JOURNAL OF ALGEBRA 131, 483–495 (1990)

Extensions régulières de $\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_n$

JEAN-FRANÇOIS MESTRE

École Normale Supérieure,
45 rue d'Ulm, 75230 Paris, Cedex 05, France

Communicated by Walter Feit

Received January 9, 1989

DEDICATED TO WALTER FEIT ON THE OCCASION OF HIS 60TH BIRTHDAY

1. INTRODUCTION

Si n est un entier naturel $\geqslant 4$, notons $\tilde{A}_n$ l'unique extension centrale non scindée du groupe alterné A_n par $\mathbf{Z}/2\mathbf{Z}$.

Dans [7], N. Vila prouve qu'il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_n$ pour les valeurs suivantes de n:

(i) $n \equiv 0, 1 \bmod 8$,

(ii) $n \equiv 2 \bmod 8$ et n somme de 2 carrés,

(iii) $n \equiv 3 \bmod 8$, et satisfaisant à une certaine relation qui semble toujours vérifiée.

Par ailleurs, W. Feit [1] a démontré que $\tilde{A}_5$ et $\tilde{A}_7$ sont groupes de Galois d'une infinité d'extensions de $\mathbf{Q}$.

Nous prouvons ici le théorème suivant:

THÉORÈME 1. *Pour tout $n \geqslant 4$, il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_n$.*

COROLLAIRE. *Pour tout $n \geqslant 4$, il existe une infinité d'extensions de $\mathbf{Q}$ deux à deux disjointes de groupe de Galois $\tilde{A}_n$.*

Je tiens à exprimer ma vive reconnaissance à G. Henniart, J. Oesterlé, et J.-P. Serre: plusieurs points importants de la démonstration de ce théorème leur sont dus.

2. LE CAS n IMPAIR: DESCRIPTION DE LA MÉTHODE

Lorsque n est impair, la démonstration du théorème ci-dessus se fait en trois étapes:

0021-8693/90 $3.00

(1) Soit $P \in \mathbf{Q}[X]$ un polynôme "suffisamment général" (dans un sens précisé dans la Section 4) de degré n. Il existe deux polynômes Q et R de degré $n-1$, premiers à P, tels que $PQ' - P'Q = R^2$.

(2) Soit F_T le polynôme de $\mathbf{Q}(T)[X]$ défini par $F_T(X) = P(X) - TQ(X)$. Si l'on note $\Delta(f)$ le discriminant d'un polynôme f, on a $\Delta(F_T) = \Delta(P)\, S(T)^2$, où S est un polynôme de $\mathbf{Q}[T]$ séparable de degré $n-1$, de racines $t_1, ..., t_{n-1}$. Pour $1 \leqslant i \leqslant n-1$, le polynôme F_{t_i} a une racine triple x_i, et $n-3$ racines simples. Les x_i sont les racines du polynôme R.

(3) Soient K l'extension de $\mathbf{Q}(T)$ obtenue par adjonction des racines de F_T, et G le groupe de Galois de $K/\mathbf{Q}(T)$. D'après (2), le groupe d'inertie en chaque t_i est cyclique, engendré par un 3-cycle. Ceci implique d'une part que $G = A_n$ (resp. S_n) si $\Delta(P)$ est un carré dans $\mathbf{Q}$ (resp. n'en est pas un), et d'autre part que la forme $Tr(x^2)$ associée à $\mathbf{Q}(T)[X]/(F_T)$ est indépendante de T. En choisissant un polynôme P suffisamment général dont les racines sont dans $\mathbf{Q}$, on en déduit le théorème.

Les sections 3 et 4 sont consacrées à la démonstration de (1) et (2).

En fait, pour P de degré impair donné, l'ensemble des solutions de l'équation $PQ' - P'Q = R^2$ se décompose en:

(i) d'une part des solutions de nature triviale, obtenues comme suit: soient P_1 un diviseur de P de degré k, $0 < k < n$, et Q_1 et R_1 des polynômes de degré $\leqslant k-1$ vérifiant $P_1 Q_1' - P_1' Q_1 = R_1^2$. Les polynômes $Q = Q_1 U$ et $R = R_1 U$, avec $U = P/P_1$, vérifient l'égalité $PQ' - P'Q = R^2$. Par construction, les polynômes P, Q, R ne sont pas premiers entre eux.

(ii) d'autre part des solutions obtenues par résolution d'équations linéaires: soit ϕ l'application linéaire qui à un polynôme f de $\mathbf{Q}[X]$ de degré $\leqslant n-1$ associe l'image de $P''f - 2P'f'$ dans $\mathbf{Q}[X]/(P)$. Si $R \in \operatorname{Ker} \phi$, $R \neq 0$, il existe un polynôme Q de degré $\leqslant n-1$ et un seul tel que $PQ' - P'Q = R^2$.

