MARCEL COURRIER

Solutions entières des équations du genre O

Thèses de l'entre-deux-guerres, 1931

<http://www.numdam.org/item?id=THESE_1931__119__1_0>

Série E
N° d'ordre :
28

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES DE STRASBOURG

POUR OBTENIR

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES

PAR

Marcel COURRIER
Agrégé de l'Université

1re **THÈSE**. — SOLUTIONS ENTIÈRES DES ÉQUATIONS DE GENRE 0.

2e **THÈSE** — PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Soutenues le 193 / *devant la Commission d'Examen*

MM. VALIRON . . . *Président*
CERF . . . . } *Examinateurs*
FLAMANT . . . }

PARIS (Ve)
LES PRESSES UNIVERSITAIRES DE FRANCE
49, Boulevard Saint-Michel, 49

1931

FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE STRASBOURG

MM.

Doyen	E. Rothé, Professeur de Physique du Globe	
Doyens honoraires....	E. Bataillon, P. Th. Muller.	
Professeurs honoraires.	H. Villat, Gignoux, Fréchet, Gault.	
Professeurs	G. Valiron	Analyse supérieure.
	P. Weiss	Physique générale.
	H. Ollivier	Physique générale.
	L. Hackspill	Chimie minérale.
	E. Topsent	Zoologie et Anatomie comparée.
	C. Houard	Botanique.
	E. Terroine	Physiologie générale.
	J. de Lapparent ...	Pétrographie.
	E. Chatton	Biologie générale.
	R. Thiry	Mécanique.
	G. Cerf	Calcul différentiel et intégral.
	G. Dubois.....	Géologie et Paléontologie.
	G. Ribaud	Physique expérimentale.
	P. Flamant	Mathematiques générales.
	E. Cornec	Chimie générale.
	P. de Beauchamp ..	Biologie générale.
	L. Bounoure	Zoologie.
	G. Foex	Physique générale.
	H. Chermezon.....	Botanique.
	G. Rempp	Physique du Globe.
	R. Romann	Chimie physique et électro-chimie.
	N.....	Astronomie.
	N.....	Chimie organique.
Chargés de cours et Maîtres de Conférences	J. Lagarde	Botanique.
	Ch. Staehling	Chimie appliquée.
	J. Lacoste	Physique du Globe.
	G. Hugel	Chimie du Pétrole.
	H. Weiss	Physico-Chimie du Pétrole.
	H. Milloux	Mathématiques.
	A. Roussel	Mathématiques générales.
	P. Soleillet	Physique mathématique.
	M. Faillebin	Chimie appliquée.
	R. Bonnet	Physique et chimie biologiques.
	G. Mignonac	Chimie organique.
	N.....	Minéralogie.
Secrétaire	G. Cuvier.	

A MES PARENTS

SOLUTIONS ENTIÈRES DES ÉQUATIONS DU GENRE 0

INTRODUCTION

Soit

$$F(X, Y, Z) = 0,$$

une équation homogène, de degré n, de genre O, à coefficients entiers. Nous nous proposons d'en trouver toutes les solutions entières.

L'idée fondamentale consiste à utiliser une représentation entière qu'admet cette courbe qui, si elle est à coefficients entiers, donne une infinité de points entiers.

Relativement au problème qui nous occupe on connaît les résultats suivants.

1° On sait reconnaître si l'équation admet une infinité de points entiers et dans ce cas trouver une représentation entière.

$$\text{(S)} \qquad \begin{cases} X = f(u, v), \\ Y = g(u, v), \\ Z = h(u, v), \end{cases}$$

de degré n, à coefficients entiers où u et v sont les deux termes premiers entre eux du paramètre t figurant dans la représentation non homogène, les coordonnées étant

$$x = \frac{X}{Z}, \qquad y = \frac{Y}{Z}.$$

Il y a correspondance biunivoque entre un point entier et le couple u, v et le système (S) donne tous les points entiers.

2° A un point entier peuvent correspondre plusieurs solutions

entières. Soit en effet d un diviseur commun à X, Y, Z correspondant à un couple u, v. La solution

$$\frac{X}{d}, \quad \frac{Y}{d}, \quad \frac{Z}{d},$$

est entière et n'est pas donnée par le système (S) qui doit être remplacé par le suivant

$$\frac{X}{D}, \quad \frac{Y}{D}, \quad \frac{Z}{D},$$

où D représente le p. g. c. d. de X, Y, Z variable avec le couple u, v.

Le calcul de D en fonction de u et v s'impose donc : Nous nous proposons de faire ce calcul qui jusqu'à présent n'a été fait que dans des cas particuliers.

Il nous semble indispensable de préciser la remarque fondamentale, ce qui nous fait adopter le plan suivant :

1re PARTIE. — *Etude analytique* :

Toute courbe de genre O admet une représentation propre, uniforme, qui est rationnelle. — Réciproque. — Emploi des adjointes.

2e PARTIE. — *Etude algébrique* :

Conditions pour qu'il y ait une infinité de points entiers. Représentation entière à coefficients entiers.

3e PARTIE. — *Etude arithmétique* :

Chapitre I. — Etude générale.

Chapitre II. — Equation

$$PX^2 + QY^2 + RZ^2 = 0.$$

Chapitre III. — Sur l'équation

$$aX^2 + bY^2 + cZ^2 + dT^2 = 0.$$

Dans les 1re et 2e parties, nous nous sommes bornés à rappeler, en les coordonnant ou complétant, quelques résultats connus en indiquant avec soin leur origine.

Dans la 3e partie nous montrons que le p. g. c. d. de X, Y, Z ne prend qu'un nombre limité de valeurs lorsque le couple u, v varie et que l'on peut distinguer entre ces différentes valeurs par un calcul régulier tandis qu'il en est *tout autrement* dans l'équation

$$aX^2 + bY^2 + cZ^2 + dT^2 = 0,$$

où le p. g. c. d. de X, Y, Z, T, prend au contraire une infinité de valeurs lorsque le triplet u, v, w, varie.

