BULLETIN DE LA S. M. F.

POTRON

Sur l'irréductibilité des polynômes à plusieurs variables

Bulletin de la S. M. F., tome 63 (1935), p. 226-230

<http://www.numdam.org/item?id=BSMF_1935__63__226_0>

© Bulletin de la S. M. F., 1935, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (http://smf.emath.fr/Publications/Bulletin/Presentation.html) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SUR L'IRRÉDUCTIBILITÉ DES POLYNOMES A PLUSIEURS VARIABLES;

PAR M. l'Abbé POTRON.

M. Hilbert a démontré le théorème suivant, que je désignerai par H(n, k) : *Si un polynome* F(x_1, ..., x_k), *à coefficients entiers, est irréductible dans le champ rationnel, il est possible, d'une infinité de manières, de donner à* x_1, ... x_n ($n < k$) *des valeurs entières* l_1, ..., l_n *telles que le polynome* F(l_1, ..., l_n, x_{n+1}, ..., x_k) *reste irréductible dans le champ rationnel* (1). Dans une Note, qu'a publiée ce *Bulletin* (2), j'ai indiqué que, une fois H(1, k) démontré, quel que soit k, il suffit, pour obtenir H(n, k), d'appliquer successivement H(1, $k-1$), ..., H(1, $k-n+1$). J'ai indiqué aussi que H(1, k) peut se déduire de H(1, 2) en représentant, au moyen du procédé de Kronecker (3) le polynome F(x_1, x_2, ..., x_k) par un polynome $f(y, x_1)$ ayant les mêmes coefficients et devant se décomposer en même temps. Mais la démonstration ne s'applique plus si le polynome $f(y, x_1)$ est réductible dans le champ C(x_1) des fonctions rationnelles de x_1 à coefficients entiers.

La démonstration qui fait l'objet de la présente Note s'applique dans tous les cas. Elle donne en même temps le résultat suivant : *Une fois* H(1, 2) *établi pour tout polynome normal* (4) *par rapport à l'une de ses deux variables*, H(1, k) *s'en déduit, quel que soit* k, *pour un polynome quelconque.*

1. Soit F(x_1, x_2, ... x_k) un polynome à coefficients entiers,

---

(1) *Crelle*, t. 110, 1892, p. 104-139.

(2) *B. S. M.*, t. LX, 1932, p. 127.

(3) *Crelle*, t. 92, 1882, p. 19-13.

(4) F(x, y), à coefficients entiers, est dit *normal par rapport à* y si, y_1, ..., y_n étant les racines de l'équation F(x, y) = 0 en y, on a, pour chacune d'elles une expression de la forme $y_i = r_i(x, y_1)$, r_i étant une fonction rationnelle à coefficients entiers.

irréductible dans le champ rationnel. On peut le considérer comme un polynome de degré m en $x_2, \ldots, x_k$, ayant pour coefficients des polynomes en x_1 à coefficients entiers. Opérant au besoin sur $x_2, \ldots, x_k$ une substitution linéaire à coefficients entiers, on peut supposer que ce polynome contient un terme $\mathrm{X}x_2^m$, X étant un polynome en x_1. Il est entendu, une fois pour toutes, que x_1 ne prendra jamais aucune des valeurs, en nombre fini, annulant X. Remplaçant alors x_2 par $\mathrm{X}^{-1}x_2'$, puis $x_3, \ldots, x_k$ par $x_3', \ldots, x_k'$, et posant $\mathrm{X}^{m-1}\mathrm{F}(x_1, x_2, \ldots, x_k) = \mathrm{F}'(x_1, x_2', \ldots, x_k')$, on obtient un polynome en $x_2', \ldots, x_k'$, contenant le terme $x_2'^m$, et dont les autres coefficients sont des polynomes en x_1 à coefficients entiers. Il suffit évidemmment (1) de démontrer $\mathrm{H}(1, k)$ pour le polynome F'. Je supprimerai désormais les accents.

2. Remplaçant, avec Kronecker, x_i par $y^{(l+1)^{i-1}}$ $(i = 2, \ldots, k)$, l désignant un entier $> m$, on obtient

$$\mathrm{F}(x_1, x_2, \ldots, x_k) = y^n + \ldots, \qquad n = ml^{k-1}.$$

Supposons, ce qui ne peut arriver que pour certaines valeurs de x_1, qu'il existe deux polynomes $\mathrm{P}(x_2, \ldots, x_k, \| x_1)$ (2) $= x_2^{\mathrm{A}} + \ldots$ et $\mathrm{Q}(x_2, \ldots, x_k, \| x_1) = x_2^{\mathrm{B}} + \ldots$ $(\mathrm{A} + \mathrm{B} = m)$ vérifiant l'identité $\mathrm{PQ} - \mathrm{F} = 0$. Par la transformation de Kronecker, il leur correspond deux polynomes $p(y, \| x_1) = y^a + \ldots$ et $q(y, \| x_1) = y^b + \ldots$ vérifiant l'identité $pq - f = 0$. Il faut remarquer qu'à tout polynome $p(y)$ de degré $< n$, la transformation de Kronecker fait correspondre un polynome complètement déterminé $\mathrm{P}(x_2, \ldots, x_k)$, de degré $\leq m$ (3); mais il est possible que, p et q vérifiant l'identité $pq - f = 0$ en y, les polynomes correspondants ne vérifient pas l'identité $\mathrm{PQ} - \mathrm{F} = 0$ en $x_2, \ldots, x_k$.

