BULLETIN DE LA S. M. F.

PAUL DUBREIL

Remarques sur le théorème de Noether

Bulletin de la S. M. F., tome 64 (1936), p. 99-118

<http://www.numdam.org/item?id=BSMF_1936__64__99_0>

REMARQUES SUR LE THÉORÈME DE NŒTHER;

PAR M. P. DUBREIL.

1. **Introduction.** — Dans deux Notes récentes, W. van der Woude (1) et B. L. van der Waerden (2) ont de nouveau attiré l'attention sur le théorème de Noether. Ce théorème, relatif à deux courbes algébriques planes $f(x, y) = 0$, $g(x, y) = 0$ où f et g sont deux polynomes de degrés m et n à coefficients quelconques n'admettant pas de facteur commun, donne comme on sait une condition suffisante (d'ailleurs aussi nécessaire, mais à ce point de vue le théorème est trivial) pour qu'un polynome $\varphi(x, y)$ satisfasse à l'identité

$$\varphi(x, y) = A(x, y) f(x, y) + B(x, y) g(x, y). \tag{1}$$

Cette condition fait intervenir le comportement du polynome φ en chacun des points d'intersection $M_1, M_2, \ldots, M_n$ des « courbes de base » $f = 0$, $g = 0$, auxquels sont attachés des nombres $\rho_1, \rho_2, \ldots, \rho_n$ appelés *exposants* ou *multiplicités de Noether*, et s'énonce de la manière suivante :

A. *Pour qu'un polynome φ satisfasse à l'identité* (1), *il faut et il suffit que, pour chacun des points $M_i(x_i, y_i)$, on puisse déterminer des polynomes A_i, B_i tels que la différence $\varphi - A_i f - B_i g$ développée suivant les puissances croissantes de $x - x_i$, $y - y_i$, commence par des termes de degré au moins égal à ρ_i.*

En particularisant, on a la condition suivante, *seulement suffisante*, mais d'un emploi commode :

---

(1) W. VAN DER WOUDE, *Über den Noetherschen Fundamentalsatz* (*Math. Ann.*, t. 111, 1935, p. 425).

(2) B. L. VAN DER WAERDEN, *Zur algebraischen Geometrie : VII. Ein neuer Beweis des Restsatzes* (*Math. Ann.*, t. 111, 1935, p. 432). *Voir aussi*, du même auteur, *Zur Begründung des Restsatzes mit dem Noetherschen Fundamentalsatz* (*Math. Ann.*, t. 104, 1931, p. 472).

B. *Pour que* φ *satisfasse à l'identité* (1), *il suffit que la courbe* $\varphi = 0$ *admette chaque point* M_i *comme point multiple d'ordre au moins égal à* ρ_i. (La condition A est en effet vérifiée en prenant $A_i = B_i = 0$).

Deux cas particuliers sont importants pour les applications géométriques. Le premier (*cas simple*) est celui où les deux courbes de base ne présentent pas de contacts en leurs points d'intersection. L'énoncé B peut alors se mettre sous la forme :

B'. *Pour que* φ *satisfasse à l'identité* (1), *il suffit que la courbe* $\varphi = 0$ *admette chaque point d'intersection* M_i *comme point multiple d'ordre* $r_i + s_i - 1$, r_i *et* s_i *désignant les ordres de multiplicité de* M_i *pour les deux courbes de base. Si l'on a* $r_i = s_i = 1$ (*cas élémentaire*), *il suffit que* $\varphi = 0$ *passe par* M_i, *condition qui, évidemment, est aussi nécessaire.*

Le second cas particulier est celui où *l'une des courbes de base*, $f = 0$ *par exemple, n'admet que des points multiples à tangentes distinctes.* On a alors l'énoncé suivant :

B''. *Pour que* $\varphi(x, y)$ *satisfasse à l'identité* (1), *il suffit que la courbe* $\varphi = 0$, *en chaque point* M_i, *coupe chaque branche* $\mathcal{B}_h^i$ *de* $f = 0$ *avec une multiplicité* (1) *au moins égale à* $r_i - 1 + \mu_h^i$, r_i *désignant l'ordre de multiplicité de* M_i *pour* $f = 0$, *et* μ_h^i *étant la multiplicité avec laquelle la même branche* $\mathcal{B}_h^i$ *est coupée par* $g = 0$.

La méthode de démonstration la plus intéressante au point de vue algébrique remonte à Noether lui-même (2). Elle consiste à utiliser le résultant $\mathcal{R}(x)$ des polynomes f et g, qui satisfait à l'identité

$$\mathcal{R}(x) = \mathcal{U}(x, y) f(x, y) + \mathcal{V}(x, y) g(x, y) \tag{2}$$

---

(1) Nombre de points d'intersection confondus en M_i.

(2) M. Noether, *Math. Ann.*, t. 40, 1892, p. 140. *Voir* aussi E. Picard et G. Simart, *Théorie des fonctions algébriques de deux variables indépendantes*, t. 2, Ch. I, p. 1.

de même forme que (1) ([1]). J'ai signalé dans ma thèse ([2]) qu'il y a intérêt pour la détermination de la multiplicité de Noether ρ, à remplacer le résultant par le polynome en x seul de *degré minimum* satisfaisant à une identité analogue à (2), polynome qui est en général un diviseur du résultant et que j'ai appelé *le sous-résultant* des polynomes f et g. Dans la première des Notes auxquelles je viens de faire allusion, W. van der Woude remarque que, si F est un polynome quelconque, on peut écrire, d'après (2)

$$\mathcal{R}(x)\,\mathrm{F}(x, y) = \mathrm{F}\mathcal{U}f + \mathrm{F}\mathcal{V}g$$

et chercher, pour obtenir l'identité (1), à faire apparaître $\mathrm{R}(x)$ en facteur au second membre sans que celui-ci cesse d'être une combinaison linéaire de f et g; il en déduit une démonstration du théorème de Noether dans le cas simple (énoncé B'). Dans la deuxième Note, B. L. van der Waerden, utilisant la même remarque, établit directement le théorème B''.