Nous employons les notations suivantes : (X, Y) désigne le p. g. c. d. de X et Y ;

$a \mid b$ indique que a divise b ;

$a \nmid b$ indique que a ne divise pas b.

Qu'il nous soit permis, avant d'aller plus loin, de remercier M. Valiron qui nous a particulièrement aidé dans l'entreprise de ce travail et M. Flamant aux nombreux conseils de qui nous sommes tant redevables.

Qu'ils veuillent bien, en égard à cette vive gratitude, accepter l'hommage respectueux de notre travail.

PREMIÈRE PARTIE

ÉTUDE ANALYTIQUE

THÉORÈME I. — *Toute courbe de genre* O *admet une représentation uniforme qui est rationnelle.*

Cette représentation rationnelle est unique, à une substitution homographique près, portant sur le paramètre.

A une valeur du paramètre correspond un seul point de la courbe et inversement.

Soit une courbe de degré n, de genre O, d'équation

$$f(x, y) = 0. \tag{1}$$

1° Pour exprimer x et y en fonction uniforme d'un paramètre t, on peut prendre pour t soit une intégrale abélienne normale de 2e espèce, soit une de 3e espèce attachées à la courbe (1). Dans le 1er cas x et y sont fonctions rationnelles de t et il y a correspondance univoque entre t et le point x, y. Dans le cas x et y sont fonctions de e^t et l'on peut aussi établir une correspondance univoque entre t et le point x, y.

D'après APPELL et GOURSAT, *Théorie des Fonctions algébriques d'une variable*, p. 440.

2° Soient

$$(T) \qquad \begin{cases} x = f(t) \\ y = g(t) \end{cases}$$

et

$$(S) \qquad \begin{cases} x = h(s) \\ y = l(s) \end{cases}$$

deux représentations distinctes de la courbe (1).

La correspondance entre s et t est biunivoque, et étant algébrique, est nécessairement homographique.

D'après PICARD, *Traité d'Analyse*, t. II, p. 552.

THÉORÈME II. — *Réciproquement soit*

$$(T) \qquad \begin{cases} x = \dfrac{f(t)}{g(t)} \\ y = \dfrac{h(t)}{g(t)} \end{cases}$$

une représentation rationnelle où f, g et h sont 3 *polynômes premiers dans leur ensemble, n étant le degré maximum pour les* 3 *ploynômes et le degré effectif de l'un d'eux. Cette représentation définit une courbe de degré n, de genre* O.

La courbe est algébrique, car son équation s'obtient en éliminant t entre x et y.

Elle est de degré n car la droite

$$ax + by + c = 0.$$

la rencontre aux n points d'intersection correspondants aux n valeurs de t racines de l'équation

$$af(t) + bh(t) + cg(t) = 0.$$

Elle est de genre O car une intégrale abélienne de 1re espèce supposée attachée à cette courbe porterait une fraction rationnelle de t et ne saurait rester finie, ce qui est contradictoire.

On peut aussi consulter à ce propos le Mémoire de CLEBSCH, *Journal de Crelle*, t. **64**, p. 45, où l'on trouve le calcul du nombre des points doubles.

Pour obtenir la représentation il est commode d'employer un faisceau d'adjointes rencontrant la courbe en un seul point mobile, donc à coordonnées, fonctions rationnelles du paramètre.

LEMME I. — *Il n'y a pas d'adjointes d'ordre* $n - 3$.

En effet une courbe de degré $n - 3$ est déterminée par $\dfrac{n(n+3)}{2}$ points. Etant adjointe elle doit passer par les $\dfrac{(n-1)(n-2)}{2}$ points doubles, ce qui est contradictoire, car

$$n(n-3) < (n-1)(n-2) = n(n-3) + 2.$$

Ce raisonnement très simple soulève une objection. En effet, nous avons dénombré les points doubles comme s'ils étaient indépendants les uns des autres ; en réalité, ils sont considérés dans leur ensemble et il se pourrait que leur ensemble n'équivaille qu'à

$$\frac{(n-1)(n-2)}{2} - k,$$

points indépendants. Autrement dit, en employant le langage de la Géométrie algébrique, le groupe de tous les points doubles pourrait être un groupe spécial conduisant à des systèmes surabondants.

Il n'en est rien, car dans ce cas on aurait

$$\frac{n(n-3)}{2} \geqslant \frac{(n-1)(n-2)}{2} - k \qquad (k \geqslant 0),$$

et il existerait au moins une adjointe d'ordre $n-3$ et par suite une intégrale abélienne de 1re espèce, ce qui n'est pas. Nous rappelons qu'une intégrale de 1re espèce attachée à la courbe $f(x, y) = 0$ est de la forme

$$\int \frac{Q(x, y)dx}{f'y},$$

Q (x,y) étant un polynôme adjoint d'ordre $n-3$.

La démonstration basée sur la non-existence d'une intégrale abélienne suffit pour démontrer le lemme ; mais la 1re démonstration quoique insuffisante est intéressante par sa simplicité et la comparaison des deux montre que le groupe des points doubles est non spécial, propriété dont nous aurons besoin dans le théorème suivant, théorème III.

Théoreme III. — *Il y a deux faisceaux d'adjointes possibles :*

1er Faisceau. — *Adjointes d'ordre* $n-1$ *passant par* $2n-3$ *points fixes de la courbe.*

2e Faisceau. — *Adjointes d'ordre* $n-2$ *passant par* $n-3$ *points fixés de la courbe.*

Soient h le degré du faisceau et k le nombre de points fixes de la courbe autres que les points doubles par où passe le faisceau.

