0) \in (C_2)^n \subset C_2 \wr H$) ne stabilise pas globalement l'ensemble des blocs $(a_i, \overline{a}_i)$. Cela contredit le fait que $\mathbb{Q}(a)$ puisse être de type CM. Par conséquent, d'après [L1, théorème 2] pour le cas réel et l'appendice pour le cas totalement imaginaire, le corps $\mathbb{Q}(a)$ peut être engendré par un entier réciproque η dont le polynôme minimal h est réciproque et de groupe de Galois $C_2 \wr H$.

Remarque. De manière analogue, on réalise dans [L3] le produit en couronne $C_2 \wr H$ comme groupe de Galois du polynôme minimal d'un nombre de Salem dès lors que H est réalisé comme groupe de Galois d'un polynôme f irréductible, totalement réel et appartenant à $\mathbb{Q}[X]$.

Exemple. Réalisons par exemple le produit en couronne $C_2 \wr C_5$ comme groupe de Galois du polynôme minimal d'un nombre de Salem. Il nous faut pour cela un polynôme $f \in \mathbb{Q}[X]$, totalement réel de groupe de Galois C_5. Le polynôme $f(X) = X^5 - 10X^3 - 5X^2 + 10X - 1$ vérifie ces conditions. Notons $\alpha_1, \ldots, \alpha_5$ ses racines. D'après ce qui précède, il existe $t \in \mathbb{Z}$ pour lequel le polynôme $g_t(X) = \prod_{i=1}^{5}(X^2 - (\alpha_i + t))$ admet $C_2 \wr C_5$ pour groupe de Galois. On peut même choisir $t \in \mathbb{Q}$ pour que g_t ait en outre exactement deux racines réelles [L3]. Le rationnel $t = -1$ convient et $g_{-1}(X) = X^{10} + 5X^8 - 25X^4 - 25X^2 - 5$. D'après [L1] (théorème 1), le corps engendré par une racine réelle de g_{-1} est engendré par un nombre de Salem et en utilisant la remarque 1 de [L1], on construit un polynôme de Salem vérifiant les conditions souhaitées. À l'aide du logiciel Pari [P], on obtient le polynôme $h(X) = X^{10} - 549210(X^9 + X) - 140115(X^8 + X^2) + 642760(X^7 + X^3) - 59310(X^6 + X^4) - 836828X^5 + 1$, polynôme minimal du nombre de Salem $\tau = 549210.255118\ldots$

2. Utilisation du programme d'Emmy Noether et construction de polynômes génériques. Soient k un corps de caractéristique nulle et n un entier naturel. Le groupe $G = C_2 \wr S_n$ vu comme sous-groupe du groupe symétrique S_{2n} agit de manière naturelle sur le corps $E = k(X_1, \ldots, X_{2n})$ des fractions rationnelles à $2n$ indéterminées en posant pour tout $\sigma \in G$ et tout $R(X_1, \ldots, X_{2n}) \in E$,

$$\sigma \cdot R(X_1, \ldots, X_{2n}) = R(X_{\sigma(1)}, \ldots, X_{\sigma(2n)}).$$

On se propose dans un premier temps de déterminer explicitement le corps des invariants de E, noté E^G, sous l'action de G. Nous utiliserons dans la suite de ce paragraphe les notations suivantes : Pour tout couple (i,j) appartenant à $\{1,\dots,n\}^2$, on pose

$$b_i = \sum_{1\leq k_1<\ldots<k_i\leq n} X_{2k_1-1}X_{2k_1}X_{2k_2-1}X_{2k_2}\dots X_{2k_i-1}X_{2k_i},$$

$$q_{i,j} = \sum_{1\leq k_1<\ldots<k_i\leq n,\, k_l\neq j} X_{2k_1-1}X_{2k_1}X_{2k_2-1}X_{2k_2}\dots X_{2k_i-1}X_{2k_i}$$

si $i\neq n$ et $q_{n,j}=1$. On a alors le résultat suivant :