Je me suis proposé ici d'indiquer en premier lieu la signification qu'on peut donner à la remarque de W. van der Woude, et le parti qu'on peut en tirer, dans la démonstration du théorème de Noether sous sa forme générale (énoncé A) : cette remarque n'entraîne sans doute pas de modification réelle des principes de la démonstration, mais a l'avantage d'apporter quelques simplifications dans les raisonnements. Je donne d'autre part (théorème IV) un théorème qui me paraît présenter un double intérêt : généralisant une proposition de ma thèse, il joue un rôle fondamental dans la détermination de la multiplicité de Noether, et, ainsi que je l'ai signalé sommairement à M. van der Waerden dans une lettre qui remonte à 1931, l'énoncé B'' en est une conséquence immédiate. Enfin j'ai essayé à cette occasion de grouper et de présenter dans leur ordre logique les différentes propositions dont l'ensemble me paraît constituer actuellement le théorème de Noether.

([1]) On obtient immédiatement cette propriété à partir du déterminant de Sylvester, *voir* par exemple B. L. VAN DER WAERDEN, ***Moderne Algebra***, t. 2, p. 4.

([2]) P. DUBREIL, ***Recherches sur la valeur des exposants des composants primaires des idéaux de polynomes, thèse***, Paris, 1930, Ch. I (***Jour. de Mathématiques pures et appliquées***, 9e série, t. 9, p. 231).

2. La remarque de W. van der Woude et la démonstration du théorème de Noether. — Nous utiliserons seulement quelques-unes des définitions fondamentales de la théorie des idéaux, ainsi qu'une remarque élémentaire concernant les idéaux simples, c'est-à-dire dont la variété se réduit à un point (1). Le théorème fondamental

---

(1) Résumons rapidement ces définitions et cette remarque. Dans l'ensemble $\mathfrak{o}$ des polynomes à deux variables x, y à coefficients complexes, on appelle *idéal* tout sous-ensemble de $\mathfrak{o}$ possédant les deux propriétés suivantes :

1° en même temps que φ et ψ ce sous-ensemble contient $\varphi - \psi$ (donc aussi O, $-\psi$, $\varphi + \psi$); 2° en même temps que φ, le sous-ensemble contient le produit de φ par un polynome quelconque de $\mathfrak{o}$.

Si $f_1, f_2, \ldots, f_h$ sont des polynomes donnés, l'ensemble des polynomes f définis par

$$f = a_1 f_1 + \ldots + a_h f_h,$$

où $a_1, \ldots, a_h$ sont des polynomes arbitraires, est un idéal $\mathfrak{a}$, que l'on désigne par

$$\mathfrak{a} = (f_1, \ldots, f_h).$$

L'ensemble des f_i est la *base* de cet idéal. En particulier, l'ensemble des polynomes φ satisfaisant à l'identité (1) est un idéal $\mathfrak{m} = (f, g)$.

Un idéal $\mathfrak{a}$ est dit *multiple* d'un idéal $\mathfrak{b}$ ($\mathfrak{b}$ *diviseur* de $\mathfrak{a}$, notation : $\mathfrak{a} \subset \mathfrak{b}$) si tout polynome de $\mathfrak{a}$ appartient à $\mathfrak{b}$. Le même signe $\subset$ sera utilisé pour exprimer qu'un élément φ appartient à l'idéal $\mathfrak{a}$: $\varphi \subset \mathfrak{a}$.

On appelle :

Plus grand commun diviseur $(\mathfrak{a}, \mathfrak{b})$ de deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ l'ensemble des polynomes de la forme $\varphi + \psi$ où φ et ψ appartiennent respectivement à $\mathfrak{a}$ et $\mathfrak{b}$; c'est évidemment un idéal. On a $\mathfrak{a} \subset (\mathfrak{a}, \mathfrak{b})$, $\mathfrak{b} \subset (\mathfrak{a}, \mathfrak{b})$. Si

$$\mathfrak{a} = (f_1, \ldots, f_h), \qquad \mathfrak{b} = (g_1, \ldots, g_k),$$

on a

$$(\mathfrak{a}, \mathfrak{b}) = (f_1, \ldots, f_h, g_1, \ldots, g_k);$$

Plus petit commun multiple $[\mathfrak{a}, \mathfrak{b}]$ de deux idéaux $\mathfrak{a}$, $\mathfrak{b}$, l'ensemble des polynomes appartenant à la fois à $\mathfrak{a}$ et à $\mathfrak{b}$. C'est évidemment un idéal.

Produit de deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ l'ensemble $\mathfrak{ab}$ des polynomes $\varphi\psi$ (produits d'un polynome φ de $\mathfrak{a}$ par un polynome ψ de $\mathfrak{b}$) et des sommes $\varphi_1\psi_1 + \ldots + \varphi_\lambda\psi_\lambda$ d'un nombre fini quelconque de tels produits; c'est encore un idéal. Si

$$\mathfrak{a} = (f_1, \ldots, f_h), \qquad \mathfrak{b} = (g_1, \ldots, g_k),$$

on a $\mathfrak{ab} = (\ldots, f_i g_j, \ldots)$. Extension immédiate à un nombre quelconque d'idéaux (commutativité, associativité du produit). Cas particulier : puissance d'un idéal.

Un idéal $\mathfrak{p}$ est dit *premier* si les deux relations $\varphi\psi \subset \mathfrak{p}$, $\varphi \not\subset \mathfrak{p}$ entraînent $\psi \subset \mathfrak{p}$. Exemple : ensemble des polynomes nuls en un point (x_0, y_0) : $\mathfrak{p} = (x - x_0, y - y_0)$.

Un idéal $\mathfrak{q}$ est dit *primaire* si les deux propriétés : $\varphi\psi \subset \mathfrak{q}$ et : aucune puissance de φ n'appartient à $\mathfrak{q}$, entraînent $\psi \subset \mathfrak{q}$. L'ensemble des polynomes dont une puissance appartient à $\mathfrak{q}$ est un idéal premier $\mathfrak{p}$, et on a $\mathfrak{q} \subset \mathfrak{p}$. Si $\varphi\psi \subset \mathfrak{q}$ et

de décomposition d'un idéal en idéaux primaires, dont le théorème de Noether est un cas particulier, n'est naturellement pas supposé connu.

