JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

G. DUMAS

Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels

Journal de mathématiques pures et appliquées 6^e série, tome 2 (1906), p. 191-258.
<http://www.numdam.org/item?id=JMPA_1906_6_2__191_0>

Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels;

PAR M. G. DUMAS.

Les polygones de Newton occupent une place importante dans la théorie des fonctions algébriques d'une variable. Par leur intermédiaire, les résultats prennent une forme concise et élégante qu'il serait difficile d'obtenir autrement.

Dans le présent travail (1) je me propose de montrer comment l'introduction de ces polygones dans l'étude des polynomes à coefficients rationnels met en évidence plusieurs faits nouveaux et permet, sous une forme tout à fait générale et intuitive, d'énoncer certains théorèmes qui se rattachent au critère d'irréductibilité découvert par Eisenstein.

Les suites ordonnées suivant les puissances croissantes d'un nombre premier p, introduites récemment dans la Science par M. Hensel, m'ont rendu la tâche facile. C'est dans celles-ci, en effet, que semble

(1) Ce Mémoire est, à peu de chose près, identique à celui que l'auteur a présenté, en décembre 1904, à l'École Polytechnique de Zürich, pour l'obtention du grade de Privat-Docent. Seules quelques adjonctions, celle notamment de tout le premier paragraphe et de plusieurs numéros du deuxième, ont été faites pour rappeler ce que sont les notions nouvelles, constituant la base même de cette étude.

résider la raison profonde de l'analogie complète entre la théorie des fonctions algébriques et l'analyse supérieure des nombres.

D'une manière générale, je supposerai connues les notions développées par ce savant dans ses Mémoires du *Journal de Crelle* (1). Il peut être utile également de comparer la première partie de ce travail avec les paragraphes du commencement de ma thèse (2) dans lesquels se trouvent exposés, sous forme différente, plusieurs résultats correspondant à ceux qui sont ici.

Les deux premiers paragraphes de la première Partie sont consacrés au rappel des notions dues à M. Hensel; les suivants à l'établissement de propositions relatives à des polynomes dont les coefficients sont des suites de Hensel.

La seconde Partie renferme des applications aux polynomes à coefficients rationnels, considérés comme cas particuliers des précédents.

Les théorèmes obtenus aux paragraphes **8**, **9** et **10**, relatifs à l'irréductibilité et à l'existence d'un plus grand commun diviseur, peuvent pour la plupart, ainsi qu'on s'en rend facilement compte, être établis directement, sans introduction des suites de Hensel.

Il n'y a pour cela qu'à donner indépendamment de celles-ci pour un polynome à coefficients rationnels (ou plus généralement pour un polynome dont les coefficients appartiennent à un domaine donné de rationalité) la définition du polygone de Newton relatif à un nombre premier. Le théorème du paragraphe **3** sur la composition des polygones n'en restera pas moins vrai et, de ce fait, toutes les considérations qui en découlent directement.

La même remarque s'appliquerait d'une façon pour le moins très étendue au problème résolu paragraphe **11**, dans lequel se détermine la puissance exacte d'un nombre premier p entrant comme diviseur dans le résultant des deux polynomes.

Le théorème du paragraphe **12** a des bases plus profondes. Son

---

(1) HENSEL, *Neue Grundlagen der Arithmetik* (*Journal de Crelle*, t. **127**). — *Ueber eine neue Begründung der Theorie der algebraischen Zahlen* (*Journal de Crelle*, t. **128**).

(2) DUMAS, *Sur les fonctions à caractère algébrique dans le voisinage d'un point donné*. Paris, 1904.

énoncé suppose les suites de Hensel, ma démonstration, les méthodes de ce géomètre. Celles-ci permettent de se passer d'idéaux dont la notion intervient souvent avec fruit dans mainte question d'irréductibilité. Le théorème du dernier paragraphe de ce Mémoire contient d'ailleurs comme cas particulier une proposition, due à Schœnemann, établie récemment par M. Michael Bauer (¹). Il me paraît utile de renvoyer à son travail pour la comparaison des méthodes.

PREMIÈRE PARTIE.

---

§ 1.

1. Les suites ou séries introduites par M. Hensel dans la Science mathématique sont de la forme

$$a_\rho p^\rho + a_{\rho+1} p^{\rho+1} + \ldots + a_{\rho+k} p^{\rho+k} + \ldots .$$

Elles se poursuivent aussi loin que l'on veut; p représente un nombre premier quelconque et les coefficients a_ρ, $a_{\rho+1}$, $a_{\rho+2}$, ... sont égaux à $0, 1, 2, \ldots$, ou $p-1$, le premier a_ρ étant différent de zéro.

Le premier exposant ρ qui, par hypothèse, est un nombre entier peut être positif, nul ou négatif; c'est une quantité toujours finie, de sorte que les suites ci-dessus ne pourront jamais contenir, si elles en contiennent, qu'un nombre fini de termes dans lesquels l'exposant de p est négatif.

Une suite dans laquelle ρ est négatif est dite à *caractère rationnel;* si ρ est nul ou positif, elle est à *caractère entier*. Ces définitions sous-entendent les mots *dans le domaine du nombre premier p*. Souvent,

---

(¹) MICHAEL BAUER, *Verallgemeinerung eines Satzes von Schœnemann* (*Journal de Crelle*, t. 128).

pour abréger, nous emploierons les termes *suites entières* et *suites rationnelles* en p.

2. Deux suites rationnelles en p sont *égales* lorsque, dans chacune d'elles, les coefficients des mêmes puissances de p sont identiques. Si l'on a, par exemple,

$$\mathrm{A} = a_0 + a_1 p + a_2 p^2 + \ldots,$$
$$\mathrm{B} = b_0 + b_1 p + b_2 p^2 + \ldots,$$

l'on dit que A est égal à B, ce qui s'écrit

$$\mathrm{A} = \mathrm{B} \qquad (p)$$

lorsque, *si loin que se poursuit la comparaison,* l'on a toujours

$$a_0 = b_0,$$
$$a_1 = b_1,$$
$$a_2 = b_2,$$
$$\ldots\ldots\ldots$$

Le (p) placé à droite de l'égalité en caractérise la nature, on ne l'écrit d'ailleurs que dans le cas d'ambiguïté possible, celui, par exemple, où A et B, au lieu de représenter les développements eux-mêmes, seront les quantités auxquelles ceux-ci correspondront. Comme nous le verrons du reste, une égalité entre deux suites rationnelles en p ne symbolise jamais qu'un nombre aussi grand que l'on veut de congruences selon des puissances de p à prendre comme modules.

3. Les suites dont on vient de parler sont *réduites,* parce que leurs coefficients a_ρ, $a_{\rho+1}$, $a_{\rho+2}$, ... sont supposés égaux à l'un ou l'autre des nombres 0, 1, 2, ..., ou $(p-1)$. Le calcul conduit constamment à des suites qui ne satisfont pas à cette condition et il faut savoir passer d'une suite quelconque à la suite réduite à laquelle elle *équivaut.*

Soit, par exemple,

$$\mathrm{A} = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$$

une suite dont les coefficients a_i sont entiers mais quelconques. Nous écrivons (¹)

$$A' = (a_0 - \varepsilon_1 p) + (\varepsilon_1 + a_1 - \varepsilon_2 p)p + (\varepsilon_2 + a_2 - \varepsilon_3 p)p^2 + \ldots + (\varepsilon_n + a_n - \varepsilon_{n+1} p)p^n + \ldots,$$

en déterminant, ce qui est toujours possible d'une seule façon, les ε_1, ε_2, ε_3, ..., de manière que les nouveaux coefficients

$$\begin{aligned} a_0 - \varepsilon_1 p &= a'_0, \\ \varepsilon_1 + a_1 - \varepsilon_2 p &= a'_1, \\ &\ldots\ldots\ldots\ldots, \\ \varepsilon_n + a_n - \varepsilon_{n+1} p &= a'_n, \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

soient tous égaux à 0, 1, 2, ... ou $(p-1)$. La nouvelle suite ainsi obtenue

$$A' = a'_0 + a'_1 p + a'_2 p^2 + \ldots + a'_n p^n + \ldots$$

est *équivalente* à la proposée A. Elle est réduite puisque ses coefficients sont tous positifs ou nuls et inférieurs à p.

4. Si l'on a

$$\begin{aligned} A &= a_0 + a_1 p + a_2 p^2 + \ldots, \\ B &= b_0 + b_1 p + b_2 p^2 + \ldots, \end{aligned}$$

la *somme* A + B et la *différence* A − B de ces deux suites seront par définition les suites réduites, égales respectivement aux deux suivantes

$$(a_0 \pm b_0) + (a_1 \pm b_1)p + (a_2 \pm b_2)p^2 + \ldots;$$

le *produit* AB, la suite réduite équivalente à

$$a_0 b_0 + (a_0 b_1 + a_1 b_0)p + (a_0 b_2 + a_1 b_1 + a_2 b_0)p^2 + \ldots;$$

(¹) HENSEL, *Neue Grundlagen*, etc., p. 52.

le *quotient* A : B la suite réduite, unique et bien déterminée C, vérifiant l'égalité

$$A = BC \qquad (p).$$

Ces définitions s'étendent immédiatement au cas où les suites au lieu de commencer chacune par un terme indépendant de p commencent par des termes quelconques de la forme $a_\rho p^\rho$ et $b_\lambda p^\lambda$, par exemple.

On pourra de même être amené à considérer les somme, différence, produit ou quotient de suites non réduites. Les définitions ci-dessus restent intactes. Il faut remarquer toutefois que nous excluons de nos considérations toute division par des suites (non réduites nécessairement) que l'on pourrait faire correspondre à la quantité zéro.

3. C'est d'une manière toute naturelle que l'on est conduit aux suites rationnelles en p. Si l'on écrit, en effet, un nombre entier rationnel positif quelconque A dans un système de numération à base p, l'on obtient, par exemple,

$$(1) \qquad A = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k,$$

où $a_0, a_1, \ldots, a_k$ sont des coefficients égaux à $0, 1, 2, \ldots,$ ou $p-1$. Sans insister sur la manière, bien connue, d'obtenir les coefficients a_i nous remarquerons que de l'égalité ci-dessus se déduisent les congruences

$$\begin{aligned}
&A \equiv a_0 && (\mathrm{mod}\, p),\\
&A \equiv a_0 + a_1 p && (\mathrm{mod}\, p^2),\\
&\ldots\ldots\ldots\ldots && \\
&A \equiv a_0 + a_1 p + \ldots + a_{k-1} p^{k-1} && (\mathrm{mod}\, p^k),\\
&A \equiv a_0 + a_1 p + \ldots + a_k p^k && (\mathrm{mod}\, p^{k+1}),
\end{aligned}$$

dont la dernière se réduit d'ailleurs à une identité.

Soient maintenant A et B deux nombres entiers quelconques positifs

ou négatifs non divisibles par p. On voit que l'algorithme

$$(2) \quad \begin{cases} A = A_0 p + B a_0, \\ A_0 = A_1 p + B a_1, \\ A_1 = A_2 p + B a_2, \\ \dots\dots\dots\dots\dots\dots, \\ A_{k-1} = A_k p + B a_k, \\ A_k = A_{k+1} p + B a_{k+1}, \\ \dots\dots\dots\dots\dots\dots\dots, \end{cases}$$

dans lequel les A_i comme les a_i sont déterminés d'une manière unique, puisque les a_i sont par hypothèse égaux à 0, 1, 2, ... ou $p-1$, permet d'écrire la suite, en général illimitée, de congruences

$$\begin{aligned} A &\equiv B a_0 && (\bmod p), \\ A &\equiv B(a_0 + a_1 p) && (\bmod p^2), \\ A &\equiv B(a_0 + a_1 p + a_2 p^2) && (\bmod p^3), \\ &\dots\dots\dots\dots\dots\dots \end{aligned}$$

Afin de résumer ces dernières en une formule unique, l'on introduit une suite de Hensel et l'on écrit

$$\frac{A}{B} = a_0 + a_1 p + a_2 p^2 + \dots \qquad (p).$$

Si, d'autre part, l'on remarque que la première des égalités (2) conduit à la congruence

$$-A \equiv B(p - a_0) \qquad (\bmod p)$$

dans laquelle $p - a_0$ comme a_0 est égal à 1, 2, ... ou $(p-1)$, l'on écrira immédiatement

$$(3) \quad \begin{cases} -A = -(B + A_0)p + B(p - a_0), \\ -(B + A_0) = -(B + A_1)p + B(p - 1 - a_1), \\ -(B + A_1) = -(B + A_2)p + B(p - 1 - a_2), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ -(B + A_{k-1}) = -(B + A_k)p + B(p - 1 - a_k), \\ -(B + A_k) = -(B + A_{k+1})p + B(p - 1 - a_{k+1}), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \end{cases}$$

et partant, la suite également réduite

$$-\frac{A}{B} = (p - a_0) + (p - 1 - a_1)p + (p - 1 - a_2)p^2 + \ldots + (p - 1 - a_k)p^k + \ldots.$$

Ceci met en évidence une règle fort utile pour passer du développement d'une quantité donnée à celui de la même quantité affectée du signe contraire.

6. *Les suites qui, dans le domaine d'un nombre premier p, correspondent à un nombre rationnel quelconque sont périodiques.*

Soit $\frac{A}{B}$ le nombre rationnel considéré; il suffit, d'après ce qui précède, de supposer A comme B tous deux positifs. Nous excluons aussi le cas où, $\frac{A}{B}$ se réduisant à un entier positif, la périodicité deviendrait évidente.

Des égalités (2) nous déduirons la suivante :

$$A = B(a_0 + a_1 p + \ldots + a_k p^k) + A_k p^{k+1}, \tag{4}$$

vraie pour tout indice k, et dans laquelle l'on a nécessairement, à partir de l'un d'entre eux,

$$-B < A_k < 0. \tag{5}$$

A étant de même que B positif, il ne pourrait, en effet, se faire que, constamment, l'on ait A_k positif. A_k, en outre, ne saurait pour aucun indice k s'annuler, puisque $\frac{A}{B}$ n'est pas entier positif.

Si, d'autre part, l'on avait A_k inférieur ou égal à $-B$, pour k quelconque l'on déduirait de (4)

$$A \leqq B(a_0 + a_1 p + \ldots + a_k p^k) - B p^{k+1}$$

et, *a fortiori*,

$$A \leqq B(p-1)(1 + p + \ldots + p^k) - B p^{k+1}, \qquad \text{c'est-à-dire} \quad A \leqq -B,$$

ce qui est contradictoire.

Les inégalités (5) subsistent donc à partir d'un certain indice k. Comme les A_k sont entiers et que l'algorithme (2) se poursuit indéfiniment, il en résulte aussitôt la périodicité de la suite qui correspond à $\frac{A}{B}$.

Le développement d'un nombre rationnel dans le domaine d'un nombre premier p est toujours unique et bien déterminé; dans le cas de A ou de B divisible par p, l'on pose simplement

$$\frac{A}{B} = \frac{A'}{B'} p^{\alpha},$$

$\frac{A'}{B'}$ représente une fraction dans laquelle ni A' ni B' ne sont divisibles par p. Le développement de $\frac{A'}{B'}$, dans lequel chaque terme séparément se trouve multiplié par p^{α}, est alors celui de $\frac{A}{B}$.

On voit également si A, B, C, ... sont des quantités rationnelles, $\alpha, \beta, \gamma, \ldots$ les développements qui leur correspondent dans le domaine de p, que toujours l'on a

$$A \pm B = \alpha \pm \beta \qquad (p),$$

$$AB = \alpha\beta \qquad (p),$$

$$\frac{A}{B} = \frac{\alpha}{\beta} \qquad (p),$$

où $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ sont les somme, différence, produit et quotient obtenus d'après les règles du n° 4, des deux suites α et β.

D'une manière générale, en désignant par $R(A, B, C, \ldots)$ une fonction rationnelle quelconque à coefficients entiers de A, B, C, ... et par $R(\alpha, \beta, \gamma, \ldots)$ la suite réduite que l'on obtient en effectuant sur α, β, γ, ... les opérations symbolisées par R, l'on aura

$$R(A, B, C, \ldots) = R(\alpha, \beta, \gamma, \ldots) \qquad (p).$$

La division par zéro est, bien entendu, exclue de toutes les considérations ci-dessus.

7. Pour représenter un développement

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots$$

M. Hensel se sert de la notation

$$a_0, a_1 a_2 a_3 \dots .$$

Cette manière d'écrire n'est pas la même que celle que l'on emploie dans un système de numération à base quelconque, mais elle est avantageuse, car les calculs effectués sur des suites de Hensel se font de la même façon que dans le cas de fractions décimales illimitées (1).

Exemple d'*addition :*

Dans le domaine de $p = 5$, on a

$$\begin{array}{l} 6990 = 0,3\,4012 \\ 5661 = 1,2104\,1 \\ \hline 12651 = 1,0114\,04 \end{array} \qquad (5)$$

L'opération se fait exactement comme dans le système de numération de base égale à 5, avec cette seule différence que l'on commence par la gauche au lieu de débuter par la droite.

Exemple de *soustraction :*

$$\begin{array}{l} 3209 = 4,13001 \\ 1137 = 2,2041\,0 \\ \hline 2072 = 2,4213\,0 \end{array} \qquad (5)$$

Lorsque la différence des deux nombres est négative, l'opération se fait de la même manière, mais la suite que l'on obtient se poursuit aussi loin que l'on veut. Exemple :

$$\begin{array}{l} 3209 = 4,13001 \\ 3637 = 2,2040\,1 \\ \hline -428 = 2,4214444444\dots \end{array} \qquad (5)$$

(1) Des exemples, analogues à ceux qui suivent, se trouvent aussi dans le premier paragraphe du Mémoire déjà cité de M. Hensel. *Neue Grundlagen,* etc.

L'opération, telle que nous la représentons ici, équivaut à soustraire de la suite non réduite qui correspond à 3209

$$3209 = 4,130015444444\ldots \qquad (5)$$

la suite qui correspond à 3637.