Théorème 2. *Sous les notations ci-dessus, $E^G = k(\alpha_1,\dots,\alpha_{2n})$ où pour tout $i\in\{1,\dots,n\}$, $\alpha_i = b_i$ et $\alpha_{n+i} = \sum_{k=1}^{n} q_{i,k}(X_{2k-1}+X_{2k})$. Autrement dit, le corps des $C_2\wr S_n$-invariants est rationnel.*

Preuve. Le corps E est une extension algébrique galoisienne de E^G de groupe de Galois G d'ordre $n!2^n$ et il est clair que le corps $F=k(\alpha_1,\dots,\alpha_{2n})$ est inclus dans E^G. Il suffit donc de montrer que E est une extension algébrique de F de degré inférieur ou égal à $n!2^n$.

Notons $\widetilde{F}$ le corps engendré par F et les $X_{2i-1}X_{2i}$. Comme chaque élément $X_{2i-1}X_{2i}$ annule le polynôme à coefficients dans F, $P(X)=X^n-\alpha_1X^{n-1}+\alpha_2X^{n-2}+\ldots+(-1)^n\alpha_n$, le degré de l'extension $\widetilde{F}/F$ est inférieur ou égal à $n!$. Par récurrence, nous allons maintenant montrer que les éléments $X_{2i-1}+X_{2i}$ appartiennent à $\widetilde{F}$. Pour plus de précisions, les $q_{i,j}$ seront désormais notés $q_{i,j}^{(n)}$, ce sont clairement des éléments de $\widetilde{F}$. Le vecteur $(X_{2i-1}+X_{2i})_{i=1,\dots,n}$ est solution du système linéaire à coefficients dans $\widetilde{F}$

$$(\Sigma)\qquad \begin{cases} (X_1+X_2)q_{1,1}^{(n)}+\ldots+(X_{2n-1}+X_{2n})q_{1,n}^{(n)}=\alpha_{n+1},\\ (X_1+X_2)q_{2,1}^{(n)}+\ldots+(X_{2n-1}+X_{2n})q_{2,n}^{(n)}=\alpha_{n+2},\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ (X_1+X_2)q_{n,1}^{(n)}+\ldots+(X_{2n-1}+X_{2n})q_{n,n}^{(n)}=\alpha_{2n}, \end{cases}$$

qui est un système inversible. En effet, si l'on note $\Delta_n(X_1,X_2,\dots,X_{2n})$ le déterminant de ce système, en posant $X_{2n}=0$, on obtient

$$\Delta_n(X_1,\dots,X_{2n-1},0)=\begin{vmatrix} q_{1,1}^{(n-1)} & q_{1,2}^{(n-1)} & \dots & q_{1,n-1}^{(n-1)} & q_{1,n}^{(n)}\\ q_{2,1}^{(n-1)} & q_{2,2}^{(n-1)} & \dots & q_{2,n-1}^{(n-1)} & q_{2,n}^{(n)}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ q_{n-2,1}^{(n-1)} & q_{n-2,2}^{(n-1)} & \dots & q_{n-2,n-1}^{(n-1)} & q_{n-2,n}^{(n)}\\ 0 & 0 & \dots & 0 & q_{n-1,n}^{(n)}\\ 1 & 1 & \dots & 1 & 1 \end{vmatrix},$$

ce qui en développant suivant l'avant-dernière ligne donne la relation

$$\Delta_n(X_1,\dots,X_{2n-1},0) = -q^{(n)}_{n-1,n}\Delta_{n-1}(X_1,\dots,X_{2n-2}).$$

Ainsi, si $\Delta_{n-1} \not\equiv 0$ alors $\Delta_n \not\equiv 0$ et comme de plus $\Delta_2 = X_3X_4 - X_1X_2 \not\equiv 0$, $\Delta_n \not\equiv 0$ pour tout entier n. Le système (Σ) est donc un système de Cramer et par suite $X_{2i-1}+X_{2i}$ appartient à $\widetilde{F}$ pour tout $i = 1,\dots,n$. Enfin, comme X_{2i-1} et X_{2i} sont racines du polynôme $f(X) = X^2 - (X_{2i-1} + X_{2i})X + X_{2i-1}X_{2i}$ appartenant à $\widetilde{F}[X]$, $F(X_1,\dots,X_{2n}) = k(X_1,\dots,X_{2n})$ est une extension de $\widetilde{F}$ de degré $\leq 2^n$ et donc de F de degré $\leq n!2^n$. On a donc $F \subset E^G \subset E$ et $[E : F] \leq [E : E^G]$, ce qui entraîne $F = E^G$ et termine cette démonstration.