En exprimant que le faisceau est déterminé par ces points on a

$$\frac{h(h+3)}{2} - 1 = k + \frac{(n-1)(n-2)}{2}. \tag{1}$$

En exprimant que le faisceau rencontre la courbe en 1 seul point mobile on a

$$hn - 1 = k + (n-1)(n-2. \tag{2}$$

La résolution de ces deux équations donne

$$h_1 = n-1 \quad \text{et} \quad k_1 = 2n-3,$$
$$h_2 = n-2 \quad \text{et} \quad k_2 = n-3.$$

Ce résultat est mentionné dans le mémoire déjà cité de Clebsch.

Le raisonnement précédent ne prête pas à objection :

En effet, la seule critique serait que l'ensemble des points doubles n'équivaille qu'à un nombre de points doubles supposés pris isolément inférieur à $\frac{(n-1)(n-2)}{2}$ et nous avons vu qu'il n'en était rien.

Nous ne parlons que de représentation propre, ce qui ne restreint pas la généralité, car une représentation impropre se ramène à la précédente par un changement de paramètre [1].

[1] Pour l'étude de la rationnalité des points multiples, on se reportera à la note placée à la fin de ce travail.

DEUXIÈME PARTIE

ÉTUDE ALGÉBRIQUE

L'étude analytique précédente nous donne le moyen d'obtenir tous les points de la courbe unicursale. Il nous faut maintenant chercher s'il existe une infinité de points rationnels ou entiers en coordonnées homogènes et les obtenir si cela est.

THÉORÈME I. — *L'ensemble des courbes unicursales admettant une représentation rationnelle à coefficients entiers est identique à l'ensemble des courbes unicursales admettant une infinité de points entiers.*

1° Soit

$$(S) \qquad \begin{cases} X = f(u, v), \\ Y = g(u, v), \\ Z = h(u, v), \end{cases}$$

la représentation entière homogène. En faisant varier le couple u, v, on obtient une infinité de points entiers distincts.

2° Inversement, soient $n + 1$ points entiers arbitraires de la courbe. Les $n + 1$ systèmes (S) correspondants aux $n + 1$ valeurs du couple u, v forment $3n + 3$ équations linéaires par rapport aux $3n + 3$ coefficients des formes. La solution de ce système est bien rationnelle et on la rend entière en multipliant ces coefficients par le p. g. c. d. de leurs dénominateurs [1].

THÉORÈME II. — *La condition nécessaire et suffisante pour qu'une courbe unicursale ait une infinité de points entiers est qu'elle en ait au moins un distinct des points multiples.*

La condition est évidemment nécessaire, et nous donnerons de sa suffisance deux démonstrations.

[1] Au sujet de cette démonstration, on se reportera à la note placée à la fin de ce travail.

1re *Démonstration* : Soit A ce point entier. Les $\frac{(n-1)(n-2)}{2}$ points doubles forment un groupe rationnel dont les fonctions symétriques des coordonnées sont rationnelles. Les $n-2$ points d'intersection de la tangente en A avec la courbe forment un groupe rationnel ; il en est de même des $n-1$ points de rencontre de la courbe et d'une sécante rationnelle issue de A. Cela fait bien $2n-3$ points fixes et le faisceau d'ordre $n-1$ dont nous avons parlé est bien rationnel.

2e *Démonstration* : Puisque le groupe des points doubles est rationnel on peut obtenir des adjointes d'ordre $n-2$ à coefficients rationnels : elles ont d'ailleurs la multiplicité $n-2$.

Soient

$$P(x, y) = 0, \qquad Q(x, y) = 0, \qquad R(x, y) = 0,$$

les équations de 3 d'entre elles linéairement distinctes.

Effectuons la transformation

$$(T) \qquad \xi = \frac{P}{R}, \qquad \eta = \frac{Q}{R}.$$

1° La transformation (T) est bien birationnelle.

A 1 point x, y correspond 1 seul point ξ, η. Inversement, à 1 point ξ, η correspond 1 seul point x, y.

En effet, éliminons y entre les 3 équations

$$(E) \qquad \begin{cases} P - \xi R = 0, \\ Q - \eta R = 0, \\ f = 0, \end{cases}$$

$f(x, y) = 0$ étant l'équation de la courbe, ce qui donne deux résultantes :

$$F = 0 \qquad et \qquad F_1 = 0.$$

Eliminons x entre F et F_1 par la méthode du p. g. c. d. La dernière équation obtenue $F_p = 0$ ne contient pas x ; elle indique que les équations F et F_1 ont une solution commune. L'avant-dernière équation obtenue $F_{p-1} = 0$ est du premier degré en x. Elle définit x en fonction rationnelle à coefficients rationnels de ξ et η.

Si l'équation $F_{p-1} = 0$ se réduisait à une identité soit d'elle-même, soit en tenant compte de l'équation $F_{p=0}$, cela voudrait dire que les équations (E) ont 2 solutions communes toutes les fois qu'elles en ont une, c'est-à-dire que les adjointes

d'ordre $n - 2$ passant par un point fixe arbitraire de f passent toutes par un 2^e point fixe, ce qui n'est pas.

La transformation est donc bien birationnelle à coefficients rationnels.

A la courbe $f(x, y) = 0$ correspond la courbe $\varphi(\xi, \eta) = 0$. Son degré est égal au nombre des points d'intersection de φ avec la droite

$$a\xi + b\eta + c = 0,$$

ou de la courbe f avec le réseau

$$aP(x, y) + bQ(x, y) + cR(x, y) = 0,$$

c'est-à-dire à

$$n(n - 2) - (n - 1)(n - 2) = n - 2.$$

En continuant ainsi, on arrivera pour n impair à une cubique qui, ayant 1 seul point double, aura ce point double rationnel, pour n pair à une conique ayant un point rationnel correspondant à A. On coupera la cubique ou la conique par une droite rationnelle pivotant soit autour du point double, soit autour du point rationnel : cette droite rencontrera la courbe en 1 seul point mobile, donc rationnel.

Il y a donc bien une infinité de points rationnels.

On trouvera l'origine de ce raisonnement dans :

PICARD, *Traité d'Analyse*, t. II, p. 549 ;

POINCARÉ, *Journal de Mathématique*, 1901, p. 102.