D'une manière générale, p étant un nombre premier et ρ un exposant entier positif, nul ou négatif quelconque, l'on peut toujours écrire

$$0 = p.p^{\rho} + (p-1)p^{\rho+1} + (p-1)p^{\rho+2} + \ldots. \qquad (p).$$

Pour trouver le développement d'un nombre négatif quelconque, il est avantageux souvent de chercher la suite qui correspond à la même quantité prise positivement et de la soustraire de zéro. Ceci est du reste conforme à la remarque du n° 5.

$$\begin{array}{r} 0 = 5,444444\ldots \\ 428 = 3,023 \\ \hline -428 = 2.421444\ldots \end{array} \qquad (5)$$

Exemple de *multiplication :*

$$\begin{array}{r} 448 = 3,423 \\ 519 = 4,304 \\ \hline 2,3142 \\ 43302 \\ 23142 \\ \hline 232512 = 2,2002442 \end{array} \qquad (5)$$

Exemple de *division :*

Prenons les deux nombres

$$\begin{array}{r} 93316 = 1,3214401 \\ 82 = 2,13 \end{array} \qquad (5)$$

dont le quotient

$$1138 = 3,2041 \qquad (5)$$

est entier.

L'opération se dispose comme suit :

$$\begin{array}{l|l} 1,3214401 & 2,13 \\ 1,441 & \hline 3,2041 \\ \hline 4243401 & \\ 4211 & \\ \hline 32401 & \\ 3032 & \\ \hline 2130 & \\ 213 & \\ \hline \cdots & \end{array} \qquad (5)$$

ce qui s'explique en remarquant, après avoir mis le quotient sous la forme $c_0, c_1 c_2 c_3 c_4$, que, d'une manière abrégée, nous n'avons fait qu'écrire les égalités

$$\begin{array}{ll} 1,3214401 - c_0 & .2,13 = 0,4243401, \\ 0,4243401 - 0,c_1 & .2,13 = 0,0032401, \\ 0,0032401 - 0,0c_2 & .2,13 = 0,0032401, \\ 0,0032401 - 0,00c_3 & .2,13 = 0,0002130, \\ 0,0002130 - 0,000c_4 & .2,13 = 0 \end{array} \qquad (5)$$

qui, additionnées membre à membre, donnent bien

$$1,3214401 - c_0, c_1 c_2 c_3 c_4 . 2,13 = 0 \qquad (5).$$

On voit, par suite, que les quantités c_0, c_1, c_2, c_3 et c_4 sont les entiers égaux à 0, 1, 2, 3 ou 4 qui, respectivement, satisfont aux congruences

$$\begin{array}{ll} 1 \equiv 2c_0 & \\ 4 \equiv 2c_1 & \\ 0 \equiv 2c_2 & \pmod 5. \\ 3 \equiv 2c_3 & \\ 2 \equiv 2c_4 & \end{array}$$

Les règles que nous venons d'exposer en les appliquant à des suites limitées restent les mêmes si celles-ci sont illimitées.

La division d'un nombre par un autre, lorsque le quotient n'est pas entier, se fait comme ci-dessus. C'est d'ailleurs de cette façon qu'on arrivera le plus rapidement au développement d'un nombre rationnel quelconque.

La division de

$$7 = 2,1 \qquad (5)$$

par

$$31 = 1,11 \qquad (5)$$

donne, par exemple, immédiatement

$$\frac{7}{31} = 2,431431431\ldots. \qquad (5)$$

On a, en effet,

$$\begin{array}{l|l} 2,1 = 2,154444444\ldots & 1,11 \\ \underline{\quad 2,22\quad} & \overline{\quad 2,431\ldots\quad} \\ \quad 424444444\ldots & \\ \quad 444 & \\ \hline \quad 34344444\ldots & \\ \quad 333 & \\ \hline \quad 1044444\ldots & \\ \quad 111 & \\ \hline \quad 424444\ldots & \\ \quad \ldots\ldots\ldots & \end{array} \qquad (5)$$

§ 2.

1. Les polynomes que nous rencontrerons le plus souvent dans ce travail seront de la forme

$$P(x) = A_0 x^n + A_1 x^{n-1} + \ldots + A_i x^{n-i} + \ldots + A_n,$$

dans laquelle les coefficients

$$A_i = a_{\rho_i} p^{\rho_i} + a_{\rho_{i+1}} p^{\rho_{i+1}} + \ldots \qquad (i = 0, 1, 2, \ldots, n)$$

sont des suites ordonnées suivant les puissances croissantes de p, rationnelles ou entières dans le domaine de p.

Aux polynomes ainsi définis, nous réservons le nom de *polynomes en x*, tandis que par *polynomes entiers* nous entendrons, au contraire, des polynomes dont les coefficients sont des nombres entiers ou rationnels.

2. Deux polynomes en x, $P(x)$ et $Q(x)$ sont dits *égaux*, ce qui s'écrit

$$P(x) = Q(x) \qquad (p),$$

lorsque, si loin que l'on pousse la comparaison, les coefficients des mêmes puissances de x dans $P(x)$ et $Q(x)$ sont identiques. L'égalité de deux polynomes peut s'exprimer aussi et cela revient au même, par une suite illimitée de congruences prises suivant des puissances entières et successives de p s'étendant aussi loin que l'on veut.

Les opérations d'addition, de soustraction, de multiplication et de division de deux ou plusieurs polynomes en x se font d'après les règles ordinaires du calcul; les combinaisons de coefficients qui en résultent, d'après les principes développés (§ **1**, n° **4**).

L'égalité dans le domaine de p peut avoir lieu également lorsque soit l'un, soit les deux polynomes $P(x)$ et $Q(x)$ sont des polynomes entiers.

3. Un polynome en x, $P(x)$, étant donné, il peut se faire qu'il existe deux polynomes en x : $f(x)$, $g(x)$, de degrés respectivement inférieurs à celui de $P(x)$ et tels que l'on ait

$$P(x) = f(x)\,g(x) \qquad (p).$$

Lorsqu'une pareille décomposition peut se faire, on dit que $P(x)$ est *réductible*, *irréductible* dans le cas contraire. Cette définition qui s'étend naturellement aux polynomes entiers sous-entend les mots *dans le domaine du nombre premier p*.

Un polynome entier réductible au sens usuel l'est aussi dans le domaine de tout nombre premier.

4. Grâce à une remarquable proposition (¹) due à **M. Hensel** on peut toujours, à la suite d'un nombre fini d'essais, reconnaître si un polynome en x est ou non irréductible dans le domaine de p. Il est utile que nous établissions un cas particulier de celle-ci.

Soit

$$P(x) = x^n + A_1 x^{n-1} + \ldots + A_n,$$

un polynome en x dont nous supposons le coefficient de la plus haute puissance de x égal à l'unité et les autres coefficients entiers dans le domaine de p; s'il existe deux polynomes entiers à coefficients entiers $f(x)$ et $g(x)$ dont le résultant n'est pas divisible par p et tels que la congruence

$$P(x) \equiv f(x)\, g(x) \pmod{p} \qquad (1)$$

soit vérifiée, $P(x)$ sera nécessairement réductible dans le domaine de p.

Nous avons, avant d'aborder la démonstration proprement dite de ce théorème, à rappeler certains faits connus.

Étant donnés deux polynomes entiers de degrés égaux respectivement à m et n

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$
$$g(x) = b_0 x^n + b_1 x^{n-1} + \ldots + b_n,$$

dont les coefficients sont des nombres rationnels entiers, on peut toujours trouver deux autres polynomes entiers $f_1(x)$ et $g_1(x)$, de même nature que les précédents, de degrés par rapport à x inférieurs respectivement à m et n et tels que, $R(f, g)$ désignant le résultant de f et g, on ait

$$fg_1 + gf_1 = R(f, g). \qquad (2)$$

Cette égalité est une simple conséquence de la suivante (écrite

(¹) HENSEL, *Neue Grundlagen, etc.*, § 4, p. 78.

pour $m = 3, n = 2$) :

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix} = \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & (a_0x^3 + a_1x^2 + a_2x + a_3)x \\ 0 & a_0 & a_1 & a_2 & (a_0x^3 + a_1x^2 + a_2x + a_3) \\ b_0 & b_1 & b_2 & 0 & (b_0x^2 + b_1x + b_2)x^2 \\ 0 & b_0 & b_1 & b_2 & (b_0x^2 + b_1x + b_2)x \\ 0 & 0 & b_0 & b_1 & (b_0x^2 + b_1x + b_2) \end{vmatrix}$$

dont le premier membre est $R(f, g)$.

De (2) on déduit immédiatement, dans le cas où $R(f, g)$ n'est pas divisible par p, l'existence de deux polynomes u et v à coefficients entiers et de même degré respectivement que g_1 et f_1 et tels que la congruence

$$fu + gv \equiv 1 \pmod{p} \tag{3}$$

soit satisfaite.

Plus généralement comme la non-divisibilité de $R(f, g)$ par p entraîne le même fait pour l'un au moins des deux nombres a_0 et b_0, si W représente un polynome à coefficients entiers, de degré au plus égal à $n + m - 1$, il existera toujours deux autres polynomes U et V, à coefficients égaux à 0, 1, 2, ... ou $(p - 1)$, de degrés respectivement inférieurs à n et m et tels qu'on ait

$$fU + gV \equiv W \pmod{p}. \tag{4}$$

De (3) on déduit en effet

$$f(uW) + g(vW) \equiv W \pmod{p},$$

ou encore, en désignant par X un polynome quelconque,

$$f(uW - gX) + g(vW + fX) \equiv W \pmod{p}. \tag{5}$$

Si maintenant nous admettons, pour fixer les idées, que b_0 n'est pas divisible par p, nous pouvons choisir X de manière à avoir

$$uW - gX \equiv U \pmod{p},$$

où U est l'un des deux polynomes dont nous voulons établir l'existence. Pour V, on prendra le polynome défini par

$$\varphi W + f X \equiv V \qquad (\text{mod } p),$$

polynome qui, à cause de (5) et de l'hypothèse relative à W, sera de degré égal ou inférieur à $(m-1)$.

Ceci dit, revenons à la proposition que nous cherchons à établir.

Dire que $P(x)$ est réductible, c'est dire qu'il existe deux polynomes en x, $Q(x)$ et $R(x)$ tels que

$$P(x) = Q(x)\,R(x) \qquad (p). \tag{6}$$

Admettons en outre, hypothèse dont on établirait facilement la légitimité, mais qui, dans le cas où nous nous trouvons, sera satisfaite d'elle-même, que $Q(x)$ et $R(x)$ sont de même forme que $P(x)$, c'est-à-dire à coefficients entiers dans le domaine de p, ceux des plus hautes puissances de x se réduisant dans ces deux polynomes à l'unité.

De même qu'on peut écrire

$$P(x) = F(x) + p\,F_1(x) + p^2 F_2(x) + p^3 F_3(x) + \dots$$

où les F, F_1, F_2, F_3, ..., sont des polynomes entiers à coefficients égaux à 0, 1, 2, ..., $(p-1)$, le premier de degré égal à n [degré de $P(x)$], les autres de degrés inférieurs, de même on aura

$$\begin{aligned} Q(x) &= f_0(x) + p\,f_1(x) + p^2 f_2(x) + \dots, \\ R(x) &= g_0(x) + p\,g_1(x) + p^2 g_2(x) + \dots; \end{aligned}$$

les f_i et g_i étant de degrés respectivement inférieurs à ceux de f_0 et g_0, mais ayant, comme ces deux polynomes, leurs coefficients égaux à 0, 1, 2, ..., ou $(p-1)$.

Remarquons maintenant que la relation (6) peut être considérée comme équivalente à la suite illimitée de congruences

$$\left\{\begin{aligned} f_0 g_0 &\equiv F && (\text{mod } p), \\ (f_0 + p f_1)(g_0 + p g_1) &\equiv F + p F_1 && (\text{mod } p^2), \\ (f_0 + p f_1 + p^2 f_2)(g_0 + p g_1 + p^2 g_2) &\equiv F + p F_1 + p^2 F_2 && (\text{mod } p^3), \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \end{aligned}\right. \tag{7}$$

Il en résulte aussitôt la possibilité de déterminer les polynomes f_i et g_j de manière que, tout en étant du degré voulu et en ayant leurs coefficients égaux à 0, 1, 2, ... ou $(p-1)$, les congruences (7) soient aussi satisfaites.

Si nous prenons, en effet,

$$f_0 = f, \qquad g_0 = g,$$

la première congruence (7) sera toujours vérifiée.

Pour qu'il en soit de même de la seconde, il suffit, chose toujours possible d'après ce que nous avons rappelé et à cause de l'hypothèse sur le résultant faite dans l'énoncé, qu'on ait

$$f_0 g_1 + g_0 f_1 \equiv h_1 + \mathrm{F}_1 \pmod{p},$$

où h_1 représente le polynome entier, de degré inférieur à n, que définit la congruence

$$\mathrm{F} - f_0 g_0 \equiv p h_1 \pmod{p^2}.$$

Pour que la troisième des congruences (7) ait lieu, il suffit après avoir obtenu le polynome h_2 par le moyen de la relation

$$(\mathrm{F}_0 + p\mathrm{F}_1) - (f_0 + pf_1)(g_0 + pg_1) \equiv p^2 h_2 \pmod{p^3},$$

qu'on ait

$$f_0 g_2 + g_0 f_2 \equiv \mathrm{F}_2 + h_2 \pmod{p}.$$

De même que f_1 et g_1, f_2 et g_2, les autres polynomes f_3 et g_3, f_4 et g_4, etc., se déterminent aisément. Le calcul se poursuit aussi loin qu'on veut.

Le passage de f_i et g_i aux polynomes f_{i+1} et g_{i+1} est d'ailleurs facile. Nous pouvons ici nous dispenser de nous en occuper, d'autant plus qu'un peu plus loin, dans un cas un peu différent, on verra comment il se présente.

$\mathrm{P}(x)$ est donc réductible, ce que nous voulions démontrer.

3. De la notion d'irréductibilité, on passe immédiatement à celle de la décomposition d'un polynome en x en ses facteurs irréductibles.

On démontre, de la même manière qu'en Algèbre élémentaire, la proposition suivante.

Tout polynome irréductible, diviseur d'un produit de plusieurs polynomes, divise au moins l'un d'eux.

De là résulte immédiatement, pour les polynomes en x, l'uniformité de la décomposition en facteurs dans le domaine d'un nombre premier p.

6. Plus loin nous aurons l'occasion de rencontrer des polynomes dont les coefficients seront des suites de même nature que celles considérées jusqu'ici, mais qui, au lieu d'être ordonnées suivant les puissances croissantes de p, le seront suivant les puissances de $p^{\frac{1}{s}}$, où s représente un entier positif quelconque.

Au paragraphe **12**, les coefficients des puissances de $p^{\frac{1}{s}}$ ne seront pas des quantités égales à 0, 1, 2, ... ou $(p-1)$, mais des quantités algébriques appartenant à un corps $\mathrm{R}(\xi)$ dont le discriminant n'est pas divisible par p. $\mathrm{R}(\xi)$ s'obtient par adjonction, aux nombres rationnels, d'une quantité ξ racine d'une équation irréductible à coefficients rationnels $f(x)=0$.

Montrons dans ce cas, qui d'ailleurs comprend les précédents, comment se fonderait l'algorithme d'Euclide.

Les polynomes que nous considérons :

$$\mathrm{P}(x)=\mathrm{A}_0x^n+\mathrm{A}_1x^{n-1}+\ldots+\mathrm{A}_n,$$

ont donc leurs coefficients de la forme

$$\mathrm{A}_i=a_{\rho_i}p^{\frac{\rho_i}{s}}+a_{\rho_{i+1}}p^{\frac{\rho_{i+1}}{s}}+\ldots \qquad (i=1,2,\ldots,n),$$

dans laquelle $a_{\rho_i}, a_{\rho_{i+1}}, \ldots$ sont des quantités de $\mathrm{R}(\xi)$.

Rappelons la définition d'après laquelle une quantité algébrique quelconque ε est entière *par rapport à* p, lorsque les coefficients de l'équation rationnelle de moindre degré, vérifiée par ε, sont tous entiers par rapport a p (1), celui de la plus haute puissance de l'inconnue

(1) Une quantité rationnelle est entière *par rapport à* p lorsque, mise sous forme irréductible, son dénominateur n'est pas divisible par p.

n'étant pas divisible par p. Remarquons aussi que, par extension, on dit que par rapport à p une quantité α est divisible par une autre β, $\beta = p^{\frac{1}{s}}$ par exemple, lorsque le quotient $\frac{\alpha}{\beta}$ est quantité entière par rapport à p, et qu'enfin la divisibilité, ainsi comprise, de $\alpha - \beta$ par $p^{\frac{1}{s}}$ est exprimable par la congruence

$$\alpha \equiv \beta \qquad \left(\bmod p^{\frac{1}{s}}\right).$$

Cela étant, soit r le degré de $f(x) = 0$; dans ce cas, toutes les quantités de $R(\xi)$ sont de la forme

$$u_0 + u_1 \xi + \ldots + u_{r-1} \xi^{r-1},$$

dans laquelle les $u_0, u_1, \ldots, u_{r-1}$ sont des quantités rationnelles.

De la non-divisibilité par p du discriminant de $R(\xi)$ résulte alors, comme on sait, l'impossibilité pour une quantité de $R(\xi)$ d'être, par rapport à p, divisible par p sans qu'il en soit de même des coefficients $u_0, u_1, \ldots, u_{r-1}$ qui lui correspondent. On verrait aussi que la même condition doit être vérifiée pour que la même quantité soit, par rapport à p, divisible algébriquement par $p^{\frac{1}{s}}$ (1).

Une quantité du corps ne peut donc être divisible par $p^{\frac{1}{s}}$ sans l'être par p lui-même. Appelons unités ou plus petits restes, selon le module p, les p^r quantités de $R(\xi)$ pour lesquelles les u_i sont indépendamment les uns des autres égaux à 0, 1, 2, ... ou $p - 1$. L'une de ces quantités, celle pour laquelle tous les u_i sont nuls, n'est, à vrai dire, pas une unité, mais cela n'a aucune importance ici.