Soit alors le polynôme $H(X) = \prod_{i=1}^{2n}(X - X_i)$ appartenant à $E[X]$. Ce polynôme est invariant sous l'action de G, il s'écrit donc sous la forme $H(X) = X^{2n} + \sum_{i=1}^{2n} R_i(\alpha_1,\dots,\alpha_{2n})X^{2n-i}$ où les R_i sont des fractions rationnelles à coefficients dans k. Une conséquence immédiate du théorème 2 et du théorème d'irréductibilité de Hilbert est alors le corollaire suivant :

Corollaire 1. *Soit k un corps hilbertien. Sous les notations ci-dessus, le polynôme $h(X) = X^{2n} + r_1X^{2n-1} + \ldots + r_{2n}$ obtenu à partir de $H(X)$ en spécialisant les α_i en des éléments de k, admet $C_2 \wr S_n$ comme groupe de Galois sur k pour une infinité de spécialisations.*

Corollaire 2. *Le polynôme $H(X, \alpha_1,\dots,\alpha_{2n})$ est un polynôme générique sur k pour le groupe $G = C_2 \wr S_n$.*

Preuve. Tout d'abord, comme polynôme en X sur le corps $k(\alpha_1,\dots,\alpha_{2n})$, un corps de décomposition de H a un groupe de Galois égal à $C_2 \wr S_n$. D'autre part, pour tout corps k' contenant k et toute extension L/k' de groupe $C_2 \wr S_n$, le corps L est le corps de décomposition d'un polynôme obtenu en spécialisant $H(X, \alpha_1,\dots,\alpha_{2n})$ en des valeurs $\alpha_i \in k'$. En effet, on a une représentation fidèle et transitive de $\mathrm{Gal}(L/k')$ dans le groupe symétrique S_{2n}, le corps L est donc le corps de décomposition d'un polynôme f irréductible de degré $2n$ appartenant à $k'[X]$. Notons $x_1,\dots,x_{2n}$ les racines de f dans L. Le polynôme f est alors obtenu à partir du polynôme H en spécialisant les α_i en les valeurs $\alpha_i(x_1,\dots,x_{2n})$ appartenant à k'.

Remarque. L'existence d'un polynôme générique pour $C_2 \wr S_n$ a déjà été montrée dans [Sa, théorème 3.3].

À l'aide du logiciel Pari, le polynôme H a été calculé dans [L3] pour $n = 2, 3, 4$. Son expression est longue et compliquée. Nous terminons ce travail en montrant que le polynôme générique réciproque est générique pour $C_2 \wr S_n$. C'est l'objet du résultat suivant.

THÉORÈME 3. *Soit k un corps de caractéristique 0. Le polynôme*

$$P(X,t_1,\dots,t_n)=X^{2n}+\sum_{i=1}^{n-1}t_i(X^{2n-i}+X^i)+t_nX^n+1$$

est un polynôme générique pour le groupe $C_2\wr S_n$ sur le corps k.

Preuve. Comme polynôme en X sur le corps $K=k(t_1,\dots,t_n)$, le polynôme P est irréductible et admet $C_2\wr S_n$ pour groupe de Galois. En effet, on a clairement $\mathrm{Gal}_K(P)\subset C_2\wr S_n$ et d'autre part, si l'on considère une extension L de k de groupe de Galois $C_2\wr S_n$, nous verrons dans la deuxième partie de cette démonstration que le corps L est le corps de décomposition d'un polynôme réciproque appartenant à $k[X]$. Par conséquent, il existe des spécialisations du polynôme P dont le groupe de Galois est $C_2\wr S_n$. Mais d'après un principe bien connu (*cf.* [La, p. 366]), le groupe de Galois ne peut pas "grossir" lors d'une spécialisation. Finalement, $\mathrm{Gal}_K(P)=C_2\wr S_n$.