Il nous suffit maintenant de savoir reconnaître à quelles conditions une conique admet un point entier.

Décomposition en carrés. — Elle est bien connue ; il suffit de la rappeler en insistant sur le fait que les transformations effectuées sont à coefficients rationnels.

Soit la conique d'équation

$$(1) \qquad ax^2 + bxy + cy^2 + dx + ey + f = 0 ;$$

1° Si $a = 0$ on a la solution

$$y = 0, \qquad dx + f = 0 ;$$

2° Si $a \not\equiv 0$ multiplions par $4a$. L'équation (1) s'écrit

$$(2ax + by + d)^2 + Dy^2 + 2(2ae - bd)y + 4af - d^2 = 0,$$

où

$$D = 4ac - b^2 ;$$

21) Si D = 0 on a la solution

$$\begin{cases} 2ax + by + d = 0, \\ 2(2ae - bd)y + 4af - d^2 = 0 ; \end{cases}$$

22) Si D $\not\equiv$ 0 multiplions par D et l'on a

$$D(2ax + by + d)^2 + [Dy + (2ae - bd)]^2 = 4aE,$$

et en coordonnées homogènes

$$D(2ax + by + dz)^2 + [Dy + (2ae - bd)z]^2 = 4aEz^2,$$

où

$$E = ae^2 + cd^2 + fb^2 - bde - 4acf.$$

Faisons la transformation

$$\begin{cases} 2dx + by + az = \xi, \\ Dy + (2ae - bd)z = \eta, \\ z = \zeta, \end{cases}$$

de déterminant $2a\ D \not\equiv 0$ et l'on obtient l'équation

$$D\xi^2 + \eta^2 - 4aE\zeta^2 = 0, \tag{2}$$

équivalentes au point de vue solutions entières, car les transformations que nous avons faites sont linéaires, à coefficients rationnels et par suite réversibles.

Equation réduite. — Nous allons transformer l'équation (2) de la façon suivante :

1° Soient :

$$D = Ap^2$$
$$-4aE = Cq^2,$$

A et C étant sans diviseurs carrés

L'équation (2) devient

$$AX^2 + Y^2 + CZ^2 = 0 \tag{3}$$

en posant

$$\text{(S)} \qquad \begin{cases} X = p\xi, \\ Y = \eta, \\ Z = q\zeta ; \end{cases}$$

2° Soient :

$$\begin{matrix} A = ad \\ C = cd \end{matrix} \qquad \text{où} \qquad d = (A, C).$$

L'équation (3) multipliée par d devient.

$$ax^2 + dy^2 + cz^2 = 0, \tag{4}$$

en posant

$$\text{(T)} \qquad \begin{cases} x = dX, \\ y = Y, \\ z = dZ. \end{cases}$$

Les coefficients a, d, c, jouissent de la double propriété suivante :
α) Ils sont sans diviseurs carrés car A et C le sont ;
β) Ils sont premiers entre eux 2 à 2 :

$(a, d) = 1$, car A est sans diviseur carré,
$(c, d) = 1$, » C » »
$(a, c) = 1$, puisque $d = (A, C)$;

Une telle équation prend le nom d'*équation réduite.*

Les transformations (S) et (T) sont réversibles : à toute solution rationnelle de (2) correspond une solution rationnelle de (4) et inversement. Il suffit donc de considérer l'équation réduite.

Nous renvoyons pour la démonstration du théorème suivant au livre de M. BACHMANN, *Zahlentheorie*, t. IV ; *Die Arithmetik der Quadratichen Formen*, p. 198.

THÉORÈME III. — *Les conditions nécessaires et suffisantes pour que l'équation réduite*

$$PX^2 + QY^2 + RZ^2 = 0$$

admette une solution entière sont que

— PQ soit reste quadratique de R,
— QR » » P,
— RP » » Q,

et P, Q, R, *non tous du même signe.*

Dans l'ouvrage cité ci-dessus on trouvera de plus le moyen d'obtenir un point entier.

Le problème algébrique de la recherche des points entiers est donc résolu et lorsqu'il est possible on abtient une représentation entière soit directement par la connaissance d'un point, soit par une suite de transformations birationnelles en utilisant la cubique ou la conique dernière transformée.

TROISIÈME PARTIE

ÉTUDE ARITHMÉTIQUE

CHAPITRE PREMIER

ÉTUDE GÉNÉRALE

Nous partons du système (S) de 3 formes de degré n définissant comme nous l'avons vu une courbe unicursale de degré n. Remarquons qu'une telle courbe est définie par

$$\frac{n(n+3)}{2}+1 \quad \text{coefficients,}$$

ce nombre étant diminué de

$$\frac{(n-1)(n-2)}{2} \quad \text{coefficients,}$$

correspondants aux points doubles et par suite par $3n$ coefficients. Il y a donc $3(n+1)-3n$ coefficients dont on peut disposer pour fixer le paramétrage sur la courbe unicursale ainsi définie. De plus, les coefficients de l'équation de la courbe obtenue par élimination de u et v peuvent être divisés par leur p. g. c. d. Il en résulte que l'étude générale que nous faisons ne permet pas de préciser tous les cas qui peuvent se produire dans la divisibilité de X, Y, Z par un facteur commun.

Dans ce chapitre nous nous contenterons de donner une borne supérieure de (X, Y, Z) et d'indiquer la marche à suivre pour dis-

tinguer entre les différentes solutions correspondantes à un même couple u, v.

L'objet du chapitre II est de donner une étude complète d'un cas particulier.

A) Recherche d'une limite de (X, Y, Z)

Théorème I. — *Lorsque u, v varie de façon arbitraire, la condition $(u, v) = 1$ étant satisfaite, le* p. g. c. d. *de* X, Y, Z *est nécessairement diviseur d'un nombre fixe, bien déterminé, indépendant de u et v.*

Autrement dit, (X, Y, Y) ne peut prendre qu'un nombre limité de valeurs.