Étant donné l'idéal $\mathfrak{M} = (f, g)$, nous supposons que les courbes de base $f = 0$, $g = 0$, sans partie commune, n'ont pas de direction

---

$\varphi \not\subset \mathfrak{p}$, on a $\psi \subset \mathfrak{q}$. Dans le cas des idéaux de polynomes, l'idéal $\mathfrak{p}$ admettant une base, il existe un nombre ρ minimum, appelé *exposant de* $\mathfrak{q}$, et tel que $\mathfrak{p}^\rho \subset \mathfrak{q}$.

Si deux idéaux $\mathfrak{p}$ et $\mathfrak{q}$ ont les trois propriétés :

1° $\mathfrak{q} \subset \mathfrak{p}$;

2° $\varphi \subset \mathfrak{p}$ entraine : il existe λ tel que $\varphi^\lambda \subset \mathfrak{q}$;

3° $\varphi\psi \subset \mathfrak{q}$, $\varphi \not\subset \mathfrak{p}$ entraînent $\psi \subset \mathfrak{q}$, $\mathfrak{q}$ est primaire et $\mathfrak{p}$ est l'idéal premier correspondant. (Démonstration facile, *voir* par exemple B. L. VAN DER WAERDEN, *Moderne Algebra*, t. 2, p. 33, III.)

Soit $\mathfrak{p}$ l'idéal premier des polynomes (à un nombre n quelconque de variables) nuls en un point O. Étant donné un entier positif α et un polynome h n'appartenant pas à $\mathfrak{p}$, il existe un polynome η tel que l'on ait

$$\eta h = 1 + P \qquad \text{avec} \qquad P \subset \mathfrak{p}^\alpha.$$

En effet O étant pris comme origine, mettons en évidence les différents polynomes homogènes dont h est la somme

$$h = h_0 + h_1 + \ldots + h_m, \qquad h_0 = \text{const. non nulle.}$$

En cherchant η sous la même forme

$$\eta = \eta_{i_0} + \eta_{i_1} + \ldots,$$

nous avons les conditions

$$\eta_{i_0} h_0 = 1,$$
$$\eta_{i_1} h_0 + \eta_{i_0} h_1 = 0,$$
$$\ldots\ldots\ldots\ldots,$$

qui déterminent de proche en proche les η_i; on peut prendre pour η un polynome de degré $\alpha - 1$.

Conséquence. — Si $\mathfrak{p}$ est l'idéal premier des polynomes nuls en un point donné et si $\mathfrak{q}$ est un idéal tel que l'on ait

$$\mathfrak{p}^\rho \subset \mathfrak{q} \subset \mathfrak{p}$$

(donc un idéal simple), $\mathfrak{q}$ est primaire; l'idéal premier correspondant est $\mathfrak{p}$.

Il suffit de montrer que

$$\varphi\psi \subset \mathfrak{q}, \qquad \varphi \not\subset \mathfrak{p},$$

entraînent $\psi \subset \mathfrak{q}$. Or il existe, d'après le lemme, un polynome η tel que

$$\eta\varphi = 1 + P \quad \text{avec} \quad P \subset \mathfrak{p}^\rho \subset \mathfrak{q};$$

d'où

$$\eta\varphi\psi = \psi + \psi P,$$

et comme l'on a

$$\eta\varphi\psi \subset \mathfrak{q}, \qquad \psi P \subset \mathfrak{q},$$

il en résulte bien

$$\psi \subset \mathfrak{q}.$$

asymptotique commune, que Oy n'est parallèle à aucune direction asymptotique de f, à aucune des droites joignant deux à deux les différents points d'intersection M_i des deux courbes de base, ni enfin à aucune des tangentes à $f = 0$ en l'un quelconque de ces points M_i : nous exprimerons l'ensemble de ces hypothèses en disant que Oy est *régulier*.

Si un polynome $\varphi(x, y)$ satisfait à l'identité

$$\varphi = Af + Bg, \tag{1}$$

on peut choisir les polynomes A et B d'une infinité de manières : à partir d'un tel couple, on en obtient une infinité d'autres en posant

$$A_1 = A + \lambda g \qquad B_1 = B - \lambda f,$$

où λ est un polynome arbitraire. Nous fixerons le choix des polynomes A et B de la manière suivante : d'après les hypothèses faites sur Oy, le polynome f, de degré m, contient effectivement un terme en y^m. On peut alors supposer B de degré $m - 1$ en y, car dans le cas contraire il suffirait de le remplacer par le reste B_1 de sa division par f suivant les puissances de y. *Avec cette convention, l'identité* (1), *pour un polynome* φ *de l'idéal* $\mathfrak{m} = (f, g)$, *n'est plus possible que d'une seule manière.*

Soit

$$R(x) = U(x, y) f(x, y) + V(x, y) g(x, y), \tag{3}$$

un polynome en x seul appartenant à l'idéal $\mathfrak{m}$. Ce polynome pourra être le résultant ou le sous-résultant; nous n'utiliserons ici qu'une propriété, vérifiée aussi bien pour le sous-résultant que pour le résultant (¹) : dans l'identité (3), où U et V sont supposés choisis de la manière qui vient d'être précisée, les coefficients de

---

(¹) Si l'on désigne par $\mathcal{R}(x)$ le résultant, par $R(x)$ le sous-résultant des polynomes f et g et que l'on pose

$$\mathcal{R}(x) = \mathfrak{U}(x, y) f + \mathfrak{V}(x, y) g, \qquad R(x) = U(x, y) f + V(x, y) g,$$
$$\mathfrak{U}(x, y) = \mathfrak{U}_0(x) y^{n-1} + \mathfrak{U}_1(x) y^{n-2} + \ldots + \mathfrak{U}_{n-1}(x),$$
$$\mathfrak{V}(x, y) = \mathfrak{V}_0(x) y^{m-1} + \mathfrak{V}_1(x) y^{m-2} + \ldots + \mathfrak{V}_{m-1}(x),$$

on a

$$\mathcal{R}(x) = R(x) P(x),$$

où $P(x)$ est le p. g. c. d. des polynomes $\mathfrak{V}_0(x)$, $\mathfrak{V}_1(x)$, ..., $\mathfrak{V}_{m-1}(x)$.

ces polynomes appartiennent au plus petit corps contenant les coefficients des polynomes f et g.