Les polynômes Q et R ainsi obtenus sont "en général" premiers entre eux deux à deux, et donc premiers à P; plus précisément, il existe un polynôme $H \in \mathbf{Z}[A_1, ..., A_n]$ tel que, si $P(X) = X^n + a_1 X^{n-1} + \cdots$ et si $H(a_1, ..., a_n) \neq 0$, $\operatorname{Ker} \phi$ est de dimension 1, et, si R est une base de $\operatorname{Ker} \phi$, R est premier à P.

3. Le cas n impair: le polynôme générique

Dans cette section, n est un entier impair $\geqslant 3$. On note A l'anneau $\mathbf{Z}[A_1, ..., A_n]$, où $A_1, ..., A_n$ sont n indéterminées, K le corps des fractions de A, et $\bar{K}$ une clôture algébrique de K. On rappelle que des éléments d'un anneau factoriel R sont dits "étrangers" si leurs seuls diviseurs communs sont les unités de R, et qu'un polynôme $f \in R[X]$ est dit *primitif* si ses coefficients sont étrangers dans R.

On note P le polynôme "générique" $X^n + A_1 X^{n-1} + \cdots + A_n$.

PROPOSITION 1. (a) *Il existe un unique polynôme primitif $Q \in A[X]$ de degré $\leqslant n-1$ tel qu'il existe un polynôme $R \in A[X]$ vérifiant la relation*

$$PQ' - P'Q = R^2.$$

Les polynômes Q et R sont de degré $n-1$, et sont étrangers dans $A[X]$. Le polynôme R est défini au signe près, il est primitif, et ses racines $r_1, ..., r_{n-1} \in \bar{K}$ sont distinctes.

(b) *Soit de plus $F_T(X) \in A[T][X]$ le polynôme défini par $F_T(X) = P(X) - TQ(X)$, où T est une nouvelle indéterminée. Le discriminant de $F_T(X)$ est égal à $\Delta(P)\, S(T)^2$, où $S(T)$ est un élément de $A[T]$ de degré $n-1$, dont les racines sont simples. Pour $1 \leqslant i \leqslant n-1$, posons $T_i = P(r_i)/Q(r_i)$. Les T_i sont deux à deux distincts, et sont les racines de S. Le polynôme $F_{T_i}(X)$ admet r_i comme racine triple, et ses autres racines sont simples.*

(a) Montrons l'existence de 2 polynômes non nuls Q et R de $A[X]$ de degré $\leqslant n-1$, tels que $PQ' - P'Q = R^2$. Comme le degré de R est inférieur à celui de P, les polynômes P et R sont étrangers dans $K[X]$.

Si $P = \prod (X - X_i)$, où les X_i sont des éléments de $\bar{K}$, on écrit $Q/P = \sum \alpha_i/(X - X_i)$, $R/P = \sum \beta_i/(X - X_i)$. Si l'on pose, pour tout i, $u_{ii} = 0$ et, pour $i \neq j$, $u_{ij} = (X_i - X_j)^{-1}$, l'égalité $(Q/P)' = (R/P)^2$ est équivalente aux équations

$$-\alpha_i = \beta_i^2 \qquad \text{et} \qquad \beta_i \left(\sum_{j=1}^{n} u_{ij} \beta_j \right) = 0,$$

avec $1 \leqslant i \leqslant n$. L'égalité $\beta_i = 0$ implique que $R(X_i) = 0$, donc que R n'est pas premier à P.

On est donc ramené à résoudre le système d'équations linéaires $\sum_{j=1}^{n} u_{ij} \beta_j = 0$, pour $1 \leqslant i \leqslant n$. La matrice $U = (u_{ij})$ est antisymétrique, donc pour n impair a un rang $< n$. D'où l'existence de deux éléments non nuls R et Q de $\bar{K}[X]$, de degré $< n$, tels que $PQ' - P'Q = R^2$. (Cette méthode m'a été indiquée par G. Henniart.)

Pour montrer que la matrice U est de rang $n-1$, il suffit de le faire dans un cas particulier. C'est l'objet de l'appendice 1, où l'on traite le cas du polynôme $P(X) = X^n - X$.

On a donc trouvé un polynôme non nul $R \in \bar{K}[X]$ de degré $\leqslant n-1$, unique à un facteur multiplicatif de $\bar{K}$ près, tel qu'il existe $Q \in \bar{K}[X]$, de degré $\leqslant n-1$, avec $PQ' - P'Q = R^2$.