Soit le système

$$(S)\qquad \begin{cases} X = au^n + bu^{n-1}v + \cdots + lv^n, \\ Y = a'u^n + \cdots, \\ Z = a''u^n + \cdots \end{cases}$$

Comme u et v sont premiers entre eux on peut répartir les facteurs premiers de (X, Y, Z) en 2 groupes :

1° Ceux qui sont premiers avec u

2° Ceux qui sont premiers avec v.

Un même facteur premier peut appartenir aux 2 groupes, mais tous ont été considérés, ce qui nous suffit.

Soit p^m la puissance maximum d'un facteur premier figurant dans (X, Y, Z) pour tout couple choisi u, v, le facteur p étant supposé premier à v.

Nous pouvons poser

$$u \equiv \alpha v \pmod{p},$$

et le fait que

$$p^m \mid X, Y, Z,$$

s'écrit

$$\left.\begin{array}{l} v^n(a\alpha^n + \cdots + l) \\ v^n(a'\alpha^n + \cdots + l') \\ v^n(a''\alpha^n + \cdots + l'') \end{array}\right\} \equiv 0 \pmod{p^m},$$

ou

$$(1)\qquad \left.\begin{array}{l} a\alpha^n + \cdots + l \\ a'\alpha^n + \cdots + l' \\ a''\alpha^n + \cdots + l'' \end{array}\right\} \equiv 0 \pmod{p^m}.$$

Résolvons le système (1), par rapport à α^n, α^{n-1} et α^{n-2}, ce qui se fait linéairement. Nous avons

$$(2)\qquad \begin{cases} D\alpha^n + A\alpha^{n-3} + \cdots + L \\ D\alpha^{n-1} + A'\alpha^{n-3} + \cdots + L' \\ D\alpha^{n-2} + A''\alpha^{n-3} + \cdots + L'' \end{cases} \equiv 0 \pmod{p^m}.$$

En multipliant la 3e équation par α et la soustrayant de la 2e et en opérant de même avec la 2e et le 1re nous obtenons

$$\begin{matrix} A\alpha^{n-2} + B\alpha^{n-3} + \cdots + L \\ A'\alpha^{n-2} + B'\alpha^{n-3} + \cdots + L' \\ A''\alpha^{n-2} + \cdots \end{matrix} \equiv 0 \pmod{p^m}.$$

En poursuivant ainsi on arrivera soit à un système du 1er degré, soit à un du 2e.

1er Cas : *système linéaire*

$$\begin{matrix} a\alpha + b \\ a'\alpha + b' \\ a''\alpha + b'' \end{matrix} \equiv 0 \pmod{p^m}.$$

Ces 3 congruences ne sont compatibles que si p^m / les 3 mineurs.

$$C = a'b'' - b'a'', \qquad C' \quad \text{et} \quad C'',$$

donc

$$p^m / (C, C', C''),$$

(C, C', C'') est donc une borne supérieure des diviseurs du 2e groupe.

2e Cas : *système quadratique*

$$\begin{matrix} a\alpha^2 + b\ \alpha + c \\ a'\alpha^2 + b'\alpha + c' \\ a''\alpha^2 + b''\alpha + c'' \end{matrix} \equiv 0 \pmod{p^m},$$

d'où nous déduisons en résolvant par rapport à α^2, α et 1.

$$D\alpha^2 \equiv D\alpha \equiv D \equiv 0 \pmod{p^m}.$$

Dans ce cas

$$D = | ab'c'' |$$

est une borne supérieure des diviseurs du 2e groupe.

En étudiant les diviseurs du 1er groupe on obtiendra une nouvelle borne supérieure et le produit de ces 2 bornes sera une borne supérieure de (X, Y, Z).

B) Problème inverse

Les transformations que nous venons de faire ne sont pas nécessairement réversibles. Il importe de reconnaître si un diviseur de la borne supérieure qui est un diviseur logiquement possible de (X, Y, Z) est un diviseur effectif pour un couple choisi u, v.

Nous allons étudier cette réciproque du théorème I successivement :

1° Dans le cas linéaire ;
2° Dans les cas quadratique ;
3° Dans le cas général.

I. — *Etude du système linéaire*

$$(S) \qquad \begin{cases} X = au + bv \\ Y = a'u + b'v \\ Z = a''u + b''v \end{cases} \qquad (u, v) = 1,$$

a, a', a'', b, b', b'', peuvent être supposés premiers dans leur ensemble, car s'ils admettaient un p. g. c. d. D, on partirait de la représentation

$$\frac{X}{D}, \quad \frac{Y}{D}, \quad \frac{Z}{D}.$$

1° Soit p un diviseur premier de (C, C', C'') supposé diviseur de (X, Y, Z) et supposé divisant v.

Alors

$$p \mid a, a', a''$$

et réciproquement un tel p doit diviser v puisque $p \nmid (b, b', b'')$.

Par analogie $q \mid u$ si et seulement si $q \mid b, b'$ et b''.

2° Supposons maintenant que $p \nmid vu$ et soit

$$u \equiv \alpha v \pmod{p},$$

d'où

$$\left.\begin{matrix} a\alpha + b \\ a'\alpha + b' \\ a''\alpha + b'' \end{matrix}\right\} \equiv 0 \pmod{p},$$

congruences compatibles puisque

$$C \equiv C' \equiv C'' \equiv 0 \pmod{p}.$$

L'un des 3 nombres a, a' et a'' au moins n'est pas nul (mod. p) soit a celui-là. Alors b aussi est différent de zéro (mod. p) car la 1re congruence donnerait

$$\alpha \equiv 0 \quad \text{ou} \quad u \equiv 0 \pmod{p},$$

solution que nous avons écartée. La congruence

$$a\alpha + b \equiv 0$$

définit donc α et cette valeur de α satisfait aux deux autres congruences.