Désignons par $\varphi(x, y)$ un polynome quelconque. Nous avons

$$R(x)\varphi(x, y) = U\varphi f + V\varphi g = Sf + Tg, \tag{4}$$

T étant le reste de la division de $V\varphi$ par f suivant les puissances de y, d'où résulte immédiatement le

THÉORÈME I. — *La condition nécessaire et suffisante pour qu'un polynome $\varphi(x, y)$ satisfasse à l'identité* (1) *est que le reste $T(x, y)$ de la division de $V\varphi$ par f suivant les puissances de y soit divisible par $R(x) = Uf + Vg$.*

Cette condition est évidemment nécessaire puisque de (1) et (4) résulte $T = RB$. Elle est suffisante, car si $R(x)$ divise T, il divise le produit Sf, donc S, puisque $f = 0$ n'admet pas Oy comme direction asymptotique.

Telle est la forme que prend la remarque de van der Woude lorsqu'on précise en outre, comme nous l'avons fait, le choix des polynomes coefficients dans toute identité de la forme (1).

On remarquera que le théorème I fournit, par un procédé rationnel, les polynomes A et B relatifs à un polynome φ de l'idéal $\mathfrak{m}$. *Les coefficients de* $A(x, y)$ *et* $B(x, y)$ *appartiennent donc au plus petit corps contenant les coefficients de f, g et φ.*

Le polynome $R(x)$ est le produit de facteurs primaires correspondant biunivoquement, d'après le choix de Oy, aux différents points d'intersection M_i des courbes de base

$$R(x) = (x - x_1)^{\sigma_1}(x - x_2)^{\sigma_2}\ldots(x - x_N)^{\sigma_N},$$

et *pour que $\varphi(x, y)$ appartienne à l'idéal $\mathfrak{m}$, il faut et il suffit que le reste $T(x, y)$ correspondant soit divisible séparément par chacun des facteurs primaires $(x - x_i)^{\sigma_i}$.* Or l'ensemble des polynomes $\varphi(x, y)$ tels que le reste T correspondant soit divisible par $(x - x_i)^{\sigma_i}$ est un idéal, $\mathfrak{q}_i$ (vérification immédiate).

Ce qui précède peut donc s'exprimer de la manière suivante : *l'idéal $\mathfrak{m}$ est le p. p. c. m. des idéaux $\mathfrak{q}_i$ relatifs aux différents points d'intersection des courbes de base*

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_N].$$

Il y a lieu maintenant d'étudier ces idéaux $\mathfrak{q}_i$ (et notamment de montrer qu'ils sont primaires).

Considérons l'un des points d'intersection, M_1 par exemple, et, pour simplifier l'écriture, prenons-le comme origine O. Posons

$$R(x) = x^{\sigma}(x - x_2)^{\sigma_2} \dots (x - x_N)^{\sigma_N} = x^{\sigma} R_1(x), \qquad R_1(o) \neq o,$$

Désignons par $\mathfrak{q}$ l'idéal $\mathfrak{q}_1$ relatif à l'origine, par $\mathfrak{p}$ l'idéal premier constitué par tous les polynomes nuls en O.

Soit $\varphi(x, y)$ un polynome quelconque de $\mathfrak{q}$; on a

$$T(x, y) = x^{\sigma} T_1(x, y);$$

d'où d'après (4)

$$R_1(x)\varphi(x, y) = S_1 f + T_1 g, \qquad \subset \mathfrak{m} \subset \mathfrak{p}, \tag{5}$$

d'où, puisque $R_1(o)$ est différent de o,

$$\varphi(x, y) \subset \mathfrak{p},$$

donc

$$\mathfrak{q} \subset \mathfrak{p}. \tag{6}$$

L'idéal $\mathfrak{q}$ *est, d'après* (5), *l'ensemble des polynomes* φ *dont le produit par* $R_1(x)$ *appartient à* $\mathfrak{m}$; $R_1(x)$ n'appartenant pas à $\mathfrak{p}$, on peut faire correspondre à tout entier positif α un polynome $L(x, y)$ tel que l'on ait

$$R_1(x) L(x, y) = 1 + P(x, y) \quad \text{avec} \quad P(x, y) \subset \mathfrak{p}^{\alpha}.$$

En multipliant les deux membres de (5) par L, on obtient

$$\varphi(x, y) = LS_1 f + LT_1 g - \varphi P \subset (\mathfrak{m}, \mathfrak{p}^{\alpha})$$

de sorte que *l'on a, quel que soit l'entier positif* α,

$$\mathfrak{q} \subset (\mathfrak{m}, \mathfrak{p}^{\alpha}). \tag{7}$$

Nous allons établir maintenant une proposition qui est en quelque sorte la réciproque de la relation (7), et dont le théorème de Noether, sous sa forme classique, résulte immédiatement.

Soient r et l les ordres en O des polynomes f et V (1).

---

(1) Un polynome f est dit d'ordre r en O quand O est point r-uple pour la courbe $f = o$.

Théorème II. — *On a*

$$(\mathfrak{m}, \mathfrak{p}^{\alpha}) \subset \mathfrak{q} \qquad \text{dès que} \qquad \alpha \geqq \sigma + r - 1 - l \quad (^1).$$

En d'autres termes, un polynome $\varphi(x, y)$, *pour lequel on peut déterminer des polynomes* A′ *et* B′ *tels que la différence*

$$\Delta = \varphi - A'f - B'g$$

soit en O *d'ordre au moins égal à* $\sigma + r - 1 - l$ (condition de Noether), *appartient à l'idéal* $\mathfrak{q}$.