D'après le théorème 90 de Hilbert, on peut en fait choisir R à coefficients dans K. Le polynôme Q de degré $\leqslant n-1$ est déterminé de manière unique par l'équation $PQ'-P'Q=R^2$, et est donc lui aussi à coefficients dans K. En multipliant les deux membres de cette équation par un élément convenable de A, on peut supposer que Q (et donc R) est un élément de $A[X]$. Soit $\alpha \in A$ (resp. β) un *pgcd* (défini au signe près) des coefficients de Q (resp. R); il est clair que α divise β^2. En remplaçant Q par Q/α et R par R/β, on est ramené à équation du type $PQ'-P'Q=\gamma R^2$, où Q et R sont des éléments primitifs de $A[X]$ de degré $\leqslant n-1$, et où $\gamma \in A$. Supposons qu'il existe $u \in A$ irréductible divisant γ. Alors, comme $PQ' \equiv P'Q \bmod u$ et que le degré de Q est strictement inférieur à celui de P, on a $\Delta(P) \equiv 0 \bmod u$, et comme $\Delta(P)$ est irréductible, $u = \pm\Delta(P)$. Le corps des fractions de $A/(u)$ est de caractéristique 0, et l'égalité $PQ' \equiv P'Q \bmod u$ implique que Q est proportionnel à P, ce qui est impossible. Donc $\gamma = \pm 1$. En remplaçant éventuellement Q par $-Q$, on a donc trouvé Q et R dans $A[X]$, primitifs, de degré $n-1$, tels que $PQ'-P'Q=R^2$. Le polynôme Q est unique, et R est défini au signe près.

Pour montrer que Q et R sont de degré exactement $n-1$, que les racines de R sont simples et que R et Q sont étrangers, il suffit de le montrer pour un polynôme P particulier, pour lequel les polynômes Q et R sont uniques à une constante multiplicative près. Ici encore, le choix de $P(X)=X^n-X$ convient (cf. App. 1). Ceci démontre la partie (a) de la proposition.

(b) Si $F_T = P - TQ$, le discriminant $\Delta(F_T)$ est un élément de $A[T]$ de degré au plus $2(n-1)$, comme on le voit en l'écrivant comme un déterminant de Sylvester.

Soit $t \in \bar{K}$ une racine de $\Delta(F_T(X))$; ceci signifie que F_t a une racine multiple, i.e., que $F_t = P - tQ$ et $F'_t = P' - tQ'$ ont une racine commune. Cette racine doit donc annuler R. Réciproquement, soit r une racine de R; posons $T_r = P(r)/Q(r)$. Le polynôme F_{T_r} admet alors r comme racine triple, car r est racine simple de R. Chaque T_r est racine d'ordre au moins 2 de $\Delta(F_T)$. Comme les T_r sont distincts deux à deux (d'après l'App. 1), et que le degré de $\Delta(F_T)$ est $2(n-1)$, ils sont en fait racines doubles de $\Delta(F_T)$, et l'on a $\Delta(F_T) = \lambda(\prod (T - T_i))^2$, avec $T_i = P(r_i)/Q(r_i)$ et $\lambda \in \bar{K}$. Comme $\Delta(F_0) = \Delta(P)$, on peut écrire $\Delta(F_T)$ sous la forme $\Delta(P)\, S(T)^2$, avec $S \in A[T]$ de degré $n-1$ et de racines simples dans $\bar{K}$.

Par suite, pour chaque racine r de R, $F_{T_r}(X) = (X-r)^3\, g_r(X)$, où g_r est séparable et n'admet pas r comme racine. Ceci achève la démonstration de la prop. 1.

Le polynôme H

Dans la suite de cet article, on note H l'élément non nul de A produit du coefficient dominant de S et de $\Delta(S)\,\mathrm{res}(P, R)$, où $\mathrm{res}(P, R)$ désigne le résultant de P et de R.

Une variante

Pour démontrer l'existence de Q et R dans $A[X]$, on peut également procéder comme suit: en dérivant l'expression $PQ' - P'Q = R^2$, on obtient l'égalité $PQ'' - P''Q = 2RR'$ d'où, en éliminant Q, l'égalité

$$P(P''Q' - P'Q'') = R(RP'' - 2P'R').$$

Comme on cherche un polynôme R non nul de degré $\leqslant n-1$, R est premier à P et $P''R - 2P'R'$ doit être divisible par P. Réciproquement, supposons qu'il existe R non nul de degré $\leqslant n-1$, tel que $P''R - 2P'R' \equiv 0 \bmod P$. Soient Q de degré $\leqslant n-1$ et L de degré $\leqslant n-2$ tels que $PL - P'Q = R^2$. En dérivant et en éliminant Q, on voit que P divise $P'^2(L-Q)$, d'où $L = Q$. Par suite, l'existence de R non nul de degré $\leqslant n-1$ vérifiant $P''R - 2P'R' \equiv 0 \bmod P$ équivaut à l'existence de Q et R de degré $\leqslant n-1$ tels que $PQ' - P'Q = R^2$.

Notons E_{n-1} le sous-espace de $K[X]$ formé des polynômes de degré $<n$, et considérons l'application linéaire $\phi: E_{n-1} \to K[X]/(P)$ qui à $U \in E_{n-1}$ associe $P''U - 2P'U' \bmod P$.