Nous ferons le changement de paramètre suivant

$$au + b\nu \equiv 0 \pmod{p},$$

ce qui peut s'écrire

$$Au + B\nu = ps,$$

en posant

$$\begin{aligned} a &= A(a, b), \\ b &= B(a, b), \end{aligned}$$

puisque $p \nmid (a, b)$ avec $(A, B) = 1$.

Nous pouvons trouver deux entiers C et D tels que

$$AD - BC = 1,$$

et par suite poser

$$Cu + D\nu = t,$$

d'où

$$\text{(T)} \qquad \left\{\begin{aligned} u &= Dps - Bt, \\ \nu &= -Cps + At. \end{aligned}\right.$$

Alors

$$p \mid (X, Y, Z).$$

En posant

$$\begin{aligned} u &= Dp^r s - Bt, \\ \nu &= -Cp^r s + At, \end{aligned}$$

on verra quelle puissance de p figure dans (X, Y, Z).

Le nombre des transformations est limité puisque l'on a une borne supérieure de (X, Y, Z).

On pourrait aussi utiliser les identités

$$a'(au + bv) - a(a'u + b'v) = v(a'b - b'a),$$
$$b'(au + bv) - b(a'u + b'v) = u(ab' - ba'),$$

pour déterminer la puissance de p dans $a'u + b'v$ connaissant celles de p dans $au + bv$ et dans $ab' - ba'$ et deux autres analogues relatives à $a''u + b''v$.

II. — *Etude du système quadratique*

$$(S) \qquad \begin{cases} X = au^2 + buv + cv^2 \\ Y = a'u^2 + b'uv + c'v^2 \\ Z = a''u^2 + b''uv + c''v^2 \end{cases} \qquad (u, v) = 1.$$

Pour la raison déjà donnée, les 9 coefficients peuvent être supposés premiers dans leur ensemble

Soit p un diviseur premier de D supposé diviseur de (X, Y, Z). On peut supposer :

1er Cas : p/v. — Alors $p/a, a', a''$

et réciproquement un tel p est diviseur de $\Delta(X, Y, Z)$ si et seulement si

$$p \,/\, v(bu + cv) \;\; ; \;\; v(b'u + c'v) \;\; ; \;\; v(b''u + c''v),$$

condition satisfaite soit par

(11) $\quad p \,/\, v,$

(12) $\quad p \,/\, bu + cv \;\; ; \;\; b'u + c'v \;\; ; \;\; b''u + c''v,$

(13) $\quad p \,/\, v \;\; et \;\; p \,/\, bu + cv \;\; ; \;\; b'u + c'v \;\; ; \;\; b''u + c''v.$

Dans chacun de ces cas nous remplaçons le couple u, v par un couple s, t, par une transformation homographique comme dans le cas du système linéaire.

2e Cas : $p \nmid v$. — Posons alors

$$u \equiv \alpha v \pmod{p},$$

et nous devons avoir

$$(S) \qquad \begin{cases} a\alpha^2 + b\alpha + c \\ a'\alpha^2 + b'\alpha + c' \\ a''\alpha^2 + b''\alpha + c'' \end{cases} \equiv 0 \pmod{p}.$$

Aucun a n'est nul (mod p). — En éliminant α^2 entre ces congruences, on obtient

$$\left.\begin{array}{l} C\alpha - B \\ C'\alpha - B' \\ C''\alpha - B'' \end{array}\right\} \equiv 0.$$

Ces 3 congruences sont compatibles car en éliminant α entre elles on obtient

$$CB' - BC' = a''D \equiv 0 \quad \textit{et} \quad \cdots$$

11) *L'un des C n'est pas nul* (mod p). — Par exemple C.
La 1re congruence (4) donne

$$\alpha \equiv \frac{B}{C}.$$

Cette valeur de α satisfait à la 1re congruence (S).

$$a\alpha^2 + b\alpha + c \equiv 0,$$

si et seulement si

$$aB^2 + bBC + cC^2 \equiv 0,$$

ce qui s'écrit, en tenant compte de

$$aA + bB + cC = D \equiv 0,$$

$$a(B^2 - AC) \equiv 0,$$

ou

$$B^2 - AC \equiv 0 \qquad \text{car} \qquad p \nmid a$$

Mais alors si $B^2 - AC \equiv 0$, les 2 dernières congruences (S) ont leur résultant nul (mod p) et ont une solution commune qui est précisément cette valeur α.
La condition $B^2 - AC \equiv 0$ est donc nécessaire et suffisante pour que $p \mid (X, Y, Z)$.

12) *Les* 3 C *sont nuls* (mod p). — Si les 3 A ne sont pas tous nuls (mod p) nous poserons

$$\nu \equiv \beta u \pmod{p}$$

et le système (4) deviendra

$$\left.\begin{array}{l} A\beta - B \\ \cdots\cdots \\ \cdots\cdots \end{array}\right\} \equiv 0,$$

qui nous ramène à un cas déjà étudié.
— Si les 3A sont nuls.

121) *Soit l'un des* b $\not\equiv$ o. — Par exemple b.

Les congruences A, A′ A″, C, C′ C″ résolues par rapport à b donnent :

$$\text{car} \quad A'' = bc' - cb' \equiv 0 \quad \text{peut s'écrire} \quad \frac{b'}{b} \equiv \frac{c'}{c},$$

$$\begin{cases} \frac{a'}{a} \equiv \frac{b'}{b} \equiv \frac{c'}{c}, \\ \frac{a''}{a} \equiv \frac{b''}{b} \equiv \frac{c''}{c}, \end{cases}$$

et les 3 congruences (S) se réduisent à une seule.