Soit maintenant

$$A = \varepsilon_0 + \varepsilon_1 p^{\frac{1}{s}} + \varepsilon_2 p^{\frac{2}{s}} + \ldots$$

une suite dans laquelle tous les coefficients ε_i sont des unités de $R(\xi)$;

(1) Ceci s'établit immédiatement si, désignant par α une quantité de $R(\xi)$ divisible par $p^{\frac{1}{s}}$ et par $S(\alpha)$ la somme de ses conjuguées, on remarque que $S(\alpha)$ est divisible par p, comme conséquence du fait que, quel que soit l'entier positif k, on a toujours $[S(\alpha)]^{p^k} \equiv S(\alpha^{p^k}) \pmod p$.

nous disons qu'il y aura toujours une autre suite, analogue à A, unique, bien déterminée,

$$B = \eta_0 + \eta_1 p^{\frac{1}{s}} + \eta_2 p^{\frac{2}{s}} + \ldots,$$

telle qu'au sens que nous avons toujours donné à de pareilles égalités, on ait

$$AB = 1 \qquad \left(p^{\frac{1}{s}}\right).$$

Si nous supposons ε_0 différent de zéro, la chose est immédiate, car on peut toujours déterminer successivement les unités η_0, η_1, η_2, η_3, ..., de manière à avoir

$$\begin{aligned}
\varepsilon_0 \eta_0 &\equiv 1 \quad \left(\bmod p^{\frac{1}{s}}\right),\\
\left(\varepsilon_0 + \varepsilon_1 p^{\frac{1}{s}}\right)\left(\eta_0 + \eta_1 p^{\frac{1}{s}}\right) &\equiv 1 \quad \left(\bmod p^{\frac{2}{s}}\right),\\
\left(\varepsilon_0 + \varepsilon_1 p^{\frac{1}{s}} + \varepsilon_2 p^{\frac{2}{s}}\right)\left(\eta_0 + \eta_1 p^{\frac{1}{s}} + \eta_2 p^{\frac{2}{s}}\right) &\equiv 1 \quad \left(\bmod p^{\frac{3}{s}}\right),\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\ldots\ldots\ldots\ldots ;
\end{aligned}$$

ou mieux de manière que les congruences suivant $p^{\frac{1}{s}}$ pris comme module, qui se déduisent successivement de celles-ci, soient toujours vérifiées. Si l'on avait, au contraire,

$$A = \varepsilon_0 p^{\frac{\rho}{s}} + \varepsilon_1 p^{\frac{\rho+1}{s}} + \ldots,$$

avec, ε_0 et ρ tous deux différents de zéro, ρ quelconque entier positif ou négatif, on aurait

$$B = \eta_0 p^{\frac{-\rho}{s}} + \eta_1 p^{\frac{-\rho+1}{s}} + \ldots,$$

les unités η_0, η_1, ... étant déterminées comme ci-dessus.

Si l'on avait deux suites A_0 et B_0 on pourrait trouver une troisième suite C_0 telle que

$$B_0 C_0 = A_0 \qquad \left(p^{\frac{1}{s}}\right).$$

Il suffirait pour cela de prendre la suite B'_0 définie par l'égalité

$$B_0 B'_0 = 1 \qquad \left(p^{\frac{1}{s}}\right),$$

puis de la multiplier par A_0. Dans $A_0 B'_0$ les coefficients ne sont en général pas des unités. On transforme alors, par un procédé analogue à celui du paragraphe 1, n° 3, $A_0 B'_0$ en une suite satisfaisant à cette condition. On aboutit ainsi à C_0. C_0 sera la suite réduite *équivalente* à $A_0 B'_0$; C_0 s'obtient facilement grâce à ce que l'on sait de la divisibilité des nombres de $R(\xi)$ par $p^{\frac{1}{s}}$.

Ceci dit, soit A_0 le coefficient de x^n dans le polynome $P(x)$ écrit plus haut, B_0 le coefficient de x^m dans le polynome de même nature

$$Q(x) = B_0 x^m + B_1 x^{m-1} + \ldots + B_m;$$

soit en outre $n \geq m$.

Si nous formons la différence

$$P(x) - C_0 x^{n-m} Q(x),$$

nous obtenons un nouveau polynome en x de degré inférieur ou égal à $n-1$.

Ceci donne le moyen d'obtenir le quotient et le reste, de degré inférieur à celui de $P(x)$, de la division de $P(x)$ par $Q(x)$, et cela quel que soit le coefficient de la plus haute puissance de x dans $Q(x)$. Il est dès lors possible de fonder l'algorithme d'Euclide pour des polynomes de la nature de ceux que nous venons de considérer. Les conséquences qu'on en déduit sont pour ces polynomes identiques à celles que nous avons énoncées au numéro précédent pour des polynomes dont les coefficients sont des suites rationnelles en p.

§ 3.

1. Pour étudier certaines propriétés des polynomes en x, que souvent nous mettrons sous la forme

$$P(x) = \sum A_{\alpha\beta} p^{\alpha} x^{\beta},$$

il est avantageux d'introduire, en correspondance avec chacun d'eux, une représentation géométrique qui n'est autre que celle de Newton pour les polynomes dépendant de deux variables x et y.

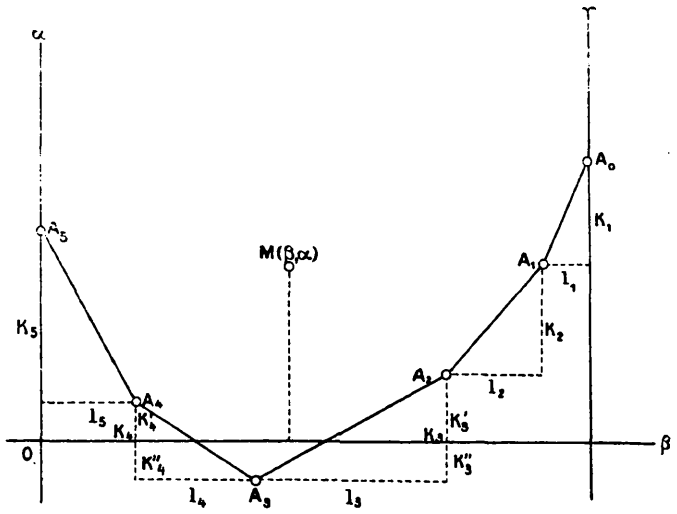
A chaque terme

$$A_{\alpha\beta}\, p^{\alpha} x^{\beta}$$

de $P(x)$ et après avoir choisi dans un plan quelconque deux axes rectangulaires, nous faisons correspondre un point M dit *point représentatif* du terme considéré. L'abscisse et l'ordonnée du point M seront respectivement égales à β et α.

Tous les points correspondant à un polynome $P(x)$ sont situés sur le contour ou au-dessus d'une certaine ligne brisée que nous appellerons *polygone* ou quelquefois *contour* relatif à $P(x)$. Ce polygone s'obtient d'après un procédé connu sur lequel il n'est pas nécessaire de revenir ici (¹). La figure formée par le polygone ainsi défini et par les

Fig. 1.



points situés au-dessus de son contour sera le *diagramme* du polynome considéré.

(¹) *Cf.* par ex. HENSEL et LANDSBERG, *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale*, p. 43 et suivantes.

Au polynome $P(x)$ correspondra, par exemple, le diagramme donné dans la figure 1.

Les points représentatifs d'un quelconque de ses termes seront situés soit sur le contour

$$\gamma A_0 A_1 \dots A_4 A_5 \alpha,$$

soit à son intérieur. La ligne brisée $A_0 A_1 A_2 \dots A_5$ peut se réduire à une droite; dans ce cas nous disons que le contour est *rectiligne; brisé* dans le cas contraire.

2. En fixant sur le polygone un sens de circulation positif lorsqu'on va du point A_0 au point A_5 nous serons à même de donner une définition précise de l'*inclinaison* d'un quelconque des côtés. Ce sera la tangente trigonométrique de l'angle formé par la direction positive du côté avec la direction négative de l'axe des abscisses.

Dans la figure 1, par exemple, les côtés A_1A_2 et A_3A_4 sont d'inclinaisons respectivement égales à

$$-\frac{k_2}{l_2} \quad \text{et} \quad +\frac{k_4}{l_4}.$$

Dans la suite, nous poserons toujours, i désignant un indice quelconque,

$$\frac{k_i}{l_i} = \frac{\lambda_i r_i}{\lambda_i s_i} = \frac{r_i}{s_i},$$

$\frac{r_i}{s_i}$ sera l'expression mise sous forme réduite du rapport $\frac{k_i}{l_i}$. Dans le cas de $k_i = 0$, on aura

$$l_i = \lambda_i, \qquad s_i = 1.$$

3. Nous considérons maintenant les diagrammes qui correspondent à deux polynomes donnés $P(x)$ et $Q(x)$ et nous nous demandons quel sera le polygone relatif à leur produit $P(x)Q(x)$.

Soient $A p^{\alpha} x^{\beta}$, $A' p^{\alpha'} x^{\beta'}$ deux termes quelconques appartenant l'un à $P(x)$, l'autre à $Q(x)$, leur produit est égal à $AA' p^{\alpha+\alpha'} x^{\beta-\beta'}$, de sorte qu'en groupant entre eux tous les produits analogues pour lesquels la somme des exposants de p est égale à $\alpha + \alpha'$, celle des exposants de x

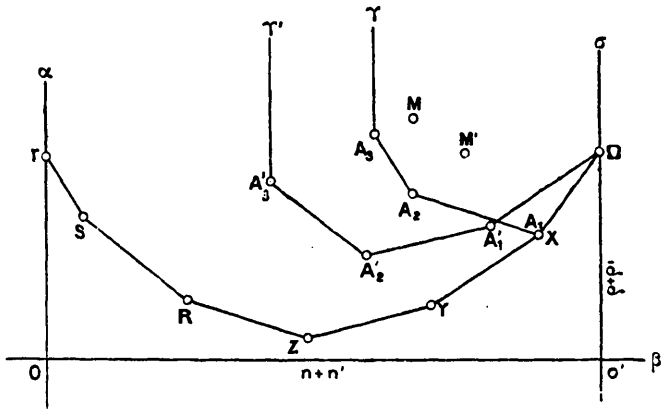
égale à $\beta + \beta'$, on pourra mettre $P(x)\,Q(x)$ sous la forme

$$P(x)\,Q(x) = \Sigma L p^{\alpha+\alpha'} x^{\beta+\beta'}.$$

Le coefficient L peut être divisible par p; il ne le sera pas s'il se réduit au seul produit AA', puisque ni A, ni A' ne sont divisibles par p.

Ceci dit, supposons (*fig.* 2) les diagrammes relatifs à P et Q et au

Fig. 2.



produit PQ, rapportés au même système d'axes de coordonnées β, α. Dans la figure, seul le polygone relatif à PQ se trouve ainsi représenté.

Soit Ω son point initial, c'est-à-dire le point de coordonnées $n+n'$, $\rho+\rho'$, si n et n' sont les degrés respectifs de P et Q, ρ et ρ' les exposants des plus petites puissances de p, facteurs de x^n et $x^{n'}$ dans P et Q.

Déplaçons ensuite les diagrammes relatifs à P et à Q parallèlement à eux-mêmes, de façon que les points initiaux de chacun des polygones viennent se confondre en Ω. Les axes restant parallèles, mais leur origine étant en Ω, les coordonnées du point M transporté, représentatif de $A p^{\alpha} x^{\beta}$, deviendront respectivement $\beta - n$ et $\alpha - \rho$ et celles de M' transporté, représentatif de $A' p^{\alpha'} x^{\beta'}$, égales à $\beta' - n'$ et $\alpha' - \rho'$. Enfin le point qui, dans le diagramme relatif au produit PQ, avait primitivement $\beta + \beta'$ et $\alpha + \alpha'$ comme coordonnées, restera immobile et admettra maintenant $\beta + \beta' - (n + n')$ comme abscisse, $\alpha + \alpha' - (\rho + \rho')$ comme ordonnée. On en déduit que ce point n'est

pas autre chose que l'extrémité de la résultante des vecteurs ΩM et $\Omega M'$ issus de Ω.

Nos trois diagrammes étant donc superposés comme il vient d'être dit, tout point représentatif de PQ se trouve situé sur une parallèle à l'axe des ordonnées, en coïncidence ou au-dessus de l'extrémité de la résultante de deux vecteurs issus de Ω et se terminant respectivement en deux points représentatifs l'un d'un terme de P, l'autre d'un terme de Q.

Soient maintenant deux systèmes de vecteurs (non représentés dans la figure) : le premier composé de ΩA_1, ΩA_2, ΩA_3, ...; le second de $\Omega A'_1$, $\Omega A'_2$, $\Omega A'_3$, ..., et tels que les deux contours $\Omega A_1 A_2 A_3$, $\Omega A'_1 A'_2 A'_3$... soient concaves du côté des ordonnées positives. Trois vecteurs dans chaque système sont suffisants pour fixer les idées.

Supposons ensuite les vecteurs ΩA_1, $A_1 A_2$, $A_2 A_3$; $\Omega A'_1$, $A'_1 A'_2$, $A'_2 A'_3$ limitant les deux contours ci-dessus, transportés parallèlement à eux-mêmes en Ω, puis composés ensemble par ordre des inclinaisons croissantes. On obtient ainsi la ligne brisée $\Omega XYZRST$ qui jouit des propriétés suivantes :

1° Tous ses sommets à l'exception du premier X s'obtiennent et cela d'une seule façon, par addition géométrique de deux vecteurs appartenant l'un au système $\Omega(A_1 A_2 A_3)$, l'autre au système $\Omega(A'_1 A'_2 A'_3)$. Le premier sommet X s'obtient lui aussi d'une manière unique; il n'est autre chose que l'extrémité du vecteur de moindre inclinaison parmi tous les vecteurs des deux systèmes que nous considérons.

2° M et M' étant deux points situés respectivement à l'intérieur ou sur les côtés des deux figures trapézoïdales $\sigma\Omega A_1 A_2 A_3 \gamma$ et $\sigma\Omega A'_1 A'_2 A'_3 \gamma'$, l'extrémité de la résultante des deux vecteurs ΩM et $\Omega M'$ tombera toujours à l'intérieur ou sur les côtés de la troisième figure trapézoïdale $\sigma\Omega XYZRST\alpha$. Cette extrémité ne pourra, en outre, coïncider avec l'un ou l'autre des sommets Ω, X, Y, ... ou T que si M se confond avec l'un des points Ω, A_1, A_2 ou A_3, et M' avec l'un des points Ω, A'_1, A'_2 ou A'_3.

On voit dès lors, à cause de tout ce qui précède, que, si $\Omega A_1 A_2 A_3$ et $\Omega A'_1 A'_2 A'_3$ sont les polygones respectifs de $P(x)$ et $Q(x)$, $\Omega XYZRST$ sera le polygone de leur produit. Nous avons donc la proposition :

Le polygone relatif au produit de deux polynomes $P(x)$ *et* $Q(x)$

s'obtient en transportant parallèlement à eux-mêmes, en un point quelconque, les côtés des polygones de $P(x)$ *et* $Q(x)$ *construits respectivement sur un même système d'axes rectangulaires et en les composant ensuite géométriquement par ordre des inclinaisons croissantes.*

Cette proposition s'étend immédiatement à un nombre quelconque de facteurs. On peut l'énoncer plus brièvement en disant :

Les polygones relatifs à un produit s'obtiennent par composition géométrique, dans l'ordre des inclinaisons croissantes, des côtés des polygones qui correspondent aux facteurs.

4. Les seuls diviseurs à polygone rectiligne AB que peut admettre un polynome $P(x)$ sont ceux pour lesquels AB est de même inclinaison que l'un ou l'autre des côtés du polygone relatif à $P(x)$. C'est là une conséquence immédiate du théorème qui précède.

§ 4.

1. Soit $P(x)$ un polynome en x, d'ailleurs quelconque, dont nous supposons le polygone brisé et que nous écrivons :

$$P(x) = p^{\rho} A'_0 x^n + A_1 x^{n-1} + \ldots + A_n.$$

Les $A_1, A_2, \ldots, A_n$ sont des suites quelconques, A'_0 une suite quelconque également mais dont le premier terme est indépendant de p et ne se réduit pas à zéro.

Nous introduisons un nouveau polynome $Q(x)$, défini par l'égalité

$$P(x) = A'_0 Q(x) \qquad (p),$$

et remarquons que $Q(x)$ et $P(x)$ ont même polygone.

Supposons, pour fixer les idées, ce polygone donné par la figure 1 du paragraphe **3**. On a, dans ce cas,

$$n = l_5 + l_4 + l_3 + l_2 + l_1,$$
$$\rho = k'_3 + k_2 + k_1,$$

et si nous nous rapportons à ce qui a été dit (§ **3**, n° **2**), touchant la signification des lettres k_i, l_i, λ_i, r_i, s_i, nous voyons que, dans $Q(x)$, l'ensemble des termes, dont les points représentatifs sont situés sur les côtés du polygone, peut être représenté respectivement par les expressions qui suivent :

Pour A_0A_1 par

$$x^{l_1+l_2+l_3+l_4}[a_1x^{l_1}p^{k_1}+\ldots+b_1x^{(\lambda_1-j)s_1}p^{(\lambda_1-j)r_1}+\ldots+c_1]p^{k'_3+k_3},$$

pour A_1A_2 par

$$x^{l_2+l_3+l_4}[a_2x^{l_2}p^{k_2}+\ldots+b_2x^{(\lambda_2-j)s_2}p^{(\lambda_2-j)r_2}+\ldots+c_2]p^{k'_3},$$

pour A_2A_3 par

$$x^{l_3+l_4}[a_3x^{l_3}p^{k_3}+\ldots+b_3x^{(\lambda_3-j)s_3}p^{(\lambda_3-j)r_3}+\ldots+c_3]p^{-k''_3},$$

pour A_3A_4 par

$$x^{l_4}[a_4x^{l_4}+\ldots+b_4x^{(\lambda_4-j)s_4}p^{jr_4}+\ldots+c_4p^{k_4}]p^{-k''_4},$$

pour A_4A_5 par

$$[a_5x^{l_5}+\ldots+b_5x^{(\lambda_5-j)s_5}p^{jr_5}+\ldots+c_5p^{k_5}]p^{k'_4}.$$

Dans ces expressions, les coefficients extrêmes a et c sont comme les b égaux à 0, 1, 2, ... ou $p-1$, mais pour eux la valeur zéro est toutefois exclue.