Pour prouver que ϕ n'est pas injective, on peut utiliser la méthode suivante, que m'a indiquée J. Oesterlé: soit l la forme linéaire sur $K[X]/(P)$ donnée par $l(U \bmod P) = \sum_{i=1}^{n} U(X_i)/P'^3(X_i)$. Si $B(U, V)$ est la forme bilinéaire non dégénérée sur $K[X]/(P)$ définie par $(U, V) \mapsto l(UV \bmod P)$, et si ι est l'isomorphisme canonique de E_{n-1} sur $K[X]/(P)$, Oesterlé prouve que $\phi \circ \iota^{-1}$ est B-antisymétrique. Comme $K[X]/(P)$ est de dimension impaire, $\phi \circ \iota^{-1}$ n'est pas injective, et ϕ non plus.

Calcul explicite du polynôme R

Soit $P(X) = \prod_{i=1}^{n} (X - X_i)$. Si M est une partie de $\{X_1, ..., X_n\}$, on pose $P_M = \prod_{x \in M} (X - x)$.

Pour tout entier j, $1 \leqslant j \leqslant n$, notons I_j l'ensemble des racines de P distinctes de X_j.

On peut montrer (cf. section 2) qu'il existe R comme dans la prop. 1 tel que

$$\frac{R}{P} = \sum_{j=1}^{n} u_j \frac{P'(X_j)}{(X - X_j)}, \tag{1}$$

où $u_j = \sum_J \Delta(P_J)\, \Delta(P/P_J/(X - X_j))$, J décrivant les parties à $(n-1)/2$ éléments de I_j.

Le cas $n = 3$

Soit $P(X) = X^3 + A_1 X^2 + A_2 X + A_3$.

Les polynômes R, Q et S de la prop. 1 sont donnés par les formules suivantes:

$$R=(A_1^2-3A_2)X^2+(A_1A_2-9A_3)X+A_2^2-3A_1A_3$$

$$Q=-(A_1^2-3A_2)^2X^2+(-A_1^3A_2+3A_1A_2^2+9A_1^2A_3-27A_2A_3)X$$
$$-A_2^3-A_1^3A_3+9A_1A_2A_3-27A_3^2$$

$$S=(A_1^2-3A_2)^3T^2+(2A_1^3-9A_1A_2+27A_3)T+1.$$

De plus, $\Delta(R)=-3\Delta(P)$, $\Delta(Q)=(A_1^2-3A_2)^2\Delta(P)$, $\Delta(S)=-27\Delta(P)$, $\mathrm{res}(P,R)=\Delta(P)^2$, $\mathrm{res}(Q,R)=(A_1^2-3A_2)^2\Delta(P)^2$, et $\mathrm{res}(P,Q)=\Delta(P)^3$.

4. Le cas n impair: démonstration du théorème

Soient k un corps de caractéristique nulle et $\bar{k}$ une clôture algébrique de k.

Dans ce qui suit, on dit qu'un polynôme $P\in k[X]$ de degré n est *H-général* s'il est unitaire et si ses coefficients $a_1, ..., a_n$ sont tels que $H(a_1, ..., a_n)\neq 0$.

Si P est H-général, on note encore R et Q (resp. S) les éléments de $k[X]$ (resp. $k[T]$) obtenus par spécialisation à partir des polynômes R et Q (resp. S) de la prop. 1. On note également F_T l'élément de $k(T)[X]$ égal à $P(X)-TQ(X)$.

D'après la section précédente, F_T est irréductible. Son discriminant s'annule en $n-1$ éléments $t_i\in\bar{k}$ distincts. En chacun d'eux, le polynôme F_{t_i} admet une racine triple et ses $n-3$ autres racines sont simples.

Proposition 2. *Soient $P\in k[X]$ un polynôme H-général de degré n, et $F_T(X)=P(X)-TQ(X)$ le polynôme de $k(T)[X]$ associé. Le groupe de Galois de la clôture galoisienne de $k(T)[X]/(F_T(X))$ sur $k(T)$ est égal à A_n si $\Delta(P)$ est un carré dans k, et à S_n sinon.*

Soit G le groupe de Galois de la clôture galoisienne de $\bar{k}(T)[X]/(F_T(X))$ sur $\bar{k}(T)$. D'après la prop. 1(b), $\Delta(F_T)$ est un carré de $\bar{k}[T]$, et on a $G\subset A_n$. De plus, comme F_T est irréductible sur $\bar{k}(T)$, G est transitif.

Par ailleurs, l'extension de $k(T)$ associée à F_T est ramifiée en les spécialisations t_i des T_i, $1\leqslant i\leqslant n-1$, définis dans la prop. 1, et est non ramifiée ailleurs (y compris à l'infini). Le groupe d'inertie en t_i est engendré par un 3-cycle; le groupe G est donc engendré par des 3-cycles. La proposition découle alors du lemme suivant (dû pour l'essentiel à Jordan):

Lemme 1. *Tout sous-groupe transitif de A_n engendré par des 3-cycles est égal à A_n.*

Comme Jordan [2, p. 171, th. 4.5] ou [3, App. C] a démontré que tout sous-groupe primitif de S_n contenant un cycle d'ordre 3 est égal à A_n ou à S_n, il suffit de prouver:

LEMME 2. *Tout sous-groupe transitif de S_n engendré par des cycles d'ordre premier est primitif.*

En effet, soit Σ un sous-groupe transitif de S_n engendré par des cycles d'ordre premier. Supposons que Σ ne soit pas primitif. Cela signifie qu'il existe une partition $Y_1, ..., Y_k$ de $\{1, 2, ..., n\}$ $(k > 1)$, stable par Σ, avec $1 < |Y_1| = \cdots = |Y_k| < n$. Si $\sigma \in \Sigma$ est un cycle qui ne laisse pas stable Y_1, son support est formé de l'union de plusieurs Y_i, son ordre est un multiple strict de Y_1, et n'est donc pas premier. Par suite, Y_1 est stable par tout cycle de Σ d'ordre premier, et donc par tout élément de Σ, ce qui contredit le fait que H est transitif.

PROPOSITION 3. *Soit P comme dans la prop. 2, et soit $B = k(T)[X]/(F_T(X))$. La forme quadratique $\mathrm{Tr}_{B/k(T)}(x^2)$ est indépendante de T.*

On peut déduire cette proposition d'un théorème général de Serre (cf. App. 2), en utilisant le fait que l'inertie en chaque point de ramification t_i est d'ordre impair.

Dans le cas ci-dessus, J. Oesterlé en a donné une démonstration directe, que l'on trouvera dans l'App. 3.

Soient à présent $x_1, ..., x_n$ des nombres rationnels distincts, choisis tels que le polynôme $P(X) = \prod (X - x_i) = X^n + a_1 X^{n-1} + \cdots$ soit H-général.

Le groupe de Galois de la clôture galoisienne K de $\mathbf{Q}(T)[X]/(F_T)$ est égal à A_n, le discriminant de P étant un carré. La forme quadratique $\mathrm{Tr}(x^2)$ associée est constante, donc isomorphe à la forme quadratique obtenue pour $T = 0$, i.e., la forme unité $X_1^2 + \cdots + X_n^2$, le polynôme P étant scindé sur $\mathbf{Q}$. Son invariant de Witt est donc nul. D'après [6], on en déduit:

THÉORÈME 2. *Pour tout n impair $\geqslant 5$, il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_n$, contenant le corps K défini ci-dessus.*

Remarque 1. On peut trouver de façon effective des $x_i \in \mathbf{Q}$ qui conviennent. Par exemple, soient l un nombre premier $> n$ tel que $l - 1$ soit divisible par $n - 1$, et $a \in \mathbf{Z}$ une racine primitive $(n-1)$-ième de l'unité mod l. Le polynôme $P(X) = X \prod_{i=0}^{n-2} (X - a^i)$ convient: en effet, $P(X) \equiv X^n - X \bmod l$, et P est H-général, puisque, d'après l'App. 1, $H(0, 0, ..., 0, -1, 0) \neq 0 \bmod l$.

Remarque 2. La démonstration ci-dessus utilise la forme $\mathrm{Tr}(x^2)$. En fait, comme me l'ont signalé S. Bloch et J.-P. Serre, on peut donner un argument cohomologique direct utilisant seulement le fait que les groupes d'inertie sont d'ordre impair.

5. Démonstration de la formule 1

D'après la démonstration que nous avons donnée de la prop. 1, la formule 1 découle des deux lemmes suivants:

Lemme 1. *Soient n un entier impair, et a_{ij}, $1 \leqslant i < j \leqslant n$, $n(n-1)/2$ indéterminées. La matrice alternée $M \in M_n(\mathbf{Q}(a_{ij}))$ définie par $m_{ii}=0$, $m_{ij}=a_{ij}$ si $i<j$ et $m_{ij}=-a_{ji}$ sinon est de rang $n-1$. Son noyau admet pour base le vecteur de composantes* $\mathrm{Pf}(M_1)$, $-\mathrm{Pf}(M_2), ..., -\mathrm{Pf}(M_{n-1})$, $\mathrm{Pf}(M_n)$, *où* Pf *est le pfaffien et où M_i est la matrice alternée obtenue à partir de M en enlevant la i-ième ligne et la i-ième colonne.*

On peut en effet aisément prouver que le (i, j)-ième cofacteur de M est égal à

$$(-1)^{i+j}\,\mathrm{Pf}(M_i)\,\mathrm{Pf}(M_j).$$

Le lemme en résulte.

Lemme 2. *Soient n un entier, et $x_1, ..., x_{2n}$ $2n$ indéterminées. Le pfaffien de la matrice alternée A de dimension $2n$ de terme général $a_{ii}=0$ et $a_{ij}=1/(x_i-x_j)$ pour $i \neq j$ est égal à*

$$\frac{\sum_I \Delta(P_I)\,\Delta(P/P_I)}{\prod_{i<j}(x_i-x_j)},$$

où I parcourt les parties à n éléments de $\{1, 2, ..., 2n\}$, $P(X)=\prod_{i=1}^{2n}(X-x_i)$, et $P_I(X)=\prod_{i\in I}(X-x_i)$.