Il s'agit donc de montrer que toute extension galoisienne de k (respectivement d'un corps k' contenant k) de groupe $C_2\wr S_n$ est le corps de décomposition d'un polynôme obtenu en spécialisant les t_i en des valeurs de k (respectivement k'), et par conséquent, le corps de décomposition d'un polynôme réciproque à coefficients dans k (respectivement k').

Soit L une extension galoisienne de k de groupe $C_2\wr S_n$. Le corps L est alors le corps de décomposition d'un polynôme f irréductible de degré $2n$ appartenant à $k[X]$. Notons alors $\alpha_1,\dots,\alpha_{2n}$ les racines de f ordonnées de telle sorte que pour cet ordre, $\mathrm{Gal}_k(f)=C_2\wr S_n$. Posons $K=k(\alpha_1)$, $F=k(\alpha_1+\alpha_2,\alpha_1\alpha_2)$ et F^{gal} la clôture galoisienne de F. On vérifie aisément que $\mathrm{Gal}(F^{\mathrm{gal}}/k)=S_n$. D'autre part, $\alpha_2\in k(\alpha_1)$. En effet, le sous-groupe de $\mathrm{Gal}_k(f)=C_2\wr S_n$ qui fixe α_1 et α_2 est un sous-groupe d'indice $2n$ isomorphe à $C_2\wr S_{n-1}$. Les extensions $k(\alpha_1,\alpha_2)/k$ et $k(\alpha_1)/k$ sont donc égales puisque toutes deux de degré $2n$. Le corps K est donc une extension quadratique de F ; nous noterons σ le générateur de $\mathrm{Gal}(K/F)=C_2$. La fin de cette démonstration utilise deux lemmes que nous démontrerons à la suite de cette preuve.

LEMME 3. *Sous les notations ci-dessus, il existe $x\in K$ tel que $y=x/\sigma(x)$ n'appartienne pas à F.*

Si on note $\alpha=y+1/y$, y est alors racine du polynôme $g(X)=X^2-\alpha X+1$ appartenant à $F[X]$ et $K=F(\sqrt{\alpha^2-4})$. Le nombre y est alors réciproque mais n'a malheureusement aucune raison d'engendrer le corps K car a priori α n'est pas un générateur du corps F. Le lemme qui suit va nous permettre de lever ce problème.

LEMME 4. *Sous les notations ci-dessus, il existe un générateur β de F tel que K soit le corps de décomposition du polynôme $h(X)=X^2+\beta X+1$ appartenant à $F[X]$.*

Notons alors u une racine du polynôme h et $u^{(1)}, u^{(2)}, \ldots, u^{(2n)}$ les conjugués de u sur k. Il est clair que $u \neq u^{(2)}$ et d'autre part, s'il existait $j \in \{2, \ldots, n\}$ tel que $u^{(2j-1)} = u$ (respectivement $u^{(2j)} = u$), comme $\mathrm{Gal}(L/k) = C_2 \wr S_n$, on aurait $u^{(2j)} = u^{(2)}$ (respectivement $u^{(2j-1)} = u^{(2)}$) et par conséquent, β serait égal à β_j, ce qui est absurde car β engendre F. Le nombre u ainsi défini est alors un nombre algébrique réciproque qui engendre K sur k. Son polynôme minimal sur k est donc un polynôme réciproque dont L est le corps de décomposition. Ceci achève la démonstration du théorème.

Revenons maintenant aux démonstrations des deux lemmes 3 et 4.

Preuve du lemme 3. Soit x appartenant à K et n'appartenant pas à F et posons $y = x/\sigma(x)$. Dire que y n'appartient pas à F revient à dire que x^2 n'appartient pas à F. En effet, $y \in F$ si et seulement si $\sigma(y) = y$, ce qui est equivalent à $x^2 = \sigma(x^2)$. D'autre part, si x^2 appartient à F, $x' = x + z$ où $z \in F$ a un carré qui n'est pas dans F et on remplace x par x'.