On a, en outre,

$$a_1=1;$$

$$c_1=a_2, \qquad c_2=a_3, \qquad \ldots, \qquad c_4=a_5.$$

Les deux exposants k''_3 et k''_4 sont égaux, nous écrirons

$$-k''_3=-k''_4=+k''.$$

Soit maintenant a_i le coefficient du premier terme dans le polynome entre crochets relatif au $i^{\text{ième}}$ côté, a_3 par exemple pour A_2A_3. Nous

prenons le nombre a'_3 défini par la congruence

$$a_3 a'_3 \equiv 1 \qquad (\mathrm{mod}\, p),$$

et formons l'expresssion

$$f_3(x) = x^{l_3} p^{k_3} + \ldots + b'_3 x^{(\lambda_3 - j)s_3} p^{(\lambda_3 - j)r_3} + \ldots + c'_3,$$

dans laquelle les coefficients $\ldots, b'_3, \ldots, c'_3$ sont les plus petits restes positifs selon le module p des produits $\ldots, a'_3 b_3, \ldots, a'_3 c_3$.

A chaque facteur entre crochets, à chaque côté par conséquent du polygone relatif à $Q(x)$, correspond ainsi un polynome que nous désignerons par $f_i(x)$ et qui, dans la suite, sera toujours représenté par cette notation-là.

Ceci dit, considérons l'expression

$$A'_0 p^{k''} \Pi f_i(x),$$

dans laquelle le produit s'étend à tous les facteurs $f_i(x)$ et où k'' est l'ordonnée du point le plus bas dans le contour relatif à $P(x)$. Construisons le polygone qui lui correspond. On voit, par application du théorème du paragraphe **3** (n° **3**), que ce polynome est identique à celui de $P(x)$, car le polygone relatif à chaque facteur $f_i(x)$ est une droite de même longueur et de même inclinaison que le côté $A_{i-1}A_i$ auquel il se rattache. Si, ensuite, nous comparons, dans $P(x)$ et dans $A'_0 p^{k''} \Pi f_i(x)$, ceux des termes dont les points représentatifs sont situés sur le polygone, nous voyons qu'ils sont identiques (¹).

Nous pouvons donc mettre $P(x)$ sous la forme

$$P(x) = A'_0 p^{k''} \Pi f_i(x) + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta}, \tag{1}$$

dans laquelle le signe Σ s'étend à des termes dont les points représen-

---

(¹) Les coefficients des différentes puissances de x dans $A'_0 p^{k''} \Pi f_i(x)$ ne sont à vrai dire pas tous égaux à 0, 1, 2, ... ou $p-1$; il faut, en conséquence, pour la construction du diagramme relatif à cette expression, commencer par développer chacun des coefficients, d'ailleurs positifs, qu'elle renferme suivant les puissances croissantes de p.

tatifs sont situés *au-dessus* du polygone de $P(x)$ et qui, tous, sont par rapport à x de degré *inférieur* à n, le degré de $P(x)$.

2. Reprenons le même polynome $P(x)$, mais admettons que son contour soit rectiligne. Dans ce cas, par application de la formule précédente, nous pourrons écrire

$$P(x) = A'_0 p^{k''} f(x) + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta} \tag{2}$$

où $f(x)$ représente un polynome de l'un ou l'autre des deux types

$$x^l p^k + \ldots + b x^{(\lambda-j)s} p^{\lambda-j)r} + \ldots + c$$

ou

$$x^l + \ldots + b x^{(\lambda-j)s} p^{jr} + \ldots + c p^k,$$

dans lesquels les coefficients b, c ont la même signification que plus haut.

Bornons-nous à considérer l'une de ces deux expressions et supposons $f(x)$ égal à la seconde d'entre elles,

$$f(x) = x^l + \ldots + b x^{(\lambda-j)s} p^{jr} + \ldots + c p^k.$$

Dans ce polynome, faisons la substitution

$$x^s = t p^r,$$

puis divisons le résultat par p^k.

On obtient alors, puisque $l = \lambda s$, $k = \lambda r$, un nouveau polynome que nous pouvons écrire

$$g(t) = t^{\lambda} + \ldots + b t^{(\lambda-j)} + \ldots + c.$$

Nous admettrons que $g(t)$, décomposé en ses facteurs irréductibles selon le module p, vérifie la congruence

$$g(t) \equiv \Pi [g_i(t)]^{m_i} \pmod{p},$$

dans laquelle

$$g_i(t) = t^{n_i} + \ldots + b_i t^{n_i - j} + \ldots + c_i.$$

Nous pouvons écrire aussi

$$g(t) = \Pi[g_i(t)]^{m_i} + p\,\varphi(t),$$

où $\varphi(t)$ représente un certain polynome de degré inférieur à λ.

Ceci nous conduit à l'égalité

$$f(x) = p^k \Pi\left[g_i\left(\frac{x^s}{p^r}\right)\right]^{m_i} + p^{k+1}\,\varphi\left(\frac{x^s}{p^r}\right),$$

qui, à cause de

$$\Sigma n_i m_i = \lambda$$

et après avoir posé

$$p^{n_i r}\, g_i\left(\frac{x^s}{p^r}\right) = G_i(x),$$

peut s'écrire encore

$$f(x) = \Pi[G_i(x)]^{m_i} + p^{k+1}\,\varphi\left(\frac{x^s}{p^r}\right).$$

Mais un terme quelconque de

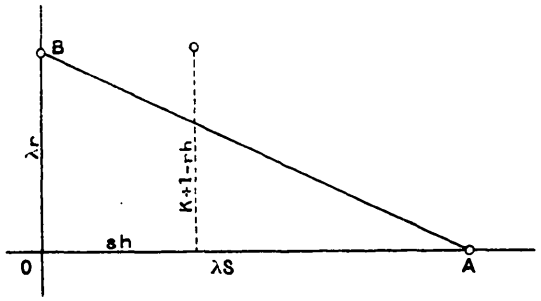
$$p^{k+1}\,\varphi\left(\frac{x^s}{p^r}\right)$$

sera de la forme

$$p^{k+1} A \left(\frac{x^s}{p^r}\right)^h,$$

où $h < \lambda$ et où A est un entier qui peut être divisible par p. Si nous nous reportons (*fig.* 3) au diagramme correspondant à $f(x)$, nous

Fig. 3.



voyons que le point représentatif du terme ci-dessus admet comme abscisse la longueur *sh*, comme ordonnée une quantité égale ou supé-

rieure à $k+1-rh$. Comme on a

$$\frac{k+1-rh}{(\lambda-h)s}=\frac{(\lambda-h)r+1}{(\lambda-h)s}=\frac{r}{s}+\frac{1}{(\lambda-h)s}>\frac{r}{s},$$

le point considéré se trouve au-dessus de AB.

Les polynomes $G_i(x)$ ont, d'autre part, tous leurs coefficients entiers; leurs contours relativement à p sont rectilignes et de même inclinaison que AB.

Dès lors nous pouvons écrire, tenant compte de (2),

$$(3)\qquad P(x)=A_0' p^{k''}\Pi[G_i(x)]^{m_i}+\Sigma A_{\alpha\beta}p^{\alpha}x^{\beta}.$$

La somme Σ figurant ici dans le second membre ne porte pas sur les mêmes termes exactement que le même signe dans (2). Tout point représentatif d'un terme quelconque $A_{\alpha\beta}p^{\alpha}x^{\beta}$ est cependant situé *au-dessus* de la droite qui ici correspond à $P(x)$ et l'exposant β est toujours *au plus* égal à $(n-1)$.

Les lettres A_0' et k'' ont même signification que pour le polynome $P(x)$ du n° **1**. Si nous avions supposé $f(x)$ égal au premier des deux types signalés de polynomes, nous serions arrivé, par un raisonnement tout à fait analogue au même résultat.

3. Par combinaison, enfin, des formules (1) et (3) et en représentant les polynomes $G_i(x)$ par la notation $f_{ij}(x)$ dont le but est de rappeler que $f_{ij}(x)$ se déduit de $f_i(x)$ de la même façon que $G_i(x)$ de $f(x)$, nous avons la formule plus générale

$$(4)\qquad P(x)=A_0' p^{k''}\Pi[f_{ij}(x)]^{m_i}+\Sigma A_{\alpha\beta}p^{\alpha}x^{\beta},$$

dans laquelle $P(x)$ est un polynome de la forme considérée au début de ce paragraphe. Sous le signe Σ ne figurent que des termes dont le degré par rapport à x est *au plus* égal à $n-1$ et dont les points représentatifs dans le diagramme de $P(x)$ se trouvent tous *au-dessus* du polygone.

Dernière remarque. — Les facteurs des produits dans les seconds membres de (1), (3) et (4) sont déterminés d'une manière unique.

Cela comme conséquence des propositions qui seront établies (§ 5 et 7).

§ 5.

1. *Tout polynome en x, $P(x)$, à coefficients ordonnés suivant les puissances entières et croissantes de p, dont le polygone n'est pas rectiligne, est nécessairement réductible. A l'un quelconque des côtés du polygone, $A_{i-1}A_i$ par exemple, correspond un diviseur de $P(x)$ dont le polygone se réduit à une droite de même longueur et de même inclinaison que $A_{i-1}A_i$.*

$P(x)$ est un polynome en x quelconque satisfaisant aux conditions de l'énoncé ; nous mettons le coefficient de sa plus haute puissance sous la forme $p^{\rho}A'_0$, A'_0 étant une suite de puissances de p, entière par rapport à p. Le premier terme de A'_0 est indépendant de p. Après multiplication de $P(x)$ par la suite $\frac{1}{A'_0}$ et après réduction des coefficients, nous obtenons un nouveau polynome $Q(x)$. $P(x)$ et $Q(x)$ admettent des polygones identiques et, si le théorème que nous avons à établir l'est pour $Q(x)$, il le sera *ipso facto* pour $P(x)$.

Nous écrivons

$$Q(x) = p^{\rho}x^n + A_1 x^{n-1} + \ldots + A_n$$

et admettons que le polynome de $Q(x)$, respectivement $P(x)$, est celui de la figure 4 (p. 229).

Nous avons par suite, d'après la formule (1) (§ 4, n° 1),

$$Q(x) = p^{k''}\Pi f_i(x) + \Sigma A_{\alpha\beta}p^{\alpha}x^{\beta}. \tag{1}$$

La possibilité d'une décomposition en facteurs s'établira relativement au troisième côté, mais la démonstration est générale et se rapporterait à n'importe lequel.

2. Soit

$$\frac{k_3}{l_3} = \frac{k}{l} = \frac{\lambda r}{\lambda s} = \frac{r}{s}$$

l'inclinaison, prise négativement, du troisième côté du polygone.

Parallèlement à ce troisième côté, à A_2A_3 (*fig.* 4), supposons tracées toutes les droites passant par les points à cotes entières. La distance de deux consécutives comptée, sur l'axe des ordonnées, est égale à $\frac{1}{s}$. En effet, β, α et β', α' étant les coordonnées respectives de deux points à cotes entières, la distance de deux parallèles à A_2A_3 menées par ces points est égale à la valeur absolue de

$$(\alpha' - \alpha) + (\beta' - \beta)\frac{r}{s}.$$

Mais r et s sont premiers entre eux et il est ainsi possible de déterminer quatre quantités α', α, β', β telles que l'expression ci-dessus soit égale à $\frac{1}{s}$.

3. A_2A_3, prolongé de part et d'autre, nous donne la droite $\Omega\gamma$ rencontrant $O\alpha$ au point Ω. La parallèle à $\Omega\gamma$ menée par le point représentatif M de coordonnées β et α, rencontre $O\alpha$ en m. Si nous rapportons M aux droites $\Omega\alpha$ et $\Omega\gamma$ que nous prenons comme nouveau système d'axes, nous avons mM comme abscisse et Ωm comme ordonnée, nouvelles de M. Un changement d'unités permet d'écrire $m\mathrm{M} = \beta$, tandis qu'on a, γ_1 désignant un entier positif, $\Omega m = \frac{\gamma_1}{s}$.

La figure montre que l'on a

$$Om - O\Omega = \Omega m,$$

c'est-à-dire

$$\alpha - \beta\frac{r}{s} - \left[k' - (l_4 + l_5 + \ldots + l_8)\frac{r}{s}\right] = \frac{\gamma_1}{s}. \tag{2}$$

4. Ceci dit, faisons dans $Q(x)$ la substitution

$$x = yp^{-\frac{r}{s}}, \tag{3}$$

et voyons ce que l'on obtient, lorsqu'on forme l'expression

$$Q\left(y, p^{\frac{1}{s}}\right) = p^{-\left[k' - (l_4 + \ldots + l_8)\frac{r}{s}\right]} Q\left(yp^{-\frac{r}{s}}\right).$$

Un terme quelconque de $Q(x)$ étant $A_{\alpha\beta}p^{\alpha}x^{\beta}$, celui qui lui correspond dans $Q\left(y, p^{\frac{1}{s}}\right)$, à cause de (2), sera $A_{\alpha\beta}p^{\frac{\eta}{s}}y^{\beta}$.

Il en résulte qu'avec les conventions du n° 3, nous pouvons considérer $A_0A_1\ldots A_8$ comme polygone de $Q\left(y, p^{\frac{1}{s}}\right)$ (1).

La formule (1) se transforme et devient

$$Q\left(y, p^{\frac{1}{s}}\right) = \Pi g_i\left(y, p^{\frac{1}{s}}\right) + \Sigma A_{\alpha\beta}p^{\frac{\eta}{s}}y^{\beta}. \tag{4}$$

Les $g_i\left(y, p^{\frac{1}{s}}\right)$ sont égaux respectivement à un facteur, puissance positive ou négative de $p^{\frac{1}{s}}$, près aux $f_i(x)$ transformés par (3). Tous les termes auxquels se rapporte Σ ont leurs points représentatifs situés à l'intérieur du polygone. Sous le signe Σ, par conséquent, tous les exposants η_i sont positifs et différents de zéro, les exposants β égaux au plus à $n-1$.

La figure nous dit elle-même ce que sont les facteurs $g_i\left(y, p^{\frac{1}{s}}\right)$. Pour les côtés d'un rang supérieur au troisième, pour le sixième, par exemple, on a

$$g_6\left(y, p^{\frac{1}{s}}\right) = y^{\lambda_6 s_6} + \ldots + b_6 p^{j\frac{\tau}{s}} y^{(\lambda_6 - j)s_6} + \ldots + c_6 p^{\lambda_6 \frac{\tau}{s}},$$

pour les côtés d'un rang inférieur au troisième, pour le second, par exemple, on a

$$g_2\left(y, p^{\frac{1}{s}}\right) = p^{\lambda_2 \frac{\tau}{s}} y^{\lambda_2 s_2} + \ldots + b_2 p^{(\lambda_2 - j)\frac{\tau}{s}} y^{(\lambda_2 - j)s_2} + \ldots + c_2,$$

---

(1) Les coefficients des polynomes tels que $Q\left(y, p^{\frac{1}{s}}\right)$ sont des suites ordonnées suivant les puissances croissantes de $p^{\frac{1}{s}}$. Il est à peine nécessaire de remarquer que tous les résultats du § 3 sont encore vrais pour ces polynomes-là. Leurs polygones s'obtiennent de la même façon que ceux du § 3; les ordonnées des points représentatifs sont, en particulier, les exposants fractionnaires de p. Ce ne sont pas ici, comme on pourrait s'y attendre, les exposants entiers de $p^{\frac{1}{s}}$.

pour le troisième enfin,

$$g_3\left(y, p^{\frac{1}{s}}\right) = g(y) = y^{\tau s} + \ldots + b y^{(\lambda-1)s} + \ldots + c.$$

Dans ces expressions τ désigne un certain entier positif. Les coefficients b et c sont égaux à 0, 1, 2, ... ou $p-1$; les b peuvent s'annuler, mais les c sont toujours différents de zéro.

5. Le résultant d'un quelconque des polynomes $g_i\left(y, p^{\frac{1}{s}}\right)$, $i \neq 3$, et de $g_3(y) = g(y)$ n'est divisible par aucune puissance de p. Un tel résultant peut être envisagé comme un polynome entier en $p^{\frac{1}{s}}$ admettant un terme indépendant de p. Pour $i = 6$, ce terme indépendant se réduit à $c^{\lambda_6 s_6}$, pour $i = 2$ à $c_2^{\lambda_2 s}$.

6. Posons (1)

$$\prod_{i \neq 3} g_i\left(y, p^{\frac{1}{s}}\right) = \mathrm{G}\left(y, p^{\frac{1}{s}}\right),$$

$$g_3\left(y, p^{\frac{1}{s}}\right) = \mathrm{H}(y),$$

et démontrons qu'il est toujours possible de décomposer, dans le domaine de $p^{\frac{1}{s}}$, $\mathrm{Q}\left(y, p^{\frac{1}{s}}\right)$ en un produit de deux facteurs. On aura

$$\mathrm{Q}\left(y, p^{\frac{1}{s}}\right) = \mathcal{G}'\left(y, p^{\frac{1}{s}}\right) \mathcal{H}'\left(y, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right), \tag{5}$$

où

$$\mathcal{G}'\left(y, p^{\frac{1}{s}}\right) = \mathrm{G}\left(y, p^{\frac{1}{s}}\right) + \Sigma \mathrm{A}_{\alpha\beta} p^{\frac{\alpha}{s}} y^{\beta},$$

$$\mathcal{H}'\left(y, p^{\frac{1}{s}}\right) = \mathrm{H}(y) + \Sigma \mathrm{A}_{\alpha\beta} p^{\frac{\alpha}{s}} y^{\beta}.$$

Les exposants α dans les deux sommes Σ, d'ailleurs distinctes, sont tous positifs et différents de zéro.

Remarquons d'abord que le résultant de H et G se réduit, (n° **5**),

(1) Toute la démonstration du n° 6 est à rapprocher de celle du § 2, n° 4.