On prouve ce lemme par récurrence, en utilisant par exemple la formule

$$\mathrm{Pf}((a_{ij}))=\sum_i a_{1i}(-1)^{i+j-1}\,\mathrm{Pf}((a_{jk})_{j,k\neq 1,i}).$$

6. L'exemple de $\tilde{A}_7$

Soit $P(X)=X(X^2-1)(X^2-4)(X^2-9)$. On vérifie que le noyau de l'endomorphisme de E_6 que à R associe $P''R-2P'R' \bmod P$ est de dimension 1. Une base de ce noyau est donnée par le polynôme $R(X)=37261X^6-255206X^4+621565X^2+360732$. Le polynôme $Q(X)=-(1388382121X^6-12818603742X^4+27216417753X^2-3614654884)$ est l'unique polynôme de degré $\leqslant 6$ vérifiant $Q'P-QP'=R^2$. On vérifie que R est premier à P, est séparable, et que les t_i correspondants sont distincts.

Par suite, le groupe de Galois du corps L des racines de $P(X)-TQ(X)$

sur $\mathbf{Q}(T)$ est égal à A_7, et il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ contenant L de groupe de Galois $\tilde{A}_7$.

7. Le cas n pair

Théorème 3. *Pour tout n pair $\geqslant 4$, il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_n$.*

Comme l'a remarqué J.-P. Serre, ce théorème se déduit du cas impair. En effet, puisque $n+1$ est impair, on peut construire d'après la section 4 un polynôme $F_T(X) = P(X) - TQ(X)$, P et Q dans $\mathbf{Q}[X]$ de degré respectivement $n+1$ et n, tel que le groupe de Galois du corps des racines L de $F_T(X)$ est A_{n+1}, et se plonge dans une extension $\tilde{L}/\mathbf{Q}(T)$ de groupe de Galois $\tilde{A}_{n+1}$. Si M est le corps $\mathbf{Q}(T)[X]/(F_T(X))$, le groupe de Galois de L/M (resp. $\tilde{L}/M$) est A_n (resp. $\tilde{A}_n$.) Comme M est une extension transcendante pure de $\mathbf{Q}(T)$, le théorème est prouvé.

Afin d'obtenir des exemples explicites de telles extensions, donnons une réinterprétation concrète de cet argument: si P et Q sont comme ci-dessus, posons

$$g(s, X) = \frac{P(s)\,Q(X) - P(X)\,Q(s)}{X - s},$$

où s est une nouvelle indéterminée. Sur $\mathbf{Q}(s)$, le groupe de Galois de $g(s, X)$ est A_n, et se plonge dans une extension de $\mathbf{Q}(s)$ de groupe de Galois $\tilde{A}_n$.

Appendice 1: Les polynômes $X^n - X$

Soit k un corps, et n un entier impair. On suppose $\mathrm{Car}(k) = 0$ ou $\mathrm{Car}(k) > n$.

Proposition 4. *Soit $P(X) = X^n - X$. Les polynômes $Q(X) = n^2X^{n-1} - (n-2)^2$ et $R(X) = nX^{n-1} + n - 2$ de $k[X]$ sont tels que $P'Q - PQ' = R^2$. A une constante multiplicative près, Q et R sont les seuls polynômes de degré $\leqslant n-1$ et premiers à P qui vérifient cette relation. Les polynômes Q et R sont premiers entre eux. De plus, $\Delta(P - TQ) = \Delta(P)(1 + n^n(n-2)^{n-2}\,T^{n-1})^2$.*

Un calcul facile montre que P, Q, R vérifient l'identité demandée, ainsi que la formule donnée pour $S(t)$.

Prouvons l'unicité du polynôme R (à une constante multiplicative près).

En reprenant la démonstration de la section 1, il suffit de démontrer que la matrice A de dimension $n-1$ et de terme général $a_{ii} = 0$ et, pour $i \neq j$,

$a_{ij}=(z^i-z^j)^{-1}$ est inversible (avec z racine primitive $n-1$-ième de l'unité). Plus précisément, prouvons que le polynôme caractéristique de A est égal à $X^{n-1}+(3.5\cdots(n-2))^2/2^{n-1}$.

Posons $a_1=0$, $a_2=1/(1-z)$, $a_3=1/(1-z^2)$, ..., $a_{n-1}=1/(1-z^{n-2})$. La matrice A est formée des vecteurs $(a_1, a_2, ..., a_{n-1})$, $z(a_{n-1}, a_1, a_2, ..., a_{n-2})$, $z^2(a_{n-2}, a_{n-1}, a_1, a_2, ...)$, ... Il est alors facile de voir que A^{n-1} est une homothétie.

Reste le calcul du déterminant de A. Il est clair qu'il est égal (à une racine de l'unité près) au déterminant de la matrice circulante

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

donc égal à $\prod_{i=1}^{n-1} \mathrm{Tr}(z^i/(1-z))$, (la trace étant prise par rapport au polynôme $(x^{n-1}-1)/(x-1)$).