Preuve du lemme 4. Dire que K est un corps de décomposition de h revient à dire que $K = F(\sqrt{\alpha^2 - 4}) = F(\sqrt{\beta^2 - 4})$ et donc qu'il existe $a, b \in F$ tels que $\sqrt{\alpha^2 - 4} = a + b\sqrt{\beta^2 - 4}$. En élévant au carré, on obtient $(\alpha^2 - 4) - a^2 - b^2(\beta^2 - 4) = 2ab\sqrt{\beta^2 - 4}$ et donc $a = 0$. Par conséquent, β doit vérifier $b^2(\beta^2 - 4) = (\alpha^2 - 4)$ et si l'on note $\delta = \alpha^2 - 4$, le couple $(\beta, 1/b)$ est solution de l'équation $X^2 - \delta Y^2 = 4$.

La courbe $\mathcal{C}$ d'équation $X^2 - \delta Y^2 = 4$ est de genre 0 et admet un point rationnel (*i.e.* à coordonnées dans F) évident, le point $(2, 0)$. Elle admet donc une infinité de points rationnels que l'on peut paramétrer en considérant les points d'intersection de $\mathcal{C}$ avec la droite D_t d'équation $X = tY + 2$ ($t \in F$). Les points rationnels de $\mathcal{C}$ sont alors les points $\left(-2\frac{t^2+\delta}{t^2-\delta}, \frac{-4t}{t^2-\delta}\right)$. Ainsi, pour tout $t \in F$, le polynôme

$$f_t(X) = X^2 - \beta_t X + 1 \quad \text{où} \quad \beta_t = -2\frac{t^2 + \delta}{t^2 - \delta}$$

admet K pour corps de décomposition. En effet,

$$\sqrt{\beta_t^2 - 4} = \frac{-4t}{t^2 - \delta}\sqrt{\alpha^2 - 4}.$$

Il reste à voir que l'on peut choisir t de telle sorte que β_t soit un générateur de F. Notons $\beta_t^{(i)}$ ($i \in \{1, \ldots, n\}$) les conjugués de β_t sur k. Si β_t n'engendre pas F alors il existe $i \neq 1$ tel que $\beta_t = \beta_t^{(i)}$, ce qui revient à dire que $(t_i/t)^2 = \delta_i/\delta$. D'autre part, comme $\mathrm{Gal}(F^{\mathrm{gal}}/k) = S_n$ est un groupe 2-transitif, on déduit de la condition ci-dessus que $(t_j/t)^2 = \delta_j/\delta$ pour tout $j \in \{1, \ldots, n\}$. Considérons alors un générateur t' de F dont le carré t'^2 n'appartient pas à k. Si aucun des deux nombres $\beta_{t'}$ et $\beta_{t'^2}$ n'engendre F alors pour tout $j \in \{1, \ldots, n\}$, $(t'_j/t')^2 = \delta_j/\delta = (t'^2_j/t'^2)^2$ et

par suite, $t'^2 = t_j'^2$ pour tout j, ce qui est absurde car t'^2 n'appartient pas à k. On peut donc choisir t de telle sorte que β_t engendre F.

REMARQUE. Un autre polynôme générique simple pour $C_2 \wr S_n$ peut être obtenu en substituant X^2 à X dans le polynôme générique général de S_n. Ceci peut se déduire du théorème 3.3 de [Sa]. Le groupe de Galois de ce polynôme a par ailleurs été calculé dans [Od].

Références

[B] N. Bourbaki, *Algèbre*, *Chapitre 5*, Masson, 1981.

[G] R. Gow, *Construction of some wreath products as Galois groups of normal real extensions of the rationals*, J. Number Theory 24 (1986), 360–372.

[L1] F. Lalande, *Corps de nombres engendrés par un nombre de Salem*, Acta Arith. 88 (1999), 191–200.

[L2] —, *Problème inverse de Galois et nombres réciproques*, C. R. Acad. Sci. Paris Sér. I 328 (1999), 745–747.