3. Soient $y_1, \ldots, y_h$ les racines distinctes de l'équa-

---

(1) *Cf.* de Séguier, *Groupes de Substitutions*, n° 128.

(2) Cette notation désigne un polynome par rapport aux variables qui précèdent le signe ||, les coefficients étant des fonctions *quelconques* de la variable qui suit ce signe.

(3) *Cf.* Konig, *Theorie der algebraischen Grossen*, p. 37.

tion $f(y, x_1) = 0$: ce sont des fonctions algébriques de x_1, racines d'une équation de même espèce $g(y, x_1) = 0$. Le discriminant de cette équation est un polynome en x_1, en général $\not\equiv 0$, qui ne peut donc s'annuler que pour certaines valeurs de x_1, en nombre fini, formant un ensemble (α). Soit $p(y, x_1) = y^a + \dots$ un polynome en y divisant $f(y, x_1)$ quel que soit x_1. C'est le produit de a facteurs linéaires $y - y_i$, distincts ou non. Soient l, hors de (α), une valeur particulière de x_1, et b_i ce que devient y_i pour $x_1 = l$. Le polynome $g(y, l)$ a exactement les h facteurs linéaires distincts $y - b_i$, correspondant aux h facteurs linéaires $y - y_i$. Il y a donc, pour l entier hors de (α), correspondance biunivoque entre les diviseurs de $f(y, l)$ et ceux de $f(y, x_1)$. Donc, *si l est hors de (α), à tout diviseur de* $F(l, x_2, \dots, x_k)$ *correspond le polynome obtenu en faisant $x_1 = l$ dans un diviseur de $f(y, x_1)$.*

Pour chaque degré a, le nombre de ces diviseurs est fini. Comme a est $\leq n - 1$, leur nombre total est fini. Ils forment deux catégories suivant que, par leurs coefficients, ils appartiennent ou non au champ $C(x_1)$. Deux diviseurs complémentaires étant toujours de la même catégorie, il suffit de considérer les diviseurs de degré $a \leq n/2$.

4. Soit $p(y, x_1) = y^a + \dots$ un diviseur de première catégorie, et $q(y, x_1) = y^b + \dots$ $(a + b = n)$ le diviseur complémentaire. D'après un théorème de Gauss (1), les coefficients non écrits sont des polynomes $p_i(x_1)$, $q_j(x_1)$ $(i = 1, \dots, a; j = 1, \dots, b)$ à coefficients entiers. Soient $P(x_1, x_2, \dots, x_k)$ et $Q(x_1, x_2, \dots, x_k)$ les polynomes correspondants (n° 2). Si on les ordonne en $x_2, \dots, x_k$, leurs coefficients sont les $p_i(x_1)$ et $q_j(x_1)$. L'identité $PQ - F = 0$ (en $x_2, \dots, x_k$) entraîne entre ces coefficients un certain nombre de relations de la forme $K(x_1) = 0$, K étant un polynome. Les $K(x_1)$ ne peuvent se réduire tous à 0, car alors l'identité $PQ = F$ aurait lieu en $x_1, x_2, \dots, x_k$, et le polynome F serait réductible dans le champ rationnel. Ainsi, pour chaque diviseur $p(y, x_1)$ de la première catégorie, le polynome correspon-

(1) *Disquis. arithm.*, art. 42. *Voir* par exemple Konig, *op. cit.*, p. 92.

dant $P(x_1, x_2, \ldots, x_k)$ ne peut diviser F que pour un nombre fini de valeurs de x_1 formant un ensemble (6). Je désignerai par ($\mathcal{B}$) la réunion des ensembles (6) relatifs aux diviseurs de première catégorie. Si l est hors de ($\mathcal{B}$), $P(l, x_2, \ldots, x_k)$ ne divise pas $F(l, x_2, \ldots, x_k)$.

5. Soit maintenant $p(y, \| x_1)$ un diviseur de la deuxième catégorie. On va voir que l'*on peut donner à x_1 une infinité de valeurs entières l telles que $p(y, \| l)$ n'appartienne pas au champ rationnel.* Alors, quand même $P(x_2, \ldots, x_k, \| l)$ diviserait $F(l, x_2, \ldots, x_k)$, ce ne serait pas un diviseur à coefficients rationnels.