Or $\mathrm{Tr}(z^{i+1}/(1-z))-\mathrm{Tr}(z^i/(1-z))=\mathrm{Tr}(-z^i)=1$, pour $i\geqslant 1$. Comme $\mathrm{Tr}(1/(1-z))=-(n-2)/2$, on en déduit que le déterminant de A est égal à $(3.5\cdots(n-2))^2/2^{n-1}$.

Le polynôme R est donc unique (à une constante multiplicative près). De plus, il est sans racine multiple, ainsi que le polynôme $S(T)$.

Appendice 2: Un théorème sur $\mathrm{Tr}(x^2)$

Dans son cours à Harvard (Octobre–Décembre 1988), J.-P. Serre démontre le résultat suivant:

Théorème. *Soient k un corps de caractéristique $\neq 2$, $E/k(T)$ une extension finie séparable de degré n, et $G\subset S_n$ le groupe de Galois de la clôture galoisienne de E. Supposons que pour toute place v de $k(T)$, sauf éventuellement la place à l'infini, le groupe d'inertie de v, défini à conjugaison près dans G, soit d'ordre impair. Alors la forme quadratique $\mathrm{Tr}_{E/k(T)}(x^2)$ est équivalente sur $k(T)$ à une forme à coefficients dans k.*

Soit A le normalisé de $k[T]$ dans E (i.e., l'algèbre affine de la courbe privée de l'image réciproque de l'infini). Si $\mathscr{D}$ est sa différente, le fait que les groupes d'inertie sont d'ordre impair implique que la différente inverse $\mathscr{D}^{-1}$ est le carré d'un idéal $\mathscr{A}$. Le $k[t]$-module libre $\mathscr{A}$ de rang n est auto-adjoint pour la forme $\mathrm{Tr}_{E/k(T)}$, donc le discriminant de cette forme est une unité. Un théorème de Harder (cf. par exemple [5, p. 211, th. 3.3]) permet alors de conclure.

On peut également démontrer ce théorème en utilisant un théorème de Milnor [4, p. 335, th. 5.3]: une forme quadratique sur $k(T)$ provient d'une forme constante si et seulement si ses "seconds résidus" [4, p. 322, lemme 2.1] sont nuls en chaque place de $k(T)$, sauf éventuellement la place à l'infini.

APPENDICE 3: UNE PREUVE DIRECTE DE LA PROPOSITION 3 (PAR J. OESTERLÉ)

Soit k un corps. Considérons trois polynômes P, Q, R dans $k[X]$ satisfaisant aux conditions suivantes:

(a) $P'Q - PQ' = R^2$;

(b) P est unitaire et l'on a $\deg Q < \deg P$;

(c) P est étranger à P' et à Q (donc aussi à R).

Nous noterons n le degré de P.

Soit t une nouvelle indéterminée. Posons

$$A = k[t]$$

$$B = A[X]/(P - tQ)\, A[X].$$

L'anneau B est un A-module libre de rang n, admettant $(1, X, ..., X^{n-1})$ pour base. Notons $M(t)$ la matrice par rapport à cette base de la forme A-bilinéaire $(u, v) \mapsto \mathrm{Tr}_{B/A}(uv)$ sur B. On a $M(t) \in M_n(A)$. Notons $Z \mapsto Z^*$ la transposition dans $M_n(A)$.

THÉORÈME. *Il existe une matrice* $N(t) \in M_n(A)$ *telle que* $M(t) = N(t)^* M(0) N(t)$.

Posons

$$A' = k(t)$$

$$B' = A'[X]/(P - tQ)\, A'[X].$$

Pour tout entier i, $0 \leqslant i \leqslant n-1$, effectuons la division euclidienne de X^iQ par P:

$$X^iQ = C_iP + D_i, \qquad \text{avec} \quad \deg D_i \leqslant n-1.$$

On a $\deg C_i \leqslant i-1$. Par suite, $(X^i - tC_i)_{0 \leqslant i \leqslant n-1}$ est une base de B' sur A'. Les résultants (par rapport à l'indéterminée X) $\mathrm{res}(P - tQ, Q)$ et $\mathrm{res}(P - tQ, R)$ sont des éléments non nuls de $k[t]$: en effet, leur valeur pour $t = 0$ est non nulle par hypothèse. Il en résulte que Q et R sont inversibles dans B'. En posant

$$e_i = \frac{Q}{R}(X^i - tC_i)$$

on obtient une base $(e_0, ..., e_{n-1})$ de B' sur A'. Démontrons que la matrice par rapport à cette base de la forme A'-bilinéaire $(u, v) \mapsto \mathrm{Tr}_{B'/A'}(uv)$ sur B' appartient à $M_n(k)$.