à un polynome entier en $p^{\frac{1}{s}}$, dont le terme indépendant est un entier non divisible par p. Puis convenons, en vue de ce qui va suivre, que toutes les lettres H_i et G_i, affectées d'un indice quelconque, représenteront des polynomes entiers en y dont les coefficients seront eux-mêmes des polynomes entiers en $p^{\frac{1}{s}}$. Les polynomes H_i seront tous de degré inférieur à celui de H, les polynomes G_i de degré inférieur à celui de G.

Ayant maintenant, à cause de (4),

$$Q\left(y, p^{\frac{1}{s}}\right) \equiv HG \qquad \left(\mathrm{mod}\, p^{\frac{1}{s}}\right),$$

nous n'avons, pour établir la décomposition possible de $Q\left(y, p^{\frac{1}{s}}\right)$, qu'à montrer qu'on peut toujours, en supposant $\alpha \geq 1$, passer de la congruence

$$(6) \qquad Q\left(y, p^{\frac{1}{s}}\right) \equiv H'G' \qquad \left(\mathrm{mod}\, p^{\frac{\alpha}{s}}\right),$$

où

$$H' = H + p^{\frac{1}{s}}H_1 + p^{\frac{2}{s}}H_2 + \ldots + p^{\frac{\alpha-1}{s}}H_{\alpha-1},$$
$$G' = G + p^{\frac{1}{s}}G_1 + p^{\frac{2}{s}}G_2 + \ldots + p^{\frac{\alpha-1}{s}}G_{\alpha-1},$$

à la suivante

$$(7) \quad Q\left(y, p^{\frac{1}{s}}\right) \equiv \left(H' + p^{\frac{\alpha}{s}}H_\alpha\right)\left(G' + p^{\frac{\alpha}{s}}G_\alpha\right) \qquad \left(\mathrm{mod}\, p^{\frac{\alpha+1}{s}}\right).$$

Or, de (6), découle l'existence d'un polynome entier $L(y)$, de degré inférieur à celui de Q, à coefficients entiers, et qui vérifie la congruence

$$Q\left(y, p^{\frac{1}{s}}\right) - H'G' \equiv p^{\frac{\alpha}{s}}L(y) \qquad \left(\mathrm{mod}\, p^{\frac{\alpha+1}{s}}\right),$$

de sorte que (7) aura lieu si l'on peut trouver deux polynomes H_α et G_α de manière à avoir

$$L \equiv H'G_\alpha + G'H_\alpha \qquad \left(\mathrm{mod}\, p^{\frac{1}{s}}\right).$$

Ces derniers existent effectivement ainsi que le montreraient des considérations semblables à celles du paragraphe **2**, n° **4**, puisque le terme indépendant de $p^{\frac{1}{s}}$, dans le résultant de H′ et G′, identique au terme analogue du résultant de H et G, n'est pas divisible par p.

La formule (5) est ainsi démontrée. La forme même du facteur $\mathfrak{H}'\left(y, p^{\frac{1}{s}}\right)$ nous montre que ce polynome admet, comme polygone, une droite de même longueur et de même inclinaison que A_2A_3. Il en résulte aussitôt, en tenant compte du théorème, paragraphe **3** (n° **3**), relatif à la composition des polygones, que celui de $\mathcal{G}'\left(y, p^{\frac{1}{s}}\right)$ sera la ligne brisée $A'_0A'_1A_3A_4\ldots A_8$ dans laquelle les segments $A'_0A'_1$ et A'_1A_3 sont respectivement égaux et parallèles à A_0A_1 et A_1A_2.

7. Dans les deux expressions

$$\mathfrak{H}'\left(y, p^{\frac{1}{s}}\right) \quad \text{et} \quad p^{\left[k'-(l_4+\ldots+l_8)\frac{r}{s}\right]}\mathcal{G}'\left(y, p^{\frac{1}{s}}\right),$$

faisons la substitution inverse de (3),

$$y = xp^{\frac{r}{s}}.$$

Ceci conduit à deux nouveaux polynomes

$$\mathfrak{H}\left(x, p^{\frac{1}{s}}\right) \quad \text{et} \quad \mathcal{G}\left(x, p^{\frac{1}{s}}\right)$$

dont les coefficients sont des suites ordonnées suivant les puissances croissantes de $p^{\frac{1}{s}}$.

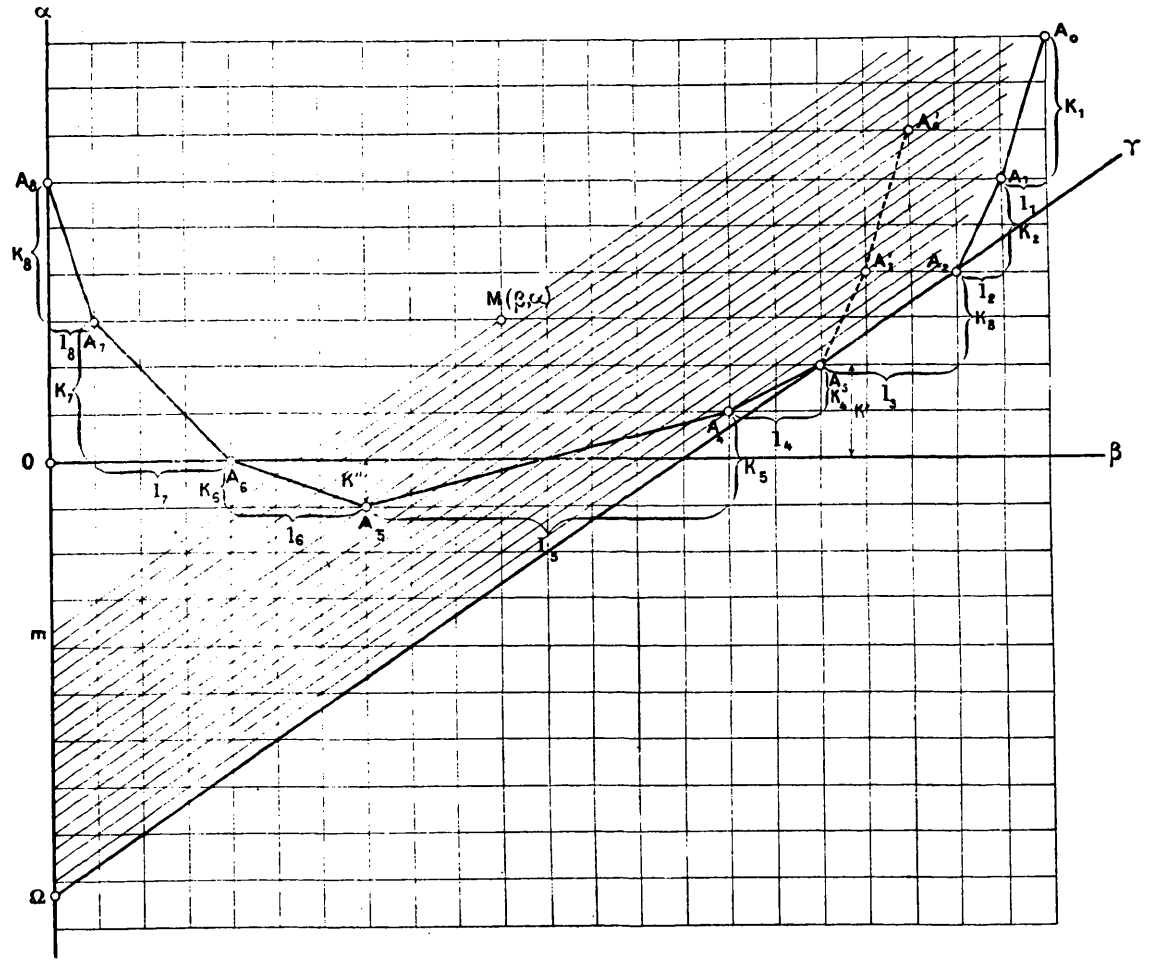
Nous pouvons, relativement à deux axes rectangulaires, construire leurs diagrammes respectifs en convenant de considérer comme point représentatif d'un terme quelconque $A_{\alpha\beta}p^{\frac{\alpha}{s}}x^{\beta}$ le point d'abscisse et d'ordonnée respectivement égales à β et à $\frac{\alpha}{s}$.

Si, pour la construction du diagramme de $\mathcal{G}\left(x, p^{\frac{1}{s}}\right)$ nous nous servons des axes $\beta O\alpha$ de la figure 4, nous obtenons comme polygone de $\mathcal{G}$ la ligne $A'_0A'_1A_3\ldots A_8$.

Le polygone de $\mathfrak{R}$ rapporté à d'autres axes rectangulaires se réduit à une droite de même inclinaison et de même longueur que A_2A_3 dans la figure 4.

Il nous est donc possible d'affirmer, paragraphe **3**, n° **4**, que

Fig. 4.



$\mathfrak{R}\left(x,\ p^{\frac{1}{s}}\right)$ et $\mathfrak{S}\left(x, p^{\frac{1}{s}}\right)$ n'ont aucun diviseur commun dans le domaine de $p^{\frac{1}{s}}$.

Si, d'autre part, au début de toutes nos considérations nous avions,

au lieu de (3), fait la substitution

$$x = y\omega^{-r}p^{-\frac{r}{s}}$$

dans laquelle ω représente une racine $s^{\text{ième}}$ primitive de l'unité, nous aurions obtenu la relation

$$Q(x) = \mathfrak{H}\left(x, \omega p^{\frac{1}{s}}\right)\mathfrak{G}\left(x, \omega p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right),$$

à la place de celle que nous avons ici et qui résulte de tout ce qui précède,

$$Q(x) = \mathfrak{H}\left(x, p^{\frac{1}{s}}\right)\mathfrak{G}\left(x, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right).$$

Comme $\mathfrak{H}\left(x, \omega p^{\frac{1}{s}}\right)$ et $\mathfrak{G}\left(x, \omega p^{\frac{1}{s}}\right)$, ainsi que le montreraient leurs polygones, n'ont pas de diviseurs communs et qu'il en est de même de $\mathfrak{H}\left(x, p^{\frac{1}{s}}\right)$ et $\mathfrak{G}\left(x, \omega p^{\frac{1}{s}}\right)$, nous avons nécessairement, puisque la décomposition de $Q(x)$ en facteurs irréductibles, dans le domaine de $p^{\frac{1}{s}}$, se fait d'une manière uniforme,

$$\mathfrak{H}\left(x, p^{\frac{1}{s}}\right) = \mathfrak{H}\left(x, \omega p^{\frac{1}{s}}\right),$$
$$\mathfrak{G}\left(x, p^{\frac{1}{s}}\right) = \mathfrak{G}\left(x, \omega p^{\frac{1}{s}}\right).$$

Les coefficients dans $\mathfrak{H}\left(x, p^{\frac{1}{s}}\right)$ et $\mathfrak{G}\left(x, p^{\frac{1}{s}}\right)$, que maintenant nous pouvons désigner par $\mathfrak{H}(x)$ et $\mathfrak{G}(x)$, ne dépendent donc pas de $p^{\frac{1}{s}}$ mais de p uniquement.

Nous avons donc

$$Q(x) = \mathfrak{H}(x)\mathfrak{G}(x) \qquad (p).$$

Le polygone de $\mathfrak{H}(x)$ est rectiligne, il se réduit à un segment de même longueur et de même inclinaison que le segment A_2A_3 de la figure 4. La proposition du début de ce paragraphe se trouve ainsi complètement établie.

8. Si, enfin, nous désignons par $P_i(x)$ le diviseur de $Q(x)$ se

rattachant au $i^{ième}$ côté du polygone, $\mathfrak{R}(x)$, par exemple, par $P_3(x)$, nous avons immédiatement :

$$Q(x) = p^{k''} \Pi P_i(x) \qquad (p).$$

Le produit du second membre s'étend à tous les diviseurs $P_i(x)$ de $Q(x)$. k'' représente l'ordonnée, prise avec son signe, du point le plus bas du polygone. On a d'autre part

$$P(x) = A'_0 Q(x) \qquad (p),$$

et, par conséquent, la formule

$$P(x) = p^{k''} A'_0 \Pi P_i(x) \qquad (p), \tag{8}$$

dans laquelle chaque facteur $P_i(x)$ se déduit de $P(x)$ par l'intermédiaire de $Q(x)$.

§ 6.

Considérons le polynome en x

$$P(x) = x^n + A_1 x^{n-1} + A_2 x^{n-2} + \ldots + A_n,$$

dans lequel nous supposerons les coefficients à caractère entier par rapport à p. Si l'on a

$$A_i = a_i p^{\rho_i} + a_{i+1} p^{\rho_i+1} + \ldots \qquad (i = 1, 2, \ldots, n),$$

on aura, par conséquent,

$$\rho_i \geq 0.$$

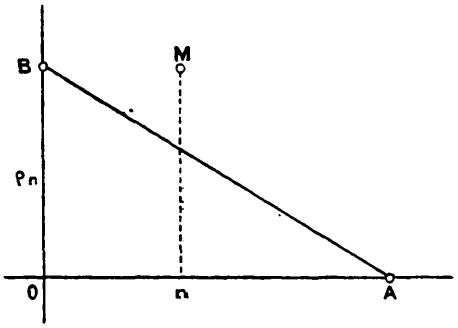
Supposons que $P(x)$ soit irréductible dans le domaine de p. Dans ce cas son polygone se réduit (*fig.* 5) à une droite AB d'inclinaison égale à $\frac{\rho_n}{n}$.

Tout point M représentatif d'un terme de $P(x)$ est alors situé soit

sur AB, soit au-dessus. Le polygone de $P(x)$ conduit ainsi aux inégalités

$$\frac{\rho_i}{i} \geq \frac{\rho_n}{n},$$

Fig. 5.



pour $i = 1, 2, \ldots, (n-1)$. Ce fait important constitue, dans les recherches de M. Hensel, un théorème fondamental (¹).

§ 7.

1. Prenons un polynome quelconque $P(x)$ de degré l dont le polygone soit rectiligne et désignons, comme au paragraphe 3, n° **1**, par $A'_0 p^{\rho}$ le coefficient de la plus haute puissance de x, tandis que k'' sera l'ordonnée du point le plus bas du polygone de $P(x)$.

Nous pouvons alors écrire, après introduction de $Q(x)$,

$$P(x) = p^{k''} A'_0 Q(x). \tag{1}$$

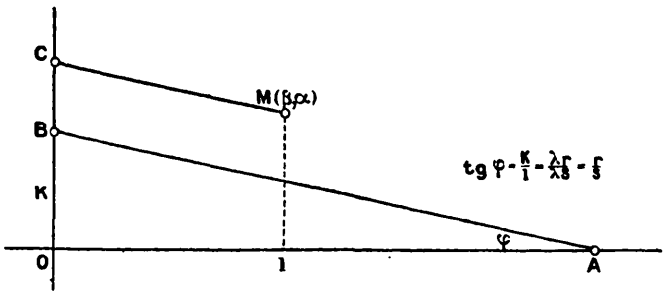
Supposons positive l'inclinaison de la droite qui correspond à $P(x)$; si celle-ci était d'inclinaison négative rien ne serait changé à notre analyse, le résultat auquel nous aboutirons étant d'ailleurs indépendant de cette hypothèse.

$Q(x)$ est alors un polynome en x dont le coefficient de la plus haute puissance de x est l'unité. Son polygone est rectiligne, c'est un segment de droite de même longueur et même inclinaison que celui

(¹) Hensel, *Ueber eine neue Begründung*, etc. (milieu de la page 15).

qui correspond à $P(x)$. Dans la figure 6 nous l'avons représenté par AB.

Fig. 6.



Ceci dit, $Q(x)$, par application de la formule (3) du paragraphe **4**, n° **2**, peut, dans l'hypothèse où nous nous plaçons, être mis sous la forme

$$Q(x) = \Pi[G_i(x)]^{m_i} + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta}, \tag{2}$$

dans laquelle les facteurs $G_i(x)$ égaux à des expressions telles que

$$x^{\lambda_i s} + \ldots + b_i x^{(\lambda_i - j)s} p^{jr} + \ldots + c_i p^{\lambda_i r}$$

se déduisent du polynome entier

$$f(x) = x^l + \ldots + b x^{(\lambda - j)s} p^{jr} + \ldots + c p^k.$$

Certains termes de $Q(x)$ ont leurs points représentatifs sur AB. Leur ensemble constitue le polynome $f(x)$; on a de plus

$$\Sigma \lambda_i m_i = \lambda.$$

Si nous posons

$$x = y p^{\frac{r}{s}}, \tag{3}$$

les $G_i(x)$ se transforment et deviennent

$$p^{\lambda_i r}(y^{\lambda_i s} + \ldots + b_i y^{(\lambda_i - j)s} + \ldots + c_i) = p^{\lambda_i r} g_i(y^s),$$

tandis que de (2), on passe à la nouvelle égalité

$$Q\left(y p^{\frac{r}{s}}\right) = p^{\lambda r} S\left(y, p^{\frac{1}{s}}\right)$$

dans laquelle

$$(4) \qquad S\left(y,\ p^{\frac{1}{s}}\right) = \Pi[g_i(y^s)]^{m_i} + \Sigma A_{\alpha\beta}\, p^{\frac{\alpha}{s}} y^{\beta}.$$

Sous le signe Σ, dans le second membre de (4), on ne rencontre que des exposants α positifs et différents de zéro. Dans (2), en effet, un terme quelconque de Σ (*fig.* 6) a son point représentatif M au-dessus de AB; son exposant, par conséquent, vérifie l'inégalité

$$\alpha s + \beta r > \lambda r.$$

Reportons-nous ensuite au paragraphe **4**, n° **2**, auquel sont empruntées la plupart des notations dont nous nous servons ici. Les polynomes $g_i(y^s)$ sont en y^s ceux que nous avons appelés $g_i(t)$ de sorte qu'il suffit de remplacer dans les premiers y^s par t pour obtenir les seconds.

Le résultant de deux quelconques des polynomes $g_i(y^s)$ est en conséquence égal à la $s^{\text{ième}}$ puissance du résultant des deux polynomes $g_i(t)$ de mêmes indices et ne peut, de ce fait, être divisible par p, puisque deux expressions $g_i(t)$ n'admettent aucun diviseur commun selon le module p.