Soit φ un tel polynome, nous devons montrer que le reste $T(x, y)$ de la division de $V\varphi$ par f suivant les puissances de y est divisible par x^{σ}. Supposons-le divisible seulement par $x^{\sigma-\tau}$ $(1 \leqq \tau \leqq \sigma)$. L'identité (4) donne

$$x^{\tau} R_1(x)\varphi = S_1 f + T_1 g, \tag{4'}$$

$T_1(0, y)$ étant un polynome non identiquement nul. En posant

$$f(0, y) = y^r f_1(y) \qquad (f_1(0) \neq 0).$$

et remarquant que $f_1(y)$ et $g(0, y)$ sont deux polynomes premiers entre eux en raison des hypothèses faites sur le choix des axes, on voit, à partir de (4′), que l'on a

$$T_1(0, y) = f_1(y)\Theta(y).$$

L'identité de la division de $V\varphi$ par f

$$V\varphi = Qf + T,$$

peut s'écrire d'autre part

$$x^{\sigma-\tau} T_1 = V(A'f + B'g + \Delta) - Qf$$

$$x^{\sigma-\tau} T_1 = B' x^{\sigma} R_1(x) + Cf + V\Delta, \tag{8}$$

en posant

$$C = A'V - B'U - Q.$$

Le polynome $Cf + V\Delta$ étant multiple de $x^{\sigma-\tau}$ et $V\Delta$ étant en O

---

(1) On remarquera que

$$(\mathfrak{m}, \mathfrak{p}^{\alpha'}) \subset (\mathfrak{m}, \mathfrak{p}^{\alpha}) \quad \text{si} \quad \alpha' \geqq \alpha.$$

d'ordre au moins égal à $\sigma + r - 1$, toute partie homogène du produit Cf de degré inférieur à $\sigma + r - 1$ est multiple de $x^{\sigma-\tau}$. Comme le polynome homogène de degré minimum r dans f n'est pas divisible par x, toutes les parties homogènes de C de degré inférieur à $\sigma - 1$ sont divisibles par $x^{\sigma-\tau}$ (ou identiquement nulles), ainsi qu'on le voit de proche en proche en commençant par celle qui a le degré minimum. Nous pouvons donc écrire

$$C = x^{\sigma-\tau} C_1 + C_2,$$

C_2 étant en O d'ordre au moins égal à $\sigma - 1$.

L'identité (8) s'écrit alors

$$T_1 = B' x^{\tau} R_1(x) + C_1 f + D, \tag{9}$$

en posant

$$C_2 f + V\Delta = x^{\sigma-\tau} D(x, y).$$

Le polynome D est en O d'ordre au moins égal à

$$\sigma + r - 1 - (\sigma - \tau) = r + \tau - 1 \geqq r,$$

de sorte que l'on a

$$D(o, y) = y^r D_1(y).$$

En faisant $x = o$ dans (9) nous obtenons

$$T_1(o, y) = f_1(y)\,\Theta(y) = C_1(o, y)\,y^r f_1(y) + y^r D_1(y),$$

qui exige

$$\Theta(y) = \text{multiple de } y^r,$$

d'où

$$T_1(o, y) = \text{multiple de } f(o, y),$$

ce qui est impossible, puisque le degré du premier membre est inférieur au degré du second.

Le théorème précédent admet plusieurs conséquences importantes.

1° En premier lieu, le théorème de Noether sous sa forme classique en résulte immédiatement. Le nombre ρ_i est au plus égal à $\sigma_i + r_i - 1 - l_i$ et un polynome φ satisfaisant à la condition de l'énoncé A appartient à chacun des idéaux $\mathfrak{q}_i$, donc à

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_N].$$

Réciproquement, pour un polynome φ satisfaisant à l'identité (1), on pourra prendre, quel que soit i, $A_i = A$, $B_i = B$ et la différence $\varphi - Af - Bg$, identiquement nulle, sera d'ordre supérieur à ρ_i.

2° Pour $\alpha \geqq \sigma + r - 1 - l$, on a

$$(\mathfrak{m}, \mathfrak{p}^\alpha) \subset \mathfrak{q}.$$

En comparant à la relation (7), valable quel que soit α, nous voyons que l'on a

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^\alpha), \tag{10}$$

dès que

$$\alpha \geqq \sigma + r - 1 - l.$$

En particulier

$$\mathfrak{p}^\alpha \subset \mathfrak{q} \subset \mathfrak{p} \tag{11}$$

pour

$$\alpha \geqq \sigma + r - 1 - l,$$

d'où résulte (note, p. 102-103), que $\mathfrak{q}$ *est primaire et que* $\mathfrak{p}$ *est l'idéal premier correspondant.* Les relations

$$S(x, y)\varphi(x, y) \subset \mathfrak{m}$$
$$S \not\subset \mathfrak{p},$$

entraînent donc

$$\varphi \subset \mathfrak{q}.$$

L'exposant ρ de $\mathfrak{q}$, plus petit entier tel que l'on ait

$$\mathfrak{p}^\rho \subset \mathfrak{q},$$

satisfait, d'après (11), à l'inégalité

$$\rho \leqq \sigma + r - 1 - l. \tag{12}$$

On vérifie immédiatement que ρ est l'entier minimum pour lequel on a

$$(\mathfrak{m}, \mathfrak{p}^\rho) \subset \mathfrak{q} \qquad \mathfrak{p}^\rho \subset (\mathfrak{m}, \mathfrak{p}^{\rho+1}).$$

3° Enfin nous pouvons énoncer le théorème de Noether sous la forme algébrique suivante :

L'idéal $\mathfrak{m} = (f, g)$ *est le p. p. c. m. d'un nombre fini*

d'idéaux primaires relatifs aux différents points d'intersection des courbes de base

$$\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_N]$$

(*théorème de décomposition*).

3. **Compléments.** — Nous supposons maintenant que *le polynome* $R(x) = x^\sigma R_1(x)$ *considéré est le sous-résultant.* Comme on a

$$x\mathfrak{p} \subset \mathfrak{p}\mathfrak{p} \subset \mathfrak{q},$$

et par suite

$$x\mathfrak{p} R_1(x) \subset \mathfrak{m},$$

σ satisfait nécessairement à l'inégalité

$$\sigma \leqq \rho \qquad (\leqq \sigma + r - 1 - l),$$

et nous avons

$$l \leqq r - 1.$$

Théorème (1). — *La valeur de* ρ *est donnée par la formule*

$$\rho = \sigma + r - 1 - l. \tag{13}$$

On en déduit bien aisément que :

Si les courbes de base ne sont pas tangentes en O (*cas simple*) *on a*

$$\rho = r + s - 1,$$

ce qui donne l'énoncé B',

La multiplicité de Noether ρ est évidemment invariante vis-à-vis des transformations homographiques. Il n'en est pas de même de l'ordre de multiplicité σ de la racine $x = 0$ pour le sous-résultant. Cependant, ainsi que je l'ai établi dans ma thèse (2), ces deux nombres sont *en général* égaux. On a en effet le théorème suivant :

Théorème. — *L'axe* Ox *étant fixé, on peut toujours choisir l'axe* Oy *de manière que l'ordre de multiplicité* σ *de la racine* $x = 0$ *pour le sous-résultant* $R(x)$ *soit égal à* ρ. *Si on appelle*

(1) *Loc. cit.* (6), p. 26.