Soient i, j compris entre 0 et $n-1$. On a

$$\begin{aligned}
\mathrm{Tr}_{B'/A'}(e_i e_j) &= \mathrm{Tr}_{B'/A'}\left(\frac{Q^2(X^i - tC_i)(X^j - tC_j)}{R^2}\right) \\
&= \mathrm{Tr}_{B'/A'}\left(\frac{Q^2(X^i - tC_i)(X^j - tC_j)}{(P-tQ)'\,Q - (P-tQ)\,Q'}\right) \\
&= \mathrm{Tr}_{B'/A'}\left(\frac{Q(X^i - tC_i)(X^j - tC_j)}{(P-tQ)'}\right).
\end{aligned}$$

Cette expression est égale au coefficient de X^{n-1} dans le reste de la division euclidienne (relative à la variable X) de $Q(X^i - tC_i)(X^j - tC_j)$ par $P - tQ$. Effectuons la division euclidienne de $X^j D_i$ par P: on a

$$X^j D_i = UP + V, \qquad \text{avec} \quad \deg V \leqslant n-1.$$

On peut alors écrire

$$\begin{aligned}
Q(X^i - tC_i)(X^j - tC_j) &= (P-tQ)\,C_i(X^j - tC_j) + D_i(X^j - tC_j) \\
&= (P-tQ)[C_i(X^j - tC_j) + U] + V + t(QU - D_i C_j).
\end{aligned}$$

Le polynôme $QU - D_i C_j$ est de degré $\leqslant n-2$ car

$$P(QU - D_i C_j) = Q(X^j D_i - V) - PD_i C_j = D_i D_j - QV$$

est de degré $\leqslant 2(n-1)$. Il en résulte que le reste de la division euclidienne de $Q(X^i - tC_i)(X^j - tC_j)$ par $P - tQ$ est $V + t(QU - D_i C_j)$ et que son coefficient de degré $n-1$ est égal à celui de V, donc appartient à k.

Nous avons ainsi démontré que, si G désigne la matrice de passage de $(e_0, ..., e_{n-1})$ à $(1, X, ..., X^{n-1})$, on a $M = G^* \theta G$, avec $\theta \in M_n(k)$. Pour terminer la démonstration du théorème, il nous suffit de démontrer que G appartient à $M_n(A)$ (et pas seulement à $M_n(A')$) et que $G(0)$ est inversible dans $M_n(k)$. La matrice $N = GG(0)^{-1}$ satisfera alors à la conclusion du théorème.

En fait, on a $G^{-1} = H_1 H_2$, où H_1 est la matrice par rapport à la base $(1, X, ..., X^{n-1})$ de la multiplication par Q/R dans B' et H_2 la matrice de passage de la base (X^i) à la base $(X^i - tC_i)$. La matrice H_2 et son inverse sont triangulaires supérieures, à coefficients dans A. Soient U, V des éléments de $k[X]$ tels que $UP + VQ = 1$. On a $U(P - tQ) + (V + tU)\,Q = 1$, d'où $R/Q = R(V + tU)$ dans B'. Cela démontre que la matrice H_1^{-1} appartient à $M_n(A)$. Sa valeur pour $t=0$ est une matrice inversible de $M_n(k)$, car Q et R sont étrangers à P par hypothèse. Cela achève la démonstration.

Remarque. Si on remplace l'hypothèse (a) par $P'Q-PQ'=R^2S$, où S est un polynôme de degré s, le théorème peut être remplacé par

Il existe des matrices $N(t)\in M_n(A)$ et $H(t)\in M_n(A)$ telles que $M(t)=N(t)^*\,H(t)\,N(t)$ et que chaque coefficient de $H(t)$ soit de degré $\leqslant s$ en t.

Définissons encore une base (e_i) de B' sur A' par la même formule que ci-dessus. Alors $\mathrm{Tr}_{B'/A'}(e_ie_j)$ est le coefficient de X^{n-1} dans le reste de la division euclidienne de $Q(X^i-tC_i)(X^j-tC_j)\,S$ par $P-tQ$. Le reste en question, avec les notations de la démonstration, est celui de la division euclidienne de $(V+t(QU-D_iC_j))\,S$ par $P-tQ$. Comme on a $\deg V\leqslant n-1$ et $\deg(QU-D_iC_j)\leqslant n-2$, le coefficient de X^{n-1} dans ce reste est de degré $\leqslant s$ en t.

Bibliographie

1. W. Feit, $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields, *J. Algebra* **104** (1986), 231–260.
2. B. Huppert, "Endliche Gruppen," Vol. I, Springer-Verlag, New York, 1967.
3. C. Jordan, "Traité des substitutions et des équations algébriques," Gauthier–Villars, Paris, 1870.
4. J. Milnor, Algebraic K-theory and quadratic forms, *Invent. Math.* **9** (1970), 318–344.
5. W. Scharlau, "Quadratic and Hermitian Forms," Springer-Verlag, New York, 1985.
6. J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment Math. Helv.* **59** (1984), 651–676 (= *Oeuvres*, **III**, 131).
7. N. Vila, On central extensions of A_n as Galois groups over **Q**, *Arch. Math.* **44** (1985), 424–437.