[L3] —, *Problèmes de Galois et nombres algébriques réciproques*, Thèse, Université Paris 6, 2000.

[La] S. Lang, *Algebra*, Addison-Wesley, 1984.

[MM] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer, 1999.

[N] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1974.

[Od] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. 51 (1985), 385–414.

[Om] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, 1963.

[P] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP*, Version 1.39, 1995.

[Sa] D. J. Saltman, *Generic Galois extension and problems in field theory*, Adv. in Math. 43 (1982), 250–283.

[S1] J. P. Serre, *Lectures on the Mordell–Weil Theorem*, translated and edited by M. Brown from notes by M. Waldschmidt, 2nd ed., Aspects of Math., 1990.

[S2] —, *Topics in Galois Theory*, Res. Notes Math., Jones and Bartlett, 1992.

[Sm] G. W. Smith, *Generic cyclic polynomials of odd order*, Comm. Algebra 19 (1991), 3367–3391.

Département de Mathématiques
Université Paris Sud
Bât. 425
91405 Orsay Cedex, France
E-mail: Franck.Lalande@math.u-psud.fr

APPENDICE

Corps de nombres engendrés par des entiers réciproques

par

Joseph Oesterlé

Dans ce qui suit, K désigne un corps de nombres, n son degré, Σ l'ensemble des plongements de K dans $\mathbb{C}$, et U_K le groupe des unités de K, c'est-à-dire des éléments inversibles de l'anneau des entiers de K.

On définit un homomorphisme $u : U_K \to \mathbb{R}^\Sigma$ en posant $u(x) = (\log|\sigma(x)|)_{\sigma\in\Sigma}$. Le noyau de u est fini et se compose des racines de l'unité de K ; l'image de u est un réseau de l'espace vectoriel formé des $(a_\sigma)_{\sigma\in\Sigma} \in \mathbb{R}^\Sigma$ tels que $a_{\overline{\sigma}} = a_\sigma$ et $\sum a_\sigma = 0$.

1. Unités de K anti-invariantes par une involution

Proposition 1. *Soit ι un automorphisme d'ordre 2 de K. Il existe $x \in U_K$ tel que :*

(a) $\iota(x) = x^{-1}$;

(b) *pour $\sigma \in \Sigma$ tel que $\sigma \circ \iota \neq \overline{\sigma}$, on a $|\sigma(x)| \neq |\sigma'(x)|$ si $\sigma' \in \Sigma$ est distinct de σ et $\overline{\sigma}$.*

On a $u \circ \iota = \iota' \circ u$ où ι' désigne l'involution $(a_\sigma)_{\sigma\in\Sigma} \mapsto (a_{\sigma\circ\iota})_{\sigma\in\Sigma}$ de $\mathbb{R}^\Sigma$. Il en résulte que l'image par u de l'ensemble des unités $x \in U_K$ telles que $\iota(x) = x^{-1}$ est un réseau du sous-espace vectoriel V de $\mathbb{R}^\Sigma$ formé des familles $(a_\sigma)_{\sigma\in\Sigma}$ telles que $a_{\sigma\circ\iota} = -a_\sigma$ et $a_{\overline{\sigma}} = a_\sigma$ pour tout $\sigma \in \Sigma$.

Notons $H_{\sigma,\sigma'}$ l'hyperplan de $\mathbb{R}^\Sigma$ formé des éléments dont les coordonnées d'indices σ et σ' sont égales. L'espace vectoriel V n'est contenu dans aucun des hyperplans $H_{\sigma,\sigma'}$ pour $\sigma \circ \iota \neq \overline{\sigma}$ et σ' distinct de σ et $\overline{\sigma}$. Il existe donc un élément x de U_K tel que $\iota(x) = x^{-1}$, dont l'image par u n'appartient à aucun de ces hyperplans, d'où la proposition.