(2) *Loc. cit.* (6), p. 7. Je considère, dans ma thèse, le cas général d'un idéal ayant pour variété un système de points.

normal un axe Oy *régulier pour lequel on a* $\sigma = \rho$, *il n'existe, lorsque* Ox *est fixé, qu'un nombre fini de positions non-normales de* Oy.

Si la direction de l'axe Oy est normale pour tous les points d'intersection M_1, M_2, ..., M_N, l'expression du sous-résultant est

$$R(x) = A \prod_{i=1}^{N} (x - x_i)^{\rho_i},$$

A étant une constante.

La condition nécessaire et suffisante pour qu'un axe Oy, régulier, soit normal (en un point d'intersection O) est que l'on ait la relation

$$l = r - 1.$$

Oy étant normal, si dans l'identité

$$R(x) = x^{\rho} R_1(x) = Uf + Vg,$$

on remplace la variable y par la fonction algébrique de x définie par une branche de la courbe $f = 0$ passant par le point O, $g(x, y)$ devient comme on sait une fonction de x dont l'ordre infinitésimal par rapport à x est $s + N$, N désignant la somme des ordres de contact de la branche de f considérée avec toutes les branches de g; $V(x, y)$, polynome d'ordre $r - 1$ en O, devient une fonction d'ordre $r - 1$ au moins. On a donc pour ρ la limite inférieure, souvent utile

$$\rho \geqq r + s - 1 + N. \tag{14}$$

Si k désigne la multiplicité de Bezout relative aux deux courbes de base et au point d'intersection O considéré, on a, d'après la définition du sous-résultant

$$\sigma \leqq k,$$

ce qui donne

$$\rho \leqq k.$$

Cas particulier. — Supposons le point O *simple pour l'une des deux courbes de base;* soit par exemple $r = 1$. La condition de normalité est satisfaite d'elle-même. On a d'autre part

$$k = s + N,$$

le nombre N étant pris pour la branche unique de f qui passe

par O; k est égal au second membre de l'inégalité (14); on a donc (en supposant Oy régulier)

$$\sigma = \rho = k = s + N. \tag{15}$$

De plus la condition nécessaire et suffisante pour qu'un polynome $\varphi(x, y)$ *appartienne au composant primaire* $\mathfrak{q}$ *de l'idéal* (f, g) *en* O *est que la multiplicité*

$$\rho' = k' = s' + N',$$

relative à l'intersection des courbes $f = 0$, $\varphi = 0$ *soit supérieure ou égale à* ρ (s', ordre de φ en O; N', somme des ordres de contact de la branche de $f = 0$ passant par O avec les différentes branches de φ).

Reprenons en effet les deux identités déjà utilisées

$$V\varphi = Qf + x^{\mu} T_1(x, y) \qquad T_1(o, y) \neq o, \tag{16}$$

$$x^{\rho} R_1(x)\varphi = Sf + x^{\mu} T_1(x, y)\, g(x, y) : \tag{17}$$

1° Si l'on a

$$\varphi \subset \mathfrak{q}, \qquad \text{c'est-à-dire} \quad \mu \geq \rho,$$

il en résulte, d'après (16), que l'ordre infinitésimal $s' + N'$ de $\varphi(x, y)$ lorsqu'on remplace y par la fonction de x définie au voisinage de O par $f = 0$, est au moins égal à μ, donc au moins égal à ρ.

2° Si l'on a

$$\varphi \not\subset \mathfrak{q}, \qquad \text{c'est-à-dire} \quad \mu < \rho,$$

on voit, en divisant les deux membres de (17) par x^{μ} et faisant $x = 0$, que le polynome $T_1(0, y)$, de degré $m - 1$ au plus en y (m, degré de f), doit être divisible par le polynome

$$f_1(y) = \frac{1}{y} f(0, y),$$

qui est de degré $m - 1$ et non nul pour $y = 0$, ce qui entraîne

$$T_1(0, 0) \neq 0.$$

L'ordre infinitésimal $s' + N'$ de φ est donc égal à μ, c'est-à-dire inférieur à ρ.

Pour poursuivre l'étude du composant primaire $\mathfrak{q}$ de l'idéal $\mathfrak{m} = (f, g)$ en un point d'intersection O des courbes de base, il y

a lieu d'utiliser la proposition suivante, bien naturelle, puisque $\mathfrak{q}$ ne dépend évidemment que des propriétés *locales* des courbes de base :

On ne diminue en rien la généralité en supposant que les polynomes $f(x, y)$, $g(x, y)$ ont leur degré en y égal à leur ordre, r ou s, au point O, *et sont de plus décomposés en facteurs irréductibles correspondant à leurs différents systèmes circulaires en* O (¹). Les théorèmes suivants vont précisément permettre d'utiliser la décomposition des polynomes de base f et g.

Soient $\varphi_1(x, y) = 0$, $\varphi_2(x, y) = 0$, $\varphi_3(x, y) = 0$, trois courbes algébriques passant par O et deux à deux sans partie commune. Soient $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\mathfrak{q}_3$, les composants primaires en O des idéaux

$$\mathfrak{m}_1 = (\varphi_1, \varphi_2\varphi_3), \qquad \mathfrak{m}_2 = (\varphi_2, \varphi_3\varphi_1), \qquad \mathfrak{m}_3 = (\varphi_3, \varphi_1\varphi_2).$$

Désignons par τ_1, τ_2, τ_3 les exposants de $\mathfrak{q}_1$, $\mathfrak{q}_2$, $\mathfrak{q}_3$.