122) *Les* 3b *sont* $\equiv 0$. — Le système (S) devient

$$(\Sigma) \qquad \begin{cases} ax^2 + c \\ a'x^2 + c' \\ a''x^2 + c'' \end{cases} \equiv 0,$$

résoluble seulement si

$$ac' - ca' \equiv a'c'' - c'a'' \equiv ac'' - ac'' \equiv 0,$$

ce qui s'écrit

$$\frac{a''}{a} \equiv \frac{c''}{c} \quad \text{et} \quad \frac{a'}{a} \equiv \frac{c'}{c},$$

puisque p ne divise aucun a.

Les 3 congruences se réduisent à une seule par exemple à la 1re qui est possible si et seulement si $-ac$ est reste quadratique de p.

2) *Un ou plusieurs* a *sont nuls, aucun* c *ne l'est* (mod p).

Nous poserons

$$v \equiv \beta u \pmod{p},$$

et les congruences (S) deviendront

$$\begin{cases} c\beta^2 + b\beta + a \\ \cdots\cdots\cdots\cdots \end{cases} \equiv 0,$$

analogues à celles que nous venons de résoudre

3) *Un a est nul par exemple* $a \equiv 0 \pmod{p}$.

Les systèmes (S) et (L) deviennent

$$(S_1) \qquad \begin{cases} b\alpha + c \\ a'\alpha^2 + b'\alpha + c' \\ a''\alpha^2 + b''\alpha + c'' \end{cases} \equiv 0 \pmod{p},$$

et

$$C\alpha - B \equiv 0.$$

Les congruences (S_1) n° 1 et (L_1) sont compatibles, car leur résultant est

$$bB' + cC = D - aA \equiv 0 \qquad (\text{car } p \nmid a).$$

Les 2 dernières congruences (S_1) sont compatibles si, et seulement si, leur résultant

$$B^2 - AC \equiv 0, \pmod{p}.$$

Leur solution commune dans ce cas est la valeur de α précédemment considérée.

4) *Deux a sont nuls, par exemple,* $a' \equiv a'' \equiv 0 \pmod{p}$.
Le système (S) devient

$$(S_3) \qquad \begin{cases} ax^2 + b\alpha + c \\ b'\alpha + c' \\ b''\alpha + c'' \end{cases} \equiv 0.$$

Les 2 dernières congruences sont compatibles car leur résultant est A et l'on a

$$aA + a'A' + a''A'' \equiv D \equiv 0,$$

et

$$a' \equiv a'' \equiv 0 \pmod{p} \qquad \text{et} \qquad a \not\equiv 0,$$

donc

$$A \equiv 0.$$

Donc p divise (X, Y, Z) si, et seulement si, cette valeur de α satisfait à $a\alpha^2 + b\alpha + c \equiv 0$, c'est-à-dire si

$$a'c''^2 - bb''c'' + cb''^2 \equiv 0 ;$$

5) *Les trois a sont nuls* (mod p).
Le système (S) se réduit à un système linéaire dont nous avons déjà fait l'étude.
Remarquons d'ailleurs que les cas 3), 4) et 5) se simplifient du fait que 1 ou plusieurs c sont alors $\equiv 0 \pmod{p}$.

Dans un exemple numérique, on aura avantage à déterminer une borne supérieure de (X, Y, Z) inférieure à celle donnée.

Soient

$$(A, A', A'') = d_1,$$
$$(B, B', B'') = d_2,$$
$$(C, C', C'') = d_3.$$

Pour résoudre le système (S) par rapport à u^2, uv, v^2 il suffit de multiplier les équations respectivement par

$$\frac{A}{d_1}, \cdots ; \quad \frac{B}{d_2}, \cdots ; \quad \frac{C}{d_3} \cdots,$$

ce qui donne

$$(X, Y, Z) \mid \begin{cases} \frac{D}{d_1} u^2, \\ \frac{D}{d_2} uv, \\ \frac{D}{d_3} v^2. \end{cases}$$

Soit Δ le p. p. c. m. de $\frac{D}{d_1}, \frac{D}{d_2}, \frac{D}{d_3}$.

Alors

$$(X, Y, Z) \mid \Delta u^2, \Delta uv, \Delta v^2.$$

Soit (X, Y, Z) maximum $= p^m \cdots$

p^m est premier certainement à l'un des deux nombres u^2 ou v^2 ou moins. Donc

$$p^m \mid \Delta,$$

et par suite Δ est une borne supérieure de (X, Y, Z).

Dans chacun des cas étudiés nous remplacerons le couple u, v par un transformé homographique s, t. La recherche de la puissance avec laquelle p figure dans (X, Y, Z) s'effectue comme dans le cas linéaire.

III. — Etude du système général

Nous pouvons toujours supposer

1) p/v. — Alors p/a, a', a''

Réciproquement un tel p est diviseur de (X, Y, Z) si et seulement si

$$p \mid \begin{cases} v(bu^{n-1} + \cdots), \\ v(b'u^{n-1} + \cdots), \\ v(b''u^{n-1} + \cdots). \end{cases}$$

Ces conditions sont satisfaites soit par

(11) $p \mid \rho$,

(12) $p \mid (bu^{n-1} + \cdots)$; $(b'u^{n-1}$; $(b''u^{n-1} + \cdots)$,

(13) $p \mid \rho$ et $bu^{n-1} + \cdots$; $b'u^{n-1} + \cdots$; $b''u^{n-1} + \cdots$

Les cas 11) et 13) se traitent immédiatement, le cas 12) se ramène à un cas analogue de degré moins élevé et se résout de proche en proche.

2) $p \nmid \rho$. — Nous arrivons comme nous l'avons déjà expliqué à un système linéaire ou à un système quadratique donnant une seule valeur de α. Si cette valeur de α satisfait aux 3 congruences alors

$$p \mid (X, Y, Z)$$

et l'on pourra remplacer le couple u, ρ par un couple transformé homographiquement s, t.

Nous terminerons cette étude générale en faisant remarquer que les seules opérations que nous avons été amené à faire sont des transformations homographiques portant sur le couple u, ρ, ce qui est bien en accord avec les résultats de l'étude analytique.