On en déduit aussitôt, comme au paragraphe **3**, n° **6**, la possibilité de décomposer $S\left(y,\ p^{\frac{1}{s}}\right)$, dans le domaine de $p^{\frac{1}{s}}$, en un produit de facteurs de la forme

$$[g_i(y^s)]^{m_i} + \Sigma A_{\alpha\beta} p^{\alpha} y^{\beta},$$

d'où nous tirons, dans le domaine de p et par une marche analogue à celle du paragraphe **3**, n° **7**, les diviseurs $R_i(x)$ de $Q(x)$,

$$(5) \qquad R_i(x) = [G_i(x)]^{m_i} + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta}.$$

Ici, comme toujours, dans le second membre de (5), le signe Σ s'étend à des termes dont les points représentatifs sont situés au-dessus de la droite constituant le polygone de $R_i(x)$ et qui s'obtient par la considération seule de $[G_i(x)]^{m_i}$.

Le produit, enfin, des différents facteurs $R_i(x)$ est égal à $Q(x)$.

Nous pouvons donc écrire, à cause de (1), et quelle que soit l'inclinaison du contour rectiligne qui correspond à $P(x)$,

$$P(x) = p^{k''} A'_0 \Pi R_i(x) \qquad (p). \tag{6}$$

2. Chaque facteur $P_i(x)$, dans le second membre de la formule (8) du paragraphe **5**, admet un polygone rectiligne. Chacun d'eux est donc décomposable en un produit de facteurs analogues aux polynomes $R_i(x)$. Si donc nous désignons par $P_{ij}(x)$ ces diviseurs des $P_i(x)$, la formule (8) du paragraphe **5** se transformera. Par application de (6) et en remarquant que pour chacun des $P_i(x)$, $k'' = 0$, $A'_0 = 1$, on obtient

$$P(x) = p^{k''} A'_0 \Pi P_{ij}(x) \qquad (p). \tag{7}$$

Le produit s'étend à tous les polynomes $P_{ij}(x)$, diviseurs des $P_i(x)$, diviseurs eux-mêmes de $P(x)$.

Cette relation (7) comprend la formule (6) comme cas particulier. Le polygone de $P(x)$, par conséquent, peut être quelconque. k'' est l'ordonnée de son point le plus bas. A'_0 s'obtient de la manière indiquée au début du paragraphe **5**.

Chaque facteur $P_{ij}(x)$, est de l'une des deux formes,

$$(x^{\lambda s} + \ldots + b x^{(\lambda - j)s} p^{jr} + \ldots + c p^{\lambda r})^m + \Sigma A_{\alpha\beta} p^\alpha x^\beta$$

ou

$$(x^{\lambda s} p^{\lambda r} + \ldots + b x^{(\lambda - j)s} p^{(\lambda - j)r} + \ldots + c)^m + \Sigma A_{\alpha\beta} p^\alpha x^\beta,$$

suivant que l'inclinaison du côté auquel il se rattache est positive ou négative. Dans le cas de $m = 1$, le polynome $P_{ij}(x)$ correspondant est irréductible dans le domaine de p, ce qui n'a pas lieu nécessairement lorsque m est supérieur à l'unité.

DEUXIÈME PARTIE.

§ 8.

1. Soit

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

un polynome à coefficients *rationnels* quelconques; par polynome *équivalent à* $f(x)$, *dans le domaine du nombre premier* p, nous entendons le polynome en x, que l'on obtient en remplaçant, dans $f(x)$, chaque coefficient a_i par son développement suivant les puissances entières et croissantes de p. Ceux-ci s'obtiennent d'après les méthodes exposées dans notre premier paragraphe (§ **1**, n° **7** spécialement).

Si $F(x)$ est, dans le domaine de p, le polynome équivalent à $f(x)$, on aura

$$f(x) = F(x) \qquad (p), \tag{1}$$

et les diviseurs de $F(x)$ seront dits, par extension, *diviseurs de* $f(x)$ *dans le domaine de* p. Le diagramme correspondant à $F(x)$ et, dans celui-ci, le polygone, seront désignés également, comme diagramme et polygone de $f(x)$, relativement à p (¹).

2. Tout diviseur, au sens usuel, de $f(x)$ est égal dans le domaine

(¹) Dans toutes ces définitions, nous avons fait intervenir le polynome $F(x)$, équivalent à $f(x)$. Ceci paraît conforme à la nature des choses. S'il ne s'agit d'obtenir que le polygone relatif à $f(x)$, on peut procéder de la manière suivante : Ax^β représentant un terme quelconque de $f(x)$, on prend la puissance entière p^α de p, diviseur exact de A, *par rapport à* p. Le point, d'abscisse β et d'ordonnée α, est alors représentatif de Ax^β. Ces points une fois construits, le polygone se forme de la même manière que pour un polynome en x.

de p, au produit de certains diviseurs irréductibles de $F(x)$. Si

$$\pm\frac{k_i}{l_i}=\pm\frac{\lambda_i r_i}{\lambda_i s_i}=\pm\frac{r_i}{s_i}\qquad(i=1,2,\ldots,m)$$

sont les inclinaisons des m côtés du polygone de $f(x)$ et, si d représente le degré de l'un des diviseurs de $F(x)$ dans le domaine de p, on a nécessairement

$$d=\sum_{i=1}^{m}\mu_i s_i,$$

où μ_i est l'une des quantités 0, 1, 2, ... ou λ_i. Cela en vertu du théorème du paragraphe **3** (n° **3**).

Nous sommes donc en mesure d'énoncer la proposition :

Un polynome $f(x)$ dont les côtés, dans le polygone qui lui correspond relativement à un nombre premier p, sont d'inclinaison

$$\pm\frac{k_i}{l_i}=\pm\frac{\lambda_i r_i}{\lambda_i s_i}=\pm\frac{r_i}{s_i}$$

ne peut admettre comme diviseurs irréductibles (au sens usuel) *que des diviseurs de degrés égaux respectivement à certaines des sommes*

$$\sum_{i=1}^{m}\mu_i s_i,$$

dans lesquelles μ_i est l'une quelconque des quantités 0, 1, 2, ... ou λ_i *et où m représente le nombre des côtés du polygone de $f(x)$.*

Les quantités k_i, l_i, λ_i, r_i, s_i ont la signification qui leur a été attribuée au paragraphe **3**, n° **2**. Dans le cas où l'un des côtés est parallèle à l'axe des abscisses ou se confond avec lui, on prendra $\lambda_i=l_i$, $s_i=1$.

5. Si, en particulier, le polygone relatif à $f(x)$ se réduit à une droite d'inclinaison égale en valeur absolue à

$$\frac{k}{l}=\frac{\lambda r}{\lambda s}=\frac{r}{s},$$

les seuls diviseurs irréductibles que peut admettre $f(x)$ seront de degrés égaux à certains des nombres s, $2s$, $3s$, ..., $(\lambda - 1)s$.

Lorsque la fraction $\frac{k}{l}$ est réduite, on a $l = s$, $f(x)$ par conséquent irréductible.

4. Une autre proposition, conséquence immédiate de la précédente et que nous énoncerons simplement, est la suivante :

Si p, p', ..., $p^{(\nu)}$ sont des nombres premiers quelconques et si

$$\Sigma\mu_i s_i, \quad \Sigma\mu'_i s'_i, \quad \ldots, \quad \Sigma\mu_i^{(\gamma)} s_i^{(\gamma)}, \quad \ldots, \quad \Sigma\mu_i^{(\nu)} s_i^{(\nu)}$$

représentent les sommes qui leur correspondent respectivement, lorsque pour chacun d'eux on construit le polygone correspondant à $f(x)$, seuls les polynomes, dont le degré est susceptible d'être égal, simultanément, à une somme de la forme de chacune des expressions $\Sigma\mu_i^{(\gamma)} s_i^{(\gamma)}$, pourront être diviseurs de $f(x)$.

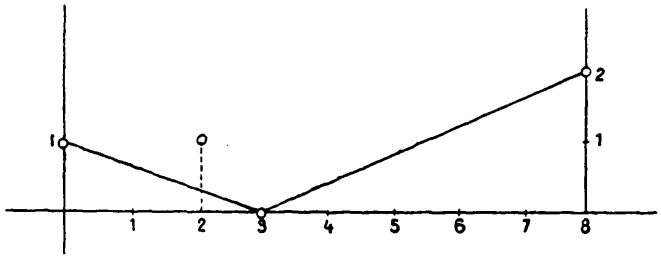
Ce théorème permettra souvent de conclure à l'irréductibilité de certains polynomes, nous allons en donner un exemple.

Soit

$$f(x) = 25x^8 - 3x^3 + 15x^2 + 45,$$

le polygone de $f(x)$, relatif au nombre 5, est donné dans la figure 7,

Fig. 7.

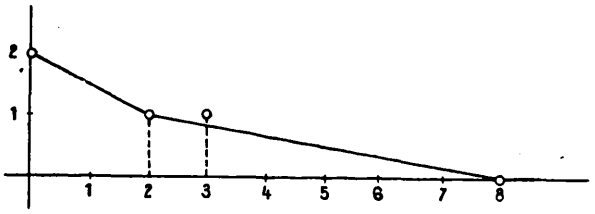


par laquelle on est assuré que, si $f(x)$ est décomposable en facteurs, il ne l'est que comme produit de deux polynomes irréductibles, l'un du cinquième et l'autre du troisième degré.

Relativement au nombre 3, le polygone (*fig.* 8), qui correspond

à $f(x)$, nous montre que $f(x)$ ne peut être égal qu'au produit d'un polynome du sixième degré par un autre du second.

Fig. 8.



Il y a contradiction; $f(x)$ est donc irréductible.

3. Les propositions très générales qui précèdent contiennent, comme cas particuliers, certains théorèmes énoncés déjà, mais d'une manière tout à fait différente, par MM. Kœnigsberger et Netto (¹).

§ 9.

1. Par application à $F(x)$ de la formule (7) du paragraphe **7**, n° **2**, on pourrait, dans chaque cas particulier, et d'une manière plus précise que par les considérations ci-dessus, être fixé sur l'irréductibilité de $f(x)$ ou le degré de ses diviseurs.

Nous retenons le plus simple de tous les cas qui peuvent se présenter.

Soit $f(x)$ un polynome à coefficients rationnels, équivalent, dans le domaine de p, au polynome en x

$$F(x) = x^{2s} + ap^r x^s + bp^{2s} + \Sigma A_{\alpha\beta} p^\alpha x^\beta,$$

(¹) Netto, *Vorlesungen ueber Algebra*, t. I, p. 56 et suiv. — *Ueber die Irreduktibilität ganzzahliger ganzer Funktionen* (*Mathematische Annalen*, t. XLVIII).

Kœnigsberger, *Ueber den Eisenstein'schen Satz von der Irreduktibilität algebraischer Gleichungen* (*Journal de Crelle*, t. 115). — *Ueber die Entwicklungsform algebraischer Funktionen und die Irreduktibilität algebraischer Gleichungen*, 1er Mémoire (*Sitzungsberichte der Kgl. Akad. der Wiss. zu Berlin*, t. II, 1898). *Idem*, 2e Mémoire (*Journal de Crelle*, t. 121).

r et s sont premiers entre eux, b égal à l'une des quantités 1, 2, ... ou $(p-1)$ de même que a, si ce coefficient ne se réduit pas à zéro. $\Sigma A_{\alpha\beta} p^{\alpha} x^{\beta}$ représente un ensemble de termes dont tous les points représentatifs sont au-dessus du polygone de $f(x)$ qui, ici, se réduit à une droite d'inclinaison égale à $\frac{r}{s}$.

$f(x)$ sera irréductible, au sens usuel, aussi bien que dans le domaine de p, s'il en est de même, selon le module p, du trinome $t^2 + at + b$. Si $p = 2$, ce dernier se réduit, soit à $t^2 + t + 1$, soit à $t^2 + 1$; dans le premier cas, $f(x)$ est irréductible, mais, dans le second, aucune conclusion n'est possible, puisque

$$t^2 + 1 \equiv (t+1)^2 \qquad (\mathrm{mod}\, 2).$$

Si p, au contraire, est un nombre premier impair, il existera toujours un entier a', vérifiant la congruence

$$2a' \equiv a \qquad (\mathrm{mod}\, p),$$

et l'irréductibilité de $f(x)$ aura lieu chaque fois que $a'^2 - b$ ne sera pas résidu quadratique de p, puisque

$$t^2 + at + b \equiv (t + a')^2 - [(a')^2 - b] \qquad (\mathrm{mod}\, p).$$

Lorsque $a'^2 - b$ est résidu quadratique de p, sans être divisible par p, $f(x)$ est certainement réductible dans le domaine de p, mais il ne l'est peut-être pas au sens usuel.

Si, enfin, $a'^2 - b$ est divisible par p, la congruence ci-dessus se réduit à

$$t^2 + at + b \equiv (t + a')^2 \qquad (\mathrm{mod}\, p),$$

et il pourra très bien se faire que, même dans le domaine de p, $f(x)$ soit irréductible.

2. Soit maintenant $f(x)$ un polynome quelconque et $\varphi(y)$ le polynome qu'on obtient en remplaçant, dans $f(x)$, x par $y + h$, où h représente un entier arbitraire. Les diviseurs irréductibles de $f(x)$ et $\varphi(y)$ se correspondent. Comme souvent le polygone, relatif à $f(x)$, se confond avec l'axe des abscisses, il y aura avantage, si l'on peut

déterminer h de manière à avoir, selon le module p ou suivant une puissance supérieure de p, $f(h)\equiv 0$, à substituer dans les considérations $\varphi(y)$ à $f(x)$.

C'est cette remarque, du reste, qui semble faire le fond de la démonstration d'Eisenstein de l'irréductibilité de l'équation

$$x^{p-1}+x^{p-2}+\ldots+1=0,$$

dans le cas où p se réduit à un nombre premier (¹).

Si, en effet, dans le premier membre de cette équation, nous remplaçons x par $y+1$, nous obtenons un polynome $\varphi(y)$ irréductible, puisque le polynome qui lui correspond se réduit à une droite d'inclinaison $\frac{k}{l}=\frac{1}{p-1}$.

5. Nous appliquerons l'observation ci-dessus en la combinant avec le théorème du paragraphe **8**, n° **4**, pour démontrer l'irréductibilité du polynome

$$f(x)=x^6-2x^3+28.$$

Le polygone de cette expression est donné, pour le nombre 2, par la

Fig. 9.

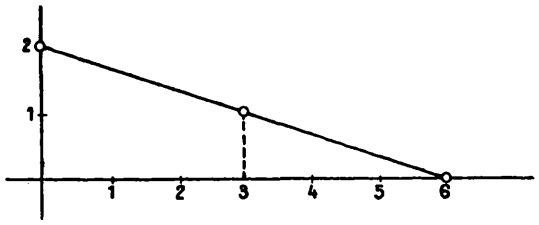


figure 9. Il se réduit à une droite et montre que $f(x)$ ne peut être égal qu'au produit de deux facteurs du troisième degré.

On a, d'autre part,

$$f(1)\equiv 0 \pmod{3^3},$$

(¹) EISENSTEIN, *Ueber die Irreduktibilität und einige andere Eigenschaften der Gleichungen von welcher die Teilung der ganzen Lemniskate abhängt* (*Journal de Crelle*, t. 39).

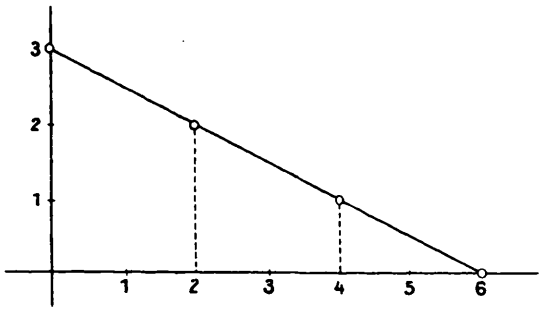
et la substitution $x = y + 1$ transforme $f(x)$ en

$$\varphi(y) = y^6 + 6y^5 + 15y^4 + 18y^3 + 9y^2 + 27.$$

Le polygone de $\varphi(y)$ relatif au nombre 3 est donné par la figure 10.

Il se réduit aussi à une droite et fait voir que les diviseurs de $\varphi(y)$, s'ils existent, sont tous du deuxième, ou l'un du deuxième et l'autre du quatrième degré.

Fig. 10.



$f(x)$ est donc irréductible, ce que nous nous proposions d'établir.

§ 10.

1. *Si, dans le polygone correspondant à un polynome $f(x)$ et relatif à un nombre premier p, aucun côté n'a même inclinaison qu'un côté quelconque du polygone correspondant à un autre polynome $g(x)$ et relatif au même nombre premier p, les deux polynomes $f(x)$ et $g(x)$ n'ont,* au sens usuel, *aucun diviseur commun.*

Cette proposition, dans laquelle $f(x)$ et $g(x)$ représentent des polynomes quelconques à coefficients rationnels, est une conséquence immédiate de celle du paragraphe **3**, n° **3**, et comme telle n'a besoin d'aucune démonstration.

2. Le théorème ci-dessus exprime une condition nécessaire pour que deux polynomes admettent un diviseur commun. Celle-ci toutefois n'est pas suffisante, mais voici comment on pourra, lorsqu'elle se vérifie, être fixé, dans la plupart des cas, sur l'existence d'un pareil diviseur.

Soient :

$$f(x) = a_0 p^{\rho} x^n + a_1 x^{n-1} + \ldots + a_n,$$
$$g(x) = b_0 p^{\sigma} x^m + b_1 x^{m-1} + \ldots + b_m$$

les deux polynomes à coefficients rationnels que nous considérons et qui, par hypothèse, admettent dans leurs polygones respectifs, relativement à p, certains côtés de même inclinaison. Dans l'expression de chacun d'eux, nous avons mis en évidence la plus haute puissance de p divisant exactement les coefficients de x^n et x^m. a_0 et b_0 ne sont plus divisibles par p.

La formule (4) (§ 4, n° 3) permet d'écrire

$$f(x) = a_0 p^{k'_1} \Pi f_{ij}(x) + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p),$$
$$g(x) = b_0 p^{k''_1} \Pi g_{ij}(x) + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p).$$

Si, parmi les polynomes $f_{ij}(x)$, il n'y en a aucun qui soit identique à l'un des polynomes $g_{ij}(x)$, nous sommes assurés que $f(x)$ et $g(x)$ n'ont aucun diviseur commun.