THÉORÈME III. — *On a*

$$[\mathfrak{q}_2, \mathfrak{q}_3] = [\mathfrak{q}_3, \mathfrak{q}_1] = [\mathfrak{q}_1, \mathfrak{q}_2],$$

et un quelconque des nombres τ_1, τ_2, τ_3 ne peut pas être supérieur à la fois aux deux autres (²).

On vérifie d'abord sans peine que, si l'on pose

$$\mathfrak{m} = (\varphi_1\varphi_2, \varphi_2\varphi_3, \varphi_3\varphi_1),$$

on a

$$\mathfrak{m} = [\mathfrak{m}_1, \mathfrak{m}_2] = [\mathfrak{m}_2, \mathfrak{m}_3] = [\mathfrak{m}_3, \mathfrak{m}_1].$$

Soit alors $\mathfrak{a}$ l'ensemble des polynomes Q à chacun desquels

---

(¹) *Loc. cit.* (6), théorème II, p. 22. La démonstration de ce théorème repose sur trois lemmes qui permettent de passer de deux polynomes f et g donnés à deux polynomes f et g satisfaisant aux conditions de l'énoncé. Dans le passage la multiplicité de Bezout k est conservée ainsi que l'ordre de contact d'une branche quelconque de f avec une branche quelconque de g. Dans les deux derniers lemmes, on peut laisser de côté les considérations relatives à l'ordre des polynomes A et B et à la normalité des axes.

(²) *Loc. cit.* (6), théorème VIII, p. 36; la démonstration de ma thèse utilise le théorème de décomposition et le fait que le p. p. c. m. de deux idéaux primaires relatifs au même idéal premier, est un idéal primaire. Il n'en est pas de même de la démonstration résumée dans le texte. On peut d'ailleurs vérifier immédiatement que l'idéal désigné par $\mathfrak{a}$ est primaire.

correspond un polynome S *non nul en* O tel que l'on ait

$$SQ \subset \mathfrak{m} \qquad (S \not\subset \mathfrak{p}).$$

On a

$$\mathfrak{a} = [\mathfrak{q}_1, \mathfrak{q}_2] = [\mathfrak{q}_2, \mathfrak{q}_3] = [\mathfrak{q}_3, \mathfrak{q}_1];$$

d'où en particulier

$$[\mathfrak{q}_2, \mathfrak{q}_3] \subset \mathfrak{q}_1, \tag{18}$$

et, si l'on suppose les notations choisies de manière que l'on ait

$$\tau_1 \geqq \tau_2 \geqq \tau_3,$$

la relation (18) entraîne nécessairement

$$\mathfrak{p}^{\tau_2} \subset \mathfrak{q}_1, \qquad \text{donc} \quad \tau_1 \leqq \tau_2$$

et par suite

$$\tau_1 = \tau_2.$$

Soient $f = 0$, $g = 0$ deux courbes sans partie commune passant par O, et supposons f décomposé en un certain nombre de facteurs deux à deux sans diviseur commun

$$f = f_1 f_2 \dots f_\mu.$$

Désignons par $\mathfrak{q}(\varphi, \psi)$ le composant primaire en O d'un idéal (φ, ψ), par $\rho(\varphi, \psi)$ son exposant et posons

$$\mathfrak{q} = \mathfrak{q}(f, g) = \mathfrak{q}(f_1 f_2 \dots f_\mu, g), \qquad \rho = \rho(f, g) = \rho(f_1 f_2 \dots f_\mu, g),$$
$$\mathfrak{q}_h = \mathfrak{q}(f_h f_{h+1} \dots f_\mu f_1 \dots f_{h-1} g), \qquad \rho_h = \rho(f_h f_{h+1} \dots f_\mu f_1 \dots f_{h-1} g)$$
$$(h = 1, 2, \dots, \mu).$$

THÉORÈME IV. — *On a*

$$[\mathfrak{q}_1, \mathfrak{q}_2, \dots \mathfrak{q}_\mu] \subset \mathfrak{q}.$$

En supposant les notations telles que l'on ait

$$\rho_1 \geqq \rho_2 \geqq \dots \geqq \rho_\mu,$$

l'exposant ρ *satisfait à l'inégalité*

$$\rho \leqq \rho_1,$$

avec nécessairement

$$\rho = \rho_1, \qquad \text{si} \quad \rho_1 > \rho_2.$$

Pour $\mu = 2$, ce théorème n'est autre que le théorème III. Sup-

posons donc la propriété établie pour un nombre de facteurs f_h inférieur ou égal à $\mu - 1$. On a, d'après le théorème III

$$\mathfrak{q} = \mathfrak{q}(f_1 \dots f_{\mu-1}, f_\mu, g) \supset [\mathfrak{q}(f_1 \dots f_{\mu-1}, f_\mu g), \mathfrak{q}_\mu],$$

et comme

$$\mathfrak{q}(f_1 \dots f_{\mu-1}, f_\mu, g) \supset [\mathfrak{q}_1, \dots, \mathfrak{q}_{\mu-1}],$$

il vient

$$\mathfrak{q} \supset [\mathfrak{q}_1, \dots, \mathfrak{q}_{\mu-1}, \mathfrak{q}_\mu].$$

L'exposant ρ est inférieur ou égal au plus grand des deux exposants ρ_μ et

$$\rho' = \rho(f_1 \dots f_{\mu-1}, f_\mu g),$$

et nécessairement égal si l'on a $\rho' \neq \rho_\mu$.