2. Corps engendrés par des entiers réciproques. Un entier de K est dit *réciproque* s'il est conjugué à son inverse et distinct de celui-ci. Si x est un tel entier, x appartient à U_K. Si de plus x engendre K, il existe un automorphisme ι de K d'ordre 2 tel que $\iota(x) = x^{-1}$. Nous nous intéressons à la réciproque. Nous commençons par examiner le cas où K possède un plongement réel.

Théorème 1. *Soit K un corps de nombres qui possède au moins un plongement réel. Si ι est un automorphisme d'ordre 2 de K, il existe un entier réciproque x tel que $\iota(x) = x^{-1}$, qui engendre K.*

Choisissons en effet $x \in U_K$ satisfaisant les conditions de la proposition 1. On a $\iota(x) = x^{-1}$, donc x est un entier réciproque. Soit σ un plongement réel de K. On a $\sigma \circ \iota \neq \sigma = \overline{\sigma}$. Par suite, pour tout plongement $\sigma' \in \Sigma$ distinct de σ, on a $|\sigma(x)| \neq |\sigma'(x)|$, et a fortiori $\sigma(x) \neq \sigma'(x)$. Il en résulte que x engendre K.

Passons au cas totalement imaginaire. Rappelons qu'un corps K totalement imaginaire est dit de type CM s'il possède un automorphisme c d'ordre 2 tel que $\sigma \circ c = \overline{\sigma}$ pour tout $\sigma \in \Sigma$.

THÉORÈME 2. *Soit K un corps totalement imaginaire qui n'est pas de type CM. Pour que K soit engendré par un entier réciproque, il faut et il suffit qu'il possède un automorphisme d'ordre* 2.

La condition est clairement nécessaire. Démontrons qu'elle est suffisante. Soit ι un automorphisme d'ordre 2 de K. Choisissons $x \in U_K$ satisfaisant les conditions de la proposition 1. On a $\iota(x) = x^{-1}$, donc x est un entier réciproque. Comme K n'est pas de type CM, il possède un plongement complexe τ tel que $\tau \circ \iota \neq \overline{\tau}$. On a alors $|\tau(x)| \neq |\sigma(x)|$, et a fortiori $\tau(x) \neq \sigma(x)$ pour tout σ dans Σ distinct de τ et $\overline{\tau}$. Distinguons alors deux cas :

(a) $\tau(x) \neq \overline{\tau}(x)$; dans ce cas x engendre K.

(b) $\tau(x) = \overline{\tau}(x)$; dans ce cas x engendre un sous-corps K_0 de K sur lequel K est de degré 2, et l'automorphisme ι' d'ordre 2 de K qui fixe K_0 est tel que $\tau \circ \iota' = \overline{\tau}$. On a donc $\iota' \neq \iota$. Le raisonnement fait pour τ montre plus généralement que $\sigma \circ \iota' = \overline{\sigma}$ pour tout $\sigma \in \Sigma$ tel que $\sigma \circ \iota \neq \overline{\sigma}$. On a en particulier

$$\tau \circ \iota \circ \iota' = \overline{\tau \circ \iota} = \overline{\tau} \circ \iota = \tau \circ \iota' \circ \iota$$

de sorte que ι et ι' commutent, et que $J = \iota \circ \iota'$ est un automorphisme d'ordre 2 de K. Pour tout $\sigma \in \Sigma$, on a $\sigma \circ \iota = \overline{\sigma}$ ou $\sigma \circ \iota' = \overline{\sigma}$, d'où $\sigma \circ J \neq \overline{\sigma}$. On reprend alors le raisonnement du début en remplaçant ι par J, ce qui montre bien que, ou bien K est engendré par un entier réciproque y tel que $J(y) = y^{-1}$, ou bien K possède un automorphisme J' tel que $\sigma \circ J' = \overline{\sigma}$ pour tout $\sigma \in \Sigma$. Or cette dernière alternative est exclue puisque K n'est pas de type CM.

REMARQUE. Sous les hypothèses du théorème 2, je n'affirme pas que, pour tout automorphisme ι d'ordre 2 de K, on puisse trouver un entier réciproque x qui engendre K et soit tel que $\iota(x) = x^{-1}$.

Reçu le 3.8.2000
et révisé le 13.8.2001 (3867)