Si le contraire a lieu (ce qui ne peut arriver que pour des f_{ij} et g_{ij} correspondant à des côtés de même inclinaison), $f(x)$ et $g(x)$ pourront admettre un diviseur commun. *Son degré sera au plus égal à la somme des degrés des polynomes identiques, parmi les f_{ij} et g_{ij}.*

Appliquons ceci à un exemple.

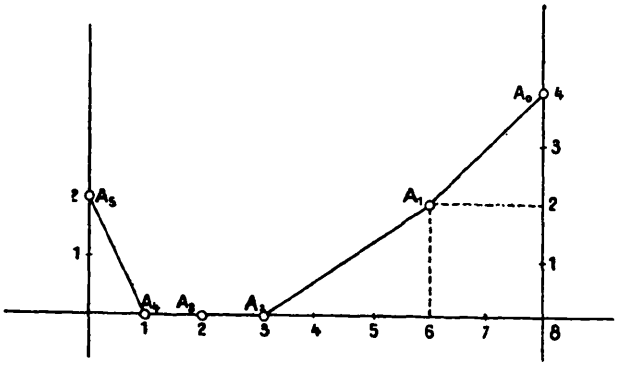
3. Supposons que les deux polynomes à coefficients rationnels $f(x)$ et $g(x)$ soient, dans le domaine du nombre premier 5, équivalents respectivement aux deuxièmes membres des relations (1) :

$$f(x) = 0{,}0002\ldots x^8 + 0{,}0002\ldots x^7 + 0{,}02\ldots x^6 + 0{,}03\ldots x^5 + 0{,}03\ldots x^4 + 3{,}\ldots x^3 + 1{,}\ldots x^2 + 1{,}\ldots x + 0{,}01\ldots;$$
$$g(x) = 0{,}03\ldots x^6 + 0{,}04\ldots x^5 + 0{,}001\ldots x^4 + 3{,}\ldots x^3 + 4{,}\ldots x^2 + 0{,}4\ldots x + 0{,}004\ldots.$$

(1) Dans les coefficients, écrits suivant la notation de M. Hensel, nous n'indiquons que le premier chiffre parce que seul celui-ci importe pour le but que nous nous proposons.

Les polygones respectifs de $f(x)$ et $g(x)$ sont alors donnés par les figures 11 et 12. Comme dans ceux-ci les côtés A_1A_2 et B_0B_1, A_2A_4 et B_1B_2, A_4A_5 et B_3B_4 ont respectivement même inclinaison, il pourrait se faire que $f(x)$ et $g(x)$ aient, au sens usuel, un plus grand commun diviseur du cinquième degré. Il n'en est rien, cependant.

Fig. 11.

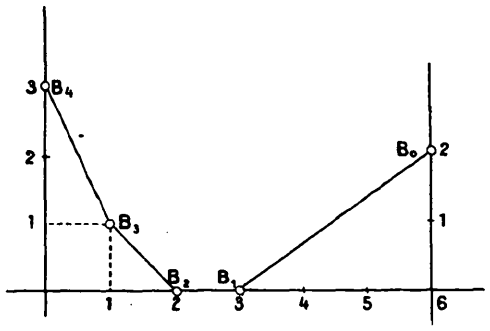


Dans le second membre de $f(x)$, le polynome

$$F(x) = 2.5^4x^8 + 2.5^2x^6 + 3x^3 + x^2 + x + 5^2$$

constitue l'ensemble des termes dont les points représentatifs sont

Fig. 12.



situés sur le contour $A_0A_1 \ldots A_5$ du polygone de la figure 11. Nous le remplaçons par le suivant :

$$F_1(x) = 5^4x^8 + 5^2x^6 + 4x^3 + 3x^2 + 3x + 3.5^2,$$

obtenu en rendant égal à l'unité le coefficient du terme 5^4x^6 dans $F(x)$. Il a fallu pour cela multiplier $F(x)$ par le facteur 3, auquel conduit la congruence

$$2.3 \equiv 1 \pmod 5,$$

puis réduire tous les nouveaux coefficients à leurs plus petits restes selon le module 5.

Relativement à $g(x)$, les polynomes

$$G(x) = 3.5^2x^6 + 3x^3 + 4x^2 + 4.5x + 4.5^3$$

et

$$G_1(x) = 5^2x^6 + x^3 + 3x^2 + 3.5x + 3.5^3$$

ont même signification que F et F_1 dans $f(x)$.

Or on peut écrire (§ **4**, n^{os} **1** et **2**)

$$F_1(x) = (5^2x^2 + 1)(5^2x^3 + 4)(x + 3)(x + 4)(x + 5^2) + \Sigma A_{\alpha\beta}5^\alpha x^\beta,$$
$$G_1(x) = (5^2x^3 + 1)(x + 3)(x + 5)(x + 5^2) + \Sigma A_{\alpha\beta}5^\alpha x^\beta,$$

ce qui montre, à cause des deux facteurs $(x + 3)$ et $(x + 5^2)$, communs à ces deux décompositions, que $f(x)$ et $g(x)$ ont, au plus, un diviseur commun du deuxième degré.

4. La remarque (§ **9**, n° **2**) peut trouver ici son application. C'est ainsi que les deux polynomes :

$$f(x) = x^4 + 6x^3 + 6x^2 + 27,$$
$$g(x) = x^4 - 12x^3 - 15x^2 + 27$$

n'ont aucun diviseur commun, bien que leurs polygones respectifs relativement au nombre 3 soient identiques. Si, en effet, on remarque que $f(1) = 40$, $g(1) = 1$, on se rend de suite compte qu'après la substitution $x = y + 1$, $f(x)$ se transforme en une expression dont le polygone relativement au nombre 2 est situé au-dessus de l'axe des abscisses, tandis que le polygone de l'expression transformée de $g(x)$ se confond avec cette droite.

§ 11.

1. Soient :

$$f(x) = a_0 p^{\rho} x^n + a_1 x^{n-1} + \ldots + a_n,$$
$$g(x) = b_0 p^{\sigma} x^m + b_1 x^{m-1} + \ldots + b_m,$$

deux polynomes à coefficients rationnels dans lesquels nous avons mis en évidence les puissances de p, facteurs de x^n et x^m; a_0 et b_0 ne sont pas divisibles par p.

Comme conséquence de la formule (8) du paragraphe 5, n° **8**, nous écrivons :

$$f(x) = a_0 p^{k_1''} \Pi \mathrm{P}_i(x) \qquad (p),$$
$$g(x) = b_0 p^{k_1''} \Pi \mathrm{Q}_j(x) \qquad (p),$$

les $\mathrm{P}_i(x)$ et $\mathrm{Q}_j(x)$ étant les polynomes qui se rattachent à chacun des côtés des polygones de $f(x)$ et $g(x)$, relativement à p. k_1'' et k_2'' sont les ordonnées des points les plus bas.

La notion de résultant de deux polynomes entiers s'étend immédiatement aux polynomes en x. Si donc nous désignons, d'une manière générale, par $\mathrm{R}(\varphi, \psi)$ le résultant de deux polynomes quelconques, polynomes en x ou polynomes entiers, φ et ψ, nous avons

$$(1) \qquad \begin{cases} \mathrm{R}(f, g) = a_0^m b_0^n p^{m k_1'' + n k_2''} \mathrm{R}[\Pi \mathrm{P}_i(x), \Pi \mathrm{Q}_j(x)] \\ \qquad\quad = a_0^m b_0^n p^{m k_1'' + n k_2''} \Pi \mathrm{R}(\mathrm{P}_i, \mathrm{Q}_j) \qquad (p). \end{cases}$$

Cette formule, dans le deuxième membre de laquelle le produit s'étend à toutes les combinaisons possibles de deux facteurs P_i et Q_j, peut servir au calcul de la puissance de p qui divise exactement le résultant $\mathrm{R}(f, g)$ de f et g.

2. Admettons que P_i et Q_j correspondent à deux côtés, d'inclinaisons distinctes, des polygones relatifs à $f(x)$ et $g(x)$. Les polygones de P_i et Q_j sont alors des droites; soient $\varphi(x)$ et $\psi(x)$ l'ensemble des termes qui, dans chacun d'eux, ont leurs points représentatifs sur

celles-ci. On aura

$$P_i = P = \varphi(x) + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p),$$
$$Q_j = Q = \psi(x) + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta} \qquad (p),$$

avec $\varphi(x)$ égal à l'un des deux polynomes

$$\varphi'(x) = x^{\lambda s} + \ldots + b x^{(\lambda - j)s} p^{jr} + \ldots + c p^{\lambda r},$$
$$\varphi''(x) = x^{\lambda s} p^{\lambda r} + \ldots + b x^{(\lambda - j)s} p^{(\lambda - j)r} + \ldots + c,$$

et $\psi(x)$ égal à l'un des deux autres polynomes

$$\psi'(x) = x^{\lambda' s'} + \ldots + b' x^{(\lambda' - j)s'} p^{jr'} + \ldots + c' p^{\lambda' r'},$$
$$\psi''(x) = x^{\lambda' s'} p^{\lambda' r'} + \ldots + b' x^{(\lambda' - j)s'} p^{(\lambda' - j)r'} + \ldots + c',$$

les coefficients c et c' n'étant pas divisibles par p. Si l'on a $r = 0$, $s = 1$ dans φ' ou φ'', les résultats auxquels on aboutit subsistent; le signe qu'on attribue à une inclinaison nulle reste d'ailleurs indifférent.

Nous distinguons quatre cas :

Premier cas : $\varphi = \varphi'$, $\psi = \psi'$. — Soit, pour fixer les idées, $\frac{r'}{s'} > \frac{r}{s}$, et faisons, dans P et Q, la substitution $x = y p^{\frac{r}{s}}$. P se transforme alors en $p^{\lambda r} P_1$, où

$$P_1 = y^{\lambda s} + \ldots + b y^{(\lambda - j)s} + \ldots + c + p^{\frac{\varepsilon}{s}} M(y)$$

et Q en $p^{\lambda' s' \frac{r}{s}} Q_1$, où

$$Q_1 = y^{\lambda' s'} + \ldots + b' y^{(\lambda' - j)s'} p^{\frac{j}{s}(r's - s'r)} + \ldots + c p^{\frac{\lambda'}{s}(r's - s'r)} + p^{\frac{\varepsilon'}{s}} N(y).$$

Dans ces deux expressions $M(y)$ et $N(y)$ sont des polynomes en y, dont les coefficients dépendent de $p^{\frac{1}{s}}$. Ceux-ci ne renferment aucune puissance négative de cette quantité; ε et ε' sont deux quantités positives différentes de zéro.

Comme maintenant, d'après la théorie des résultants, on a

$$R\left(p^{\lambda r} P_1, p^{\lambda' s' \frac{r}{s}} Q_1\right) = p^{\lambda r \lambda' s'} R(P, Q) \qquad (p),$$

tandis que, d'autre part,

$$R\left(p^{\lambda r}P_1, p^{\lambda' s' \frac{r}{s}}Q_1\right) = p^{2\lambda r \lambda' s'} R(P_1, Q_1) \qquad (p),$$

on aura

$$R(P, Q) = p^{\lambda r \lambda' s'} R(P_1, Q_1) \qquad (p). \tag{2}$$

Mais le résultant $R(P_1, Q_1)$ ne peut être qu'une suite à caractère entier de puissances de $p^{\frac{1}{s}}$. Son premier terme est égal à $c^{\lambda' s'}$; on a donc

$$R(P, Q) = c^{\lambda' s'} p^{\lambda r \lambda' s'} + \ldots \qquad (p),$$

$R(P, Q)$, par conséquent, divisible exactement, dans le domaine de p, par $p^{\lambda r \lambda' s'}$; mais ceci suppose l'inégalité $\frac{r'}{s'} > \frac{r}{s}$.

Les trois autres cas se traitent d'une manière analogue.

Deuxième cas : $\varphi = \varphi''$, $\psi = \psi'$. — On trouve

$$R(P, Q) = c^{\lambda' s'} + \ldots \qquad (p).$$

Troisième cas (identique au précédent) : $\varphi = \varphi'$, $\psi = \psi''$.

$$R(P, Q) = c'^{\lambda s} + \ldots \qquad (p).$$

Quatrième cas : $\varphi = \varphi''$, $\psi = \psi''$.

$$R(P, Q) = c'^{\lambda s} p^{\lambda r \lambda' s'} + \ldots \qquad (p).$$

Ici, comme dans le premier cas, on a par hypothèse $\frac{r'}{s'} > \frac{r}{s}$.

Soient, en conséquence et pour résumer, $P(x)$ *et* $Q(x)$ *deux polynomes en* x, *dont les polygones respectifs sont des droites, d'inclinaisons distinctes, situées, en le touchant, au-dessus de l'axe des abscisses, l'une d'elles pouvant se confondre avec lui; suivant que les deux inclinaisons sont, ou non, de même signe, le résultant de* $P(x)$ *et de* $Q(x)$ *est, ou non, divisible par* p. *Si les deux droites ont des inclinaisons de même signe, représentées respectivement en*

valeur absolue par les rapports

$$\frac{k}{l} = \frac{\lambda r}{\lambda s} = \frac{r}{s} \qquad et \qquad \frac{k'}{l'} = \frac{\lambda' r'}{\lambda' s'} = \frac{r'}{s'},$$

le résultant de $P(x)$ *et* $Q(x)$, *en supposant* $\frac{r'}{s'} > \frac{r}{s}$, *est toujours exactement divisible par* $p^{\lambda r \lambda' s'} = p^{kl'}$.

3. Reste enfin le cas où les deux inclinaisons sont égales, $\frac{r}{s} = \frac{r'}{s'}$.

Le résultant $R(P, Q)$ est alors certainement divisible par $p^{kl'}$; mais il peut l'être aussi par une puissance supérieure.

Si nous nous plaçons dans le premier des cas examinés, P et Q, par la substitution $x = y p^{\frac{r}{s}}$, se transforment et deviennent $p^{\lambda r} P_1$ et $p^{\lambda' r'} Q_1$. P_1 est le polynome du premier cas, Q_1 prend la forme

$$Q_1 = y^{\lambda' s} + \ldots + b' y^{(\lambda' - j)s} + \ldots + c' + p^{\frac{\varepsilon'}{s}} N(y).$$

Le résultant de P et Q est divisible par une puissance de p, supérieure à $p^{kl'}$, lorsque le résultant des deux polynomes formés par les termes indépendants de $p^{\frac{1}{s}}$, dans P_1 et Q_1, se trouve divisible par p. Si la chose a lieu, $R(P_1, Q_1)$ dans (2), est alors divisible par une puissance positive de p. Pour l'évaluation exacte de celle-ci, certains termes de $p^{\frac{\varepsilon}{s}} M(y)$ et de $p^{\frac{\varepsilon'}{s}} N(y)$, dans P_1 et Q_1, ceux qui dépendent des plus petites puissances de p, doivent être pris en considération.

Une conclusion analogue s'obtiendrait en partant du quatrième cas.

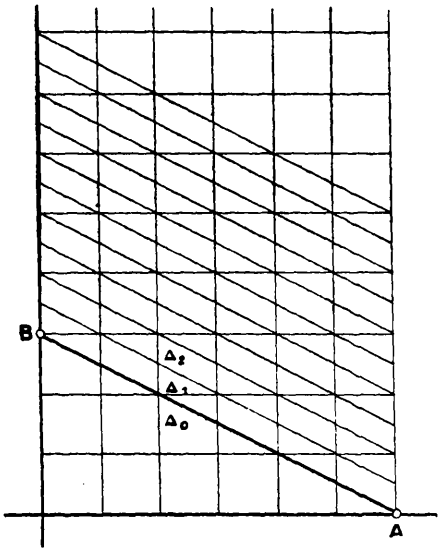
4. Les résultats de ce paragraphe donnent en conséquence le moyen par l'intermédiaire de la formule (1), et par l'examen seul des polygones, de déterminer dans des cas étendus, ressortant de ce qui précède, la puissance de p qui entre exactement dans le résultant de deux polynomes à coefficients rationnels.

§ 12.

1. Supposons un polynome en x, admettant (*fig.* 13), comme po-

lygone une droite AB dont l'inclinaison mise sous forme réduite est égale à $\frac{r}{s}$.

Fig. 13.



On peut alors envisager les points représentatifs des termes de tout polynome en x, à coefficients ordonnés suivant les puissances croissantes du même nombre premier p, comme répartis sur des droites parallèles à AB, dont la distance (§ 3, n° 2) comptée sur l'axe des ordonnées est égale à $\frac{1}{s}$.

Nous numérotons ces parallèles à partir de AB et dans l'ordre où elles se présentent nous les appelons Δ_1, Δ_2, Δ_3, ..., en désignant par Δ_0 la droite AB elle-même. Les indices négatifs resteront réservés pour les autres parallèles à AB, situées au-dessous de AB. Enfin, nous introduisons une notation en convenant que des congruences telles que

$$h(x) \equiv 0 \qquad (\mathrm{mod}\,\Delta_k),$$
$$h(x) \equiv h'(x) \qquad (\mathrm{mod}\,\Delta_k),$$

dans lesquelles $h(x)$ et $h'(x)$ sont des polynomes en x, signifient que les points représentatifs de $h(x)$, respectivement de $h(x) - h'(x)$, sont situés *sur* Δ_k ou *au-dessus*.

Si $h(x)$ et $h'(x)$, ou seulement l'un de ces deux polynomes, sont *entiers*, la même définition subsiste; mais, dans ce cas, les points représentatifs de $h(x)$ et $h'(x)$ seront, par définition, ceux de leurs polynomes en x équivalents dans le domaine de p.

Soient maintenant $h(x)$ et $g(x)$ deux polynomes entiers, vérifiant, le premier, $h(x)$, la première des congruences ci-dessus, le second, $g(x)$, la suivante

$$g(x) \equiv 0 \qquad (\mathrm{mod}\,\Delta_j).$$

Dans ces deux congruences, K et j sont, par hypothèse, aussi grands que possible.