Or nous avons

$$\rho' \leqq \rho_1 \qquad \rho_\mu \leqq \rho_1;$$

d'où

$$\rho \leqq \rho_1.$$

D'autre part, l'inégalité $\rho_1 > \rho_2$ entraîne

$$\rho' = \rho_1 \qquad (> \rho_\mu),$$

et par suite

$$\rho = \rho_1 \qquad \text{C. Q. F. D.}$$

Il nous reste à indiquer les conséquences de ce théorème :

1° *Supposons que* O *soit point r-uple à tangentes distinctes pour la courbe* $f = 0$. On peut alors remplacer f par l'ensemble de r courbes passant simplement par O : $f_1 = 0, \dots, f_r = 0$. Si nous désignons par N_h la somme des ordres de contact de la branche $f_h = 0$ avec les différentes branches de $g = 0$, par N le plus grand des nombres N_h, nous avons d'après (15)

$$\rho_h = \rho(f_h, f_{h+1} \dots f_{h-1} g) = r + s - 1 + N_h;$$

d'où

$$\rho \leqq r + s - 1 + N,$$

et, puisque $r + s - 1 + N$ est précisément une limite inférieure de ρ,

$$\rho = r + s - 1 + N.$$

Pour qu'un polynome φ appartienne à $\mathfrak{q}$, il *suffit* qu'il appartienne aux idéaux $\mathfrak{q}_h (h = 1, 2, \dots, r)$. Or les multiplicités d'in-

tersection de $f_h = 0$ avec $g = 0$ et $f_{h+1} \ldots f_{h-1}\, g = 0$ sont

$$s + N_h = \mu_h \qquad \text{et} \qquad r + s - 1 + N_h = r - 1 + \mu_h,$$

et la condition nécessaire et suffisante pour que φ appartienne à $\mathfrak{q}_h$ est que $\varphi = 0$ coupe $f_h = 0$ avec une multiplicité au moins égale à $r - 1 + \mu_h$: *nous obtenons donc l'énoncé* B″ (1).

2° Si au point O les courbes $f = 0$, $g = 0$ n'admettent qu'*une tangente commune, simple par exemple pour* $f = 0$, on a, en désignant par N la somme des ordres de contact de la branche $f_1 = 0$ de f tangente à $g = 0$, par $f_2 = 0$ l'ensemble des autres branches de f

$$\rho_1 = \rho(f_1, f_2 g) = r + s - 1 + N,$$
$$\rho_2 = \rho(f_2, f_1 g) = r + s - 1;$$

d'où

$$\rho = \rho_1 = r + s - 1 + N,$$

et comme la multiplicité de Bezout a pour valeur ici

$$k = rs + N,$$

on obtient

$$\rho = k - (r - 1)(s - 1),$$

relation déjà vérifiée lorsque les deux courbes de base ne présentent aucun contact ($\rho = r + s - 1$, $k = rs$).

Quelle que soit la disposition des courbes de base en O, *on a l'inégalité* (2)

$$\rho \leq k - (r - 1)(s - 1),$$

et l'égalité n'a lieu que si les courbes de base ont au plus une tangente commune simple pour l'une d'elles (3). De ce qui précède et de la relation (15) résulte immédiatement que *la*

---

(1) La condition ainsi obtenue est seulement *suffisante.* Mais on peut la remplacer par une condition nécessaire et suffisante en imposant à la courbe $B = 0$ (B étant le polynome défini par l'identé $\varphi = Af + Bg$) d'être une *adjointe* pour $f = 0$. Sur ce point et sur l'intérêt de l'énoncé B″ pour la démonstration du théorème du Reste, *voir* les travaux de B. L. van der Waerden déjà cités note (2), p. 99.

(2) Cette inégalité a été établie par Bertini et Voss; *voir* par exemple, Voss, *Uber einen Fundamentalsatz der theorie der algebraischen Funktionen* (*Math. Ann.*, t. 27, p. 533).

(3) *Loc. cit.* (6), p. 35.

condition nécessaire et suffisante pour que le résultant et le sous-résultant soient identiques ($\rho = k$ *en tout point d'intersection*) *est que tout point d'intersection des deux courbes de base soit simple au moins pour l'une de ces deux courbes.*

3° Soient $f = 0$, $g_1 = 0$, $g_2 = 0$ trois courbes deux à deux sans partie commune admettant O comme point multiple d'ordres r, s_1 et s_2. Posons

$$q = q(f, g_1 g_2), \qquad q_1 = q(f, g_1), \qquad q_2 = q(f, g_2),$$
$$\rho = \rho(f, g_1 g_2), \qquad \rho_1 = \rho(f, g_1), \qquad \rho_2 = \rho(f, g_2).$$

Théorème V (¹). — *On a*

$$\rho \geqq \rho_1 + s_2,$$

et l'égalité a lieu si les courbes $f = 0$, $g_2 = 0$ *ne sont pas tangentes en* O.

En appliquant simultanément ce théorème et le théorème IV, on obtient un résultat fondamental pour le calcul de l'exposant.

Soient D_1, D_2, ..., D_λ les tangentes communes, simples ou multiples, aux deux courbes de base au point O. On peut supposer, sans diminuer la généralité, les équations de ces courbes de la forme

$$f = f_0 f_1 \dots f_\lambda = 0, \qquad g = g_0 g_1 \dots g_\lambda = 0,$$

$f_0 = 0$ n'étant pas tangente à $g = 0$, $g_0 = 0$ n'étant pas tangente à $f = 0$, $f_h = 0$ et $g_h = 0$ groupant les branches de $f = 0$ et de $g = 0$ tangentes à D_h. Si l'on pose

$$\rho(f_h, g_h) = r_h + s_h - 1 + M_h$$

et

$$f = f_h f_h, \qquad g = g'_h g_h,$$

on a, d'après le théorème V,

$$\rho(f_h, f'_h g) = r + s - 1 + M_h.$$

Si les notations sont telles que l'on ait

$$M_1 \geqq M_2 \geqq \dots \geqq M_\lambda \qquad (\geqq M_0 = 0)$$

(¹) *Loc. cit.* (6), théorème VII, p 28.

le théorème IV entraîne

$$\rho(f, g) = \rho \leqq r + s - 1 + M_1.$$

Or du théorème V résulte l'inégalité

$$\rho(f, g) \geqq \rho(f, g_1) + s - s_1 = \rho(f_1, g_1) + r - r_1 + s - s_1 = r + s - 1 + M_1,$$

de sorte que l'on a finalement

$$\rho = r + s - 1 + M_1.$$

Ainsi *on est ramené, pour le calcul de l'exposant, au cas où les courbes de base ont toutes leurs tangentes confondues avec une même droite* (1).

---

(1) Pour l'étude de ce cas, voir *loc. cit.* (6), Chapitre III, p. 43 à 70.