Soit $R(v, x_1) = 0$ la « résolvante générale » de l'équation $g(y, x_1) = 0$ (1). C'est une équation normale de degré $h!$, avant $h!$ racines distinctes, qui sont les $h!$ valeurs distinctes que prend une fonction rationnelle de $y_1, \ldots, y_h$, convenablement choisie, quand on effectue, sur ces h racines, toutes les permutations possibles. Le discriminant de $R(v, x_1)$ est un polynome en x_1, en général $\not\equiv 0$, qui ne s'annule donc que pour certaines valeurs de x_1, en nombre fini, formant un ensemble (c), lequel contient évidemment l'ensemble (α) du n° 3. Soit $R_1(v, x_1)$ un diviseur de $R(v, x_1)$, irréductible dans $C(x_1)$, ayant pour racines $v_1, \ldots, v_j$. On sait que toute racine y_i a une expression rationnelle $r_i(v_1, x_1)$, et qu'il existe un groupe S, formé des j substitutions s_a sur les y_i qui transforment v_1 en v_a ($a = 1, \ldots, j$), s_a remplaçant y_i par $y_{i_a} = r_i(v_a, x_1)$. Ce groupe S est le groupe pour le champ $C(x_1)$, de l'équation $g(y, x_1) = 0$.

Soient, pour $x_1 = l$ hors de (c), $b_1, \ldots, b_h, c_1, \ldots, c_j$ les valeurs, toutes distinctes, que prennent $y_1, \ldots, y_h, v_1, \ldots, v_j$. On a toujours $b_i = r_i(c_1, l)$; et, à chaque substitution s_a, répond une substitution t_a remplaçant b_i par $b_{i_a} = r_i(c_a, l)$. Ces substitutions t_a forment un groupe T, qui n'est autre que le groupe S écrit avec d'autres symboles.

D'après le théorème H(1, 2) pour tout polynome normal, on

---

(1) Pour la théorie des équations algébriques, *voir*, par exemple, BIANCHI, *Teoria dei Gruppi di Sostituzioni*, ou DICKSON, *Theory and Application of finite Groups*, Part. III.

peut donner à x_1 une infinité de valeurs entières l formant un ensemble $(\mathcal{D})$ telles que $R_1(v, l)$ reste irréductible dans le champ rationnel. Alors, pour tout nombre l de $(\mathcal{D})$ hors de (c), T est le groupe, pour le champ rationnel, de l'équation $g(y, l) = 0$.

6. D'après les propriétés fondamentales de ce groupe :

1° Si son ordre j était égal à 1, toutes les racines y_i, donc tous les diviseurs de $f(y, x_1)$, appartiendraient au champ $C(x_1)$. L'existence d'un diviseur de deuxième catégorie suppose donc que j est > 1.

2° Si l'on opère sur les y_i toutes les substitutions s_a du groupe S, le diviseur considéré se transforme en b (> 1) diviseurs distincts $p_1(y, \| x_1), \ldots, p_b(y, \| x_1)$.

3° Le produit $(z - p_1)\ldots(z - p_b)$ est un polynome en z et y appartenant à $C(x_1)$. Le p. p. c. m. des dénominateurs de ses coefficients est un polynome en x_1, en général $\not\equiv 0$, qui ne s'annule donc que pour certaines valeurs de x_1, en nombre fini, formant un ensemble (e). En multipliant le produit considéré par ce p. p. c. m., on obtient un polynome $G(z, y, x_1)$, de degré b en z, admettant les b racines distinctes $p_1, \ldots, p_b$. Son discriminant est un polynome en y et x_1, en général $\not\equiv 0$, qui ne peut donc se réduire à 0 que pour certaines valeurs de x_1, en nombre fini, formant un ensemble (f). $(\mathcal{E})$ et $(\mathcal{F})$ désigneront la réunion des ensembles (e) et (f) relatifs aux diviseurs n'appartenant pas à $C(x_1)$.

Si l'on donne à x_1 une valeurs l appartenant à $(\mathcal{D})$ et située hors de (c), $(\mathcal{E})$, $(\mathcal{F})$, les transformés de chaque diviseur de la deuxième catégorie par le groupe T restent distincts. Il est donc impossible qu'aucun d'eux appartienne au champ rationnel, car il serait alors invariant par le groupe T.

7. Si donc, de l'ensemble infini $(\mathcal{D})$, on retranche les entiers, en nombre fini, pouvant appartenir à l'un des ensembles $(\mathcal{B})$, (c), $(\mathcal{E})$, $(\mathcal{F})$, il reste une infinité d'entiers l pour lesquels $F(l, x_2, \ldots, x_k)$ ne peut avoir aucun polynome diviseur en $x_2, \ldots, x_k$, à coefficients rationnels.