Nous disons alors que $h(x)$ n'est pas divisible par $g(x)$, *le long de* Δ_k, s'il n'y a aucun polynome entier $\varphi(x)$, cas échéant indépendant de x, de manière à avoir

$$h(x) \equiv g(x)\,\varphi(x) \qquad (\mathrm{mod}\,\Delta_{k+1}).$$

$g(x)$ de son côté, sera irréductible, *le long de* Δ_j, s'il est impossible de trouver deux polynomes entiers, de degrés respectivement inférieurs à celui de $g(x)$, $l(x)$ et $r(x)$, donnant lieu à la congruence

$$g(x) \equiv l(x)\,r(x) \qquad (\mathrm{mod}\,\Delta_{j+1}).$$

Nous faisons ces conventions, autant pour simplifier l'énoncé du prochain théorème, que pour mettre en évidence le rapport qui existe entre les congruences, prises par rapport à un nombre premier p, et celles que nous considérons ici. Il suffit, en effet, de supposer (*fig.* 13) que AB se confond avec l'axe des abscisses, pour pouvoir remplacer Δ_k par p^k, dans toute congruence où intervient le module Δ_k.

Ajoutons, enfin, que la figure 13 se rapporte au polynome $f(x)$, dont nous allons nous occuper. AB sera le polygone rectiligne, Δ_0, de $f(x)$, relativement à p. Δ_0 sera la $0^{\text{ième}}$ parallèle à AB, tandis que Δ'_0, le polygone de $g(x)$, serait, dans la même figure, une certaine droite d'indice négatif.

2. Ces préliminaires établis nous avons la proposition (1) :

Soit $g(x)$ un polynome entier qui ne dépend que de x^s, à coeffi-

(1) Pour avoir le théorème de Schoenemann (M. Bauer, *loc. cit.*) il suffit de

cients rationnels, susceptible d'être mis sous la forme

$$g(x) = x^{\lambda s} + b_1 x^{(\lambda-1)s} p^r + \ldots + b_j x^{(\lambda-j)s} p^{jr} + \ldots + b_\lambda p^{\lambda r},$$

dans laquelle $b_1, b_2, \ldots, b_\lambda$ *sont des entiers par rapport au nombre premier* p, *le dernier* b_λ *n'étant pas, par rapport à* p, *divisible par* p; *soit* q *un entier positif,* $h(x)$ *un polynome entier, à coefficients rationnels, cas échéant indépendant de* x *et de degré inférieur à* $n = \lambda qs$.

Si cela est, le polynome entier, de degré n, *et dont le polygone, relativement à* p, *est une droite,* Δ_n, *d'inclinaison égale à* $\frac{r}{s}$,

$$f(x) = g^q(x) + h(x), \tag{1}$$

est irréductible, lorsque les conditions suivantes se trouvent réalisées.

a. $h(x) \equiv 0 \pmod{\Delta_\theta}$, θ *étant égal ou supérieur à l'unité et* Δ_θ *la dernière des droites* Δ *entrant dans pareille congruence,*

b. $g(x)$, *irréductible le long de son polygone rectiligne* Δ'_0,

c. $h(x)$, *non divisible par* $g(x)$, *le long de* Δ_θ,

d. le plus grand commun diviseur de q *et* θ, *égal à l'unité,*

e. le discriminant de l'équation $G(y) = 0$, *non divisible par* p, $G(y)$ *étant le polynome entier défini par l'égalité*

$$g\left(yp^{\frac{r}{s}}\right) = p^{\lambda r} G(y).$$

---

supposer que le polygone de $f(x)$ se confond avec l'axe des abscisses, ou, ce qui revient au même, de faire $r = 0$, $s = 1$, dans l'énoncé que nous avons ici. Les conditions *a*, *b*, *c* se transforment alors, conformément à ce que nous avons dit touchant les congruences suivant les lignes Δ_k. Au lieu de *a*, on aurait

$$h(x) \equiv 0 \pmod{p^\theta}, \quad \ldots,$$

d reste telle quelle et *e* se trouve satisfaite d'elle-même. Ajoutons qu'en déterminant, comme dans la note du bas de la page 236, directement les points représentatifs des polynomes entiers, on peut donner une autre définition des congruences le long des lignes Δ_k, absolument équivalente à celle que nous avons adoptée. Celle-ci rendrait l'énoncé du théorème indépendant des suites de Hensel.

3. La substitution

$$x = y\,p^{\frac{r}{s}} \tag{2}$$

transforme $g(x)$ en $p^{\lambda r}\,\mathrm{G}(y)$ où

$$\mathrm{G}(y) = y^{\lambda s} + b_1 y^{(\lambda-1)s} + \ldots + b_j y^{(\lambda-j)s} + \ldots + b_\lambda.$$

A cause de (b) et comme au paragraphe **4**, n° **2**, on verrait que le polynome

$$g'(t) = t^\lambda + b_1 t^{\lambda-1} + \ldots + b_j t^{\lambda-j} + \ldots + b_\lambda,$$

est irréductible selon le module p, irréductible par conséquent au sens usuel. Si donc nous écrivons

$$g'(t) = 0, \tag{3}$$

les racines $t_1, t_2, \ldots, t_\lambda$ de cette équation seront algébriquement conjuguées.

Remarquons toutefois que l'irréductibilité de $g'(t)$ n'entraîne pas nécessairement celle de $\mathrm{G}(y)$. On a, par exemple, $t^2 + t + 1$ irréductible selon le module 2, alors que

$$y^4 + y^2 + 1 = (y^2 + y + 1)(y^2 - y + 1).$$

4. Mettons en évidence les racines de $\mathrm{G}(y)$ et soit

$$\mathrm{G}(y) = (y - \xi_1)(y - \xi_2)\ldots(y - \xi_{\lambda s}). \tag{4}$$

Remplaçons $h(x)$ par le polynome en x, $\mathrm{H}(x)$ équivalent à $h(x)$ dans le domaine de p.

Décomposons ensuite $\mathrm{H}(x)$ en deux parties et écrivons

$$\mathrm{H}(x) = h'(x) + h''(x) \qquad (p); \tag{5}$$

$h'(x)$ est le polynome entier formé des termes de $\mathrm{H}(x)$ dont les points représentatifs se trouvent sur Δ_0. De tels termes existent toujours à cause de (a). Si dans $\mathrm{H}(x)$ nous faisons la substitution (2),

nous obtenons, après division par $p^{\lambda rq+\frac{\theta}{s}}$, en correspondance avec (5), la relation

$$H\left(y, p^{\frac{1}{s}}\right) = H'(y) + p^{\frac{\varepsilon}{s}} H''\left(y, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right), \tag{6}$$

dans laquelle H et H'' sont des polynomes en y, dont les coefficients à caractère entier dépendent de $p^{\frac{1}{s}}$, $H'(y)$ un polynome entier, à coefficients égaux à 1, 2, ..., ou $(p-1)$ et ε un exposant entier, positif et différent de zéro. L'exposant $\lambda rq + \frac{\theta}{s}$, que nous venons de rencontrer, provient de ce que la substitution (2), effectuée sur un terme $A p^{\alpha} x^{\beta}$ dont le point représentatif se trouve sur la droite $\Delta_{\theta+\varepsilon}$, transforme celui-ci en $A p^{\lambda rq+\frac{\theta+\varepsilon}{s}} y^{\beta}$.

Si $h(x)$ était divisible par $g(x)$, le long de Δ_θ, il existerait un polynome entier $\varphi(x)$, tel que la congruence

$$h'(x) \equiv g(x)\varphi(x) \qquad (\operatorname{mod} \Delta_{\theta+1})$$

soit vérifiée. On en déduirait aussitôt, par l'intermédiaire de (2), l'existence d'un polynome entier, $\Phi(y)$, susceptible en même temps que $\varphi(x)$ de se réduire à une constante, et tel qu'on ait

$$H'(y) \equiv G(y)\Phi(y) \qquad (\operatorname{mod} p).$$

La réciproque est vraie également.

L'hypothèse (c) entraîne donc, avec elle, l'existence de deux polynomes entiers $\sigma(y)$ et $\tau(y)$, à coefficients entiers, vérifiant la congruence

$$H'(y)\sigma(y) + G(y)\tau(y) \equiv 1 \qquad (\operatorname{mod} p).$$

On a donc, à cause de (4),

$$H'(\xi_i)\sigma(\xi_i) \equiv 1 \qquad (\operatorname{mod} p), \qquad (i = 1, 2, \ldots, \lambda s),$$

d'où résulte, $H'(\xi_i)$, non divisible algébriquement par aucune puissance entière ou fractionnaire de p. Le premier terme du développement de $H\left(\xi_i, p^{\frac{1}{s}}\right)$, suivant les puissances croissantes de $p^{\frac{1}{s}}$, sera donc, par suite de (6), différent de zéro et indépendant de $p^{\frac{1}{s}}$.

5. Une première conséquence de (e), c'est le fait que les résultants des polynomes tels que

$$(y-\xi_i)^q \qquad \text{et} \qquad \left(\frac{G(y)}{y-\xi_i}\right)^q$$

ne sont divisibles algébriquement par aucune puissance entière ou fractionnaire de p.

6. L'égalité (1) conduit à l'équivalence

$$F(x) = g^q(x) + H(x) \qquad (p). \tag{7}$$

$H(x)$ représente, comme plus haut, le polynome équivalent à $h(x)$; $F(x)$ le polynome équivalent à $f(x)$, dans le domaine de p.

Appliquée à (7), la substitution (2) transforme cette équivalence en une nouvelle,

$$F\left(y, p^{\frac{1}{s}}\right) = [G(y)]^q + p^{\frac{\theta}{s}} H\left(y, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right). \tag{8}$$

Or ici, de par le n° 5 et parce que les suites en $p^{\frac{1}{s}}$, coefficients des polynomes qui s'introduisent dans la décomposition en facteurs, effectuées comme au paragraphe 5, n° 6, sont du type considéré (§ 2, n° 6), nous sommes assurés que $F\left(y, p^{\frac{1}{s}}\right)$ est réductible dans le domaine de $p^{\frac{1}{s}}$.

On pourra toujours mettre $F\left(y, p^{\frac{1}{s}}\right)$ sous la forme

$$F\left(y, p^{\frac{1}{s}}\right) = R_i\left(y, p^{\frac{1}{s}}\right) S_i\left(y, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right), \tag{9}$$

où

$$\begin{cases} R_i\left(y, p^{\frac{1}{s}}\right) = (y-\xi_i)^q + p^{\frac{\theta}{s}} H_i\left(y, p^{\frac{1}{s}}\right), \\ S_i\left(y, p^{\frac{1}{s}}\right) = \left(\frac{G(y)}{y-\xi_i}\right)^q + p^{\frac{\theta}{s}} K_i\left(y, p^{\frac{1}{s}}\right). \end{cases} \tag{10}$$

ξ_i est une racine quelconque de l'équation $G(y) = 0$, H_i et K_i des

polynomes en y, dont les coefficients égaux à des suites telles que

$$\varepsilon_0^{(i)} + \varepsilon_1^{(i)} p^{\frac{1}{s}} + \varepsilon_2^{(i)} p^{\frac{2}{s}} + \dots$$

sont tous à caractère entier. Les $\varepsilon_0^{(i)}$, $\varepsilon_1^{(i)}$, ... sont tous des entiers algébriques, par rapport à p, du corps $\mathrm{R}(\xi_i)$. 0, enfin, est toujours la même quantité, celle dont il est question dans (a).

Supposons maintenant l'équation $\mathrm{G}(y) = 0$ irréductible; puis considérons le corps normal ou de Galois que l'on obtient par adjonction de toutes les racines $\xi_1, \xi_2, \dots, \xi_{\lambda s}$ au domaine des nombres rationnels. A cause de (e), le discriminant de ce corps n'est pas divisible par p.

Si donc $\alpha_\rho, \alpha_{\rho+1}, \dots$ représentent, par rapport à p, des unités de ce dernier, la décomposition de $\mathrm{F}\left(y, p^{\frac{1}{s}}\right)$ en un produit de polynomes en y, irréductibles, et dont les coefficients seraient des suites telles que

$$\alpha_\rho p^{\frac{\rho}{s}} + \alpha_{\rho+1} p^{\frac{\rho+1}{s}} + \dots,$$

se ferait (§ **2**, n° **6**) d'une manière uniforme.

De ce dernier type sont aussi les coefficients, mis sous forme réduite, des polynomes R_i; on peut du moins les envisager comme tels. Deux quelconques des polynomes R_i n'ont, en outre, aucun diviseur commun (puisque les racines ξ_i sont toutes distinctes); ils sont, d'autre part, tous diviseurs de $\mathrm{F}\left(y, p^{\frac{1}{s}}\right)$ et la somme de leurs degrés respectifs est égale à celui de ce polynome. Nous avons donc ce que nous voulions obtenir,

$$\mathrm{F}\left(y, p^{\frac{1}{s}}\right) = \prod_{i=1}^{\lambda s} \mathrm{R}_i\left(y, p^{\frac{1}{s}}\right). \tag{11}$$

Si l'équation $\mathrm{G}(y) = 0$ n'est pas irréductible, la même conclusion subsiste. On le voit facilement et sans avoir à modifier, pour ainsi dire, les quelques remarques qui précèdent.

7. Donnons à i, pour fixer les idées, une valeur particulière $i = 1$

et remarquons que de (8) on déduit

$$F\left(\xi_1, p^{\frac{1}{s}}\right) = p^{\frac{\theta}{s}} H\left(\xi_1, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right),$$

et, par conséquent, à cause de (10) et (11),

$$H\left(\xi_1, p^{\frac{1}{s}}\right) = H_1\left(\xi_1, p^{\frac{1}{s}}\right) \prod_{i=2}^{\lambda s} R_i\left(\xi_i, p^{\frac{1}{s}}\right) \qquad \left(p^{\frac{1}{s}}\right).$$

Si l'on ordonnait le produit suivant les puissances croissantes de $p^{\frac{1}{s}}$, la suite qu'on obtiendrait commencerait par un terme différent de zéro, non divisible par $p^{\frac{1}{s}}$. On sait (n° **4**) qu'il en est de même de $H\left(\xi_1, p^{\frac{1}{s}}\right)$.

$H_1\left(\xi_1, p^{\frac{1}{s}}\right)$ et, d'une manière générale, les expressions $H_i\left(\xi_i, p^{\frac{1}{s}}\right)$ jouissent donc de cette même propriété.

8. Remplaçons maintenant dans R_i, y par $z + \xi_i$. On obtient alors un nouveau polynome que l'on peut écrire

$$R_i'\left(z, p^{\frac{1}{s}}\right) = z^q + p^{\frac{\theta}{s}} H_i\left(\xi_i, p^{\frac{1}{s}}\right) + p^{\frac{\theta}{s}} z^\varepsilon H_i'\left(z, p^{\frac{1}{s}}\right),$$

où H_i' représente un certain polynome en z, dont les coefficients, suites ordonnées suivant les puissances de $p^{\frac{1}{s}}$, sont tous à caractère entier. ε est un entier positif différent de zéro.

En vertu de ce que nous venons de voir relativement à $H_i\left(\xi_i, p^{\frac{1}{s}}\right)$ le polygone, construit en portant en abscisses les exposants de z et en ordonnées ceux de $p^{\frac{1}{s}}$, devient une droite d'inclinaison $\frac{\theta}{q}$, fraction réduite à cause de (d).

On en déduit aussitôt, par application du théorème du paragraphe **3**, n° **3**, ou par extension de celui du paragraphe **8**, n° **3**, l'irréductibilité de R_i', dans le domaine de $p^{\frac{1}{s}}$; par suite, celle aussi de chacun des diviseurs R_i.

9. Soient maintenant $d(x)$ un diviseur de $f(x)$, $D(x)$ le polynome équivalent à $d(x)$ dans le domaine de p. $D(x)$ est alors diviseur de $F(x)$ et, comme tel, on pourra écrire

$$D(x) = x^{\lambda' s} + \ldots + b x^{(\lambda'-j)s} p^{jr} + \ldots + c p^{\lambda' r} + \Sigma A_{\alpha\beta} p^{\alpha} x^{\beta},$$

où

$$\lambda' \leq \lambda q,$$

et où $\Sigma A_{\alpha\beta} p^{\alpha} x^{\beta}$ représente l'ensemble des termes de $D(x)$ dont les points représentatifs sont situés au-dessus du contour, rectiligne également, relatif à ce polynome. Les coefficients b, ..., c sont égaux à 0, 1, 2, ..., ou $(p-1)$, le dernier d'entre eux c étant d'ailleurs différent de zéro.

La substitution (2), effectuée dans $D(x)$, conduit après simplification par $p^{\lambda' r}$ à

$$D\left(y, p^{\frac{1}{s}}\right) = y^{\lambda' s} + \ldots + b y^{(\lambda'-j)s} + \ldots + c + p^{\frac{\varepsilon}{s}} D'\left(y, p^{\frac{1}{s}}\right),$$

où D' est, comme toujours, un polynome dont les coefficients sont à caractère entier. ε est une quantité positive différente de zéro.

Mais $D\left(y, p^{\frac{1}{s}}\right)$ est diviseur de $F\left(y, p^{\frac{1}{s}}\right)$, et, comme tel, égal au produit d'un certain nombre de facteurs R_i. La forme même de $D\left(y, p^{\frac{1}{s}}\right)$ nous montre que ce produit doit être susceptible de s'écrire

$$\prod \left[(y^s - t_j)^q + p^{\frac{0}{s}} T(y) \right].$$

Les t_j sont racines de l'équation (3) et le signe Π doit être étendu à certains des indices $j = 1, 2, \ldots, \lambda$. $T(y)$ est encore un polynome en y, dont les coefficients sont, comme toujours, à caractère entier.

Les suites qui multiplient, dans $D\left(y, p^{\frac{1}{s}}\right)$, les différentes puissances de y, suites que nous représentons par $\Sigma \alpha_i p^{\frac{i}{s}}$, ont d'autre part leurs coefficients α_i tous rationnels. Pour que cela ait lieu, il faut que le produit ci-dessus s'étende à tous les indices $j = 1, 2, \ldots, \lambda$.

On a donc $\lambda' = \lambda q$, $d(x)$ par conséquent de même degré, $\lambda s q = n$, que $f(x)$ dont l'irréductibilité est ainsi démontrée.