L'objet du chapitre II est de dénombrer et distinguer toutes les valeurs de (X, Y, Z) pour l'équation réduite

$$PX^2 + QY^2 + RZ^2 = 0.$$

CHAPITRE II

ÉQUATION RÉDUITE $PX^2 + QY^2 + RZ^2 = 0$.

L'application de la méthode générale n'offre aucune difficulté. Aussi, la modifions-nous afin de donner une solution indépendante des théories générales précédentes.

En coupant la conique précédente par une droite rationnelle pivotant autour d'un point rationnel ξ, η, ζ on obtiendra 1 seul point mobile, donc rationnel.

A une droite rationnelle (de paramètre $\frac{u}{v}$ rationnel) correspond 1 seul point rationnel et inversement. D'ailleurs, si l'on change de point de départ, le paramètre $\frac{u}{v}$ sera changé en un paramètre $\frac{S}{t}$ en correspondance homographique avec le premier. La méthode indiquée conduit donc à toutes les solutions et cela quelle que soit la solution première supposée connue.

Soit ξ, η, ζ une solution connue avec

$$(\xi, \eta, \zeta) = 1.$$

Posons

$$\text{(T)} \qquad \begin{cases} X = \xi + \lambda u, \\ Y = \eta + \lambda v, \\ Z = \zeta, \end{cases}$$

ζ étant prise comme variable d'homogénéité.

Nous obtenons alors

$$\lambda^2 C + 2\lambda D = 0,$$

avec

$$C = Pu^2 + Qv^2,$$
$$D = Pu\xi + Qv\eta,$$

et en reportant ces valeurs dans le système (T) après avoir chassé les dénominateurs, nous obtenons la solution

$$(S) \qquad \begin{cases} X = \xi C - 2uD \\ Y = \eta C - 2vD \\ Z = \zeta C \end{cases} \qquad (u, v) = 1.$$

Signalons de suite le lemme suivant que nous utiliserons fréquemment.

LEMME. — *Les* 3 *nombres* $P\xi$, $Q\eta$, $R\zeta$ *sont premiers deux à deux.*

Rappelons que d'après la définition de la forme réduite P, Q R sont premiers 2 à 2 et sans diviseurs carrés.

1) ξ et η par exemple, sont premiers entre eux, car si l'on avait

$$\delta = (\xi, \eta),$$

on aurait

$$\delta^2 / R\zeta^2,$$

ce qui n'est pas
car R est sans diviseur carré et $(\delta, \xi) = 1$ d'après la condition $(\xi, \eta, \zeta) = 1$.

2) P et ζ par exemple, sont premiers entre eux car l'hypothèse

$$(P, \zeta) = d,$$

entraîne

$$d / Q\eta^2,$$

ce qui est impossible
puisque

$$(P, Q) = 1 \qquad \text{et} \qquad (\zeta, \eta) = 1.$$

Ce lemme établi, les formes C et D semblent devoir jouer un rôle important, que nous allons indiquer.

THÉORÈME I. — *Les facteurs premiers de* (X, Y, Z) *sont les mêmes que ceux de* (C, 2D).

En se reportant au système (S) on voit de suite que tout nombre divisant C et 2D divise X, Y, Z.

Réciproquement soit p un facteur premier de (X, Y, Z) supposé ne pas diviser (C, 2D). Les seules hypothèses à faire sont :

1) $p/2D$ et $p \nmid C$. — Ce qui entraîne

$$p / \xi, \eta \text{ et } \zeta,$$

divisibilité impossible car $(\xi, \eta, \zeta) = 1$.

2) p/C et $\not| 2D$. — D'où l'on déduit

$$p \mid u \text{ et } v,$$

ce qui n'est pas car $(u, v) = 1$.

3) $p \not| C$ *et* $\not| 2D$. — Comme p/Z on a p/ζ et par suite

$$P\xi^2 + Q\eta^2 \equiv 0 \pmod{p}. \tag{1}$$

Le système

$$\begin{matrix} \xi C - 2uD \\ \eta C - 2vD \end{matrix} \equiv 0 \pmod{p},$$

donne

$$\frac{\xi}{u} \equiv \frac{\eta}{v} \pmod{p},$$

ce qui transforme la congruence (1) dans les deux suivantes

$$\begin{matrix} P\xi u + Q\eta v \\ Pu^2 + Qv^2 \end{matrix} \equiv 0 \pmod{p},$$

c'est-à-dire

$$C \equiv D \equiv 0 \pmod{p}.$$

Cette troisième hypothèse est encore inadmissible, ce qui démontre le théorème.

THÉORÈME II. — *Lorsque le couple* u, v *varie de façon arbitraire sous la condition* $(u, v) = 1$, *le p. g. c. d. de* X, Y, Z, *est un diviseur de*

$$2PQ(P\xi^2 + Q\eta^2) = D.$$

Le système (S) admet la combinaison entière

$$\eta X + \xi Y = -2uv(P\xi^2 + Q\eta^2).$$

Considérons un couple particulier arbitraire u, v et soit $\rho^\alpha \cdots$ le diviseur maximum de u divisant (X, Y, Z).

En se reportant au système (S) on voit que

$$\rho^\alpha \mid Q\xi v^2, \quad Q\eta v^2, \quad Q\zeta v^2.$$

Or $p \not| v$ car $(u, v) = 1$.

De plus $\rho \mid \xi, \eta, \zeta$ à la fois.

Donc

$$\rho^\alpha \mid Q.$$

Le même raisonnement s'applique à tout diviseur premier r de ν et à tout diviseur premier de u ou de ν pour un couple quelconque u, ν.

On a donc

$$\rho^{\alpha} \cdots / Q,$$
$$r^{\beta} \cdots / P,$$

et comme $(u, \nu) = 1$, les ρ et les r sont différents et l'on a bien

$$\underset{\text{maxima}}{\rho^{\alpha} \cdots r^{\beta}} / QP,$$

et par suite

$$(X, Y, Z) / 2PQ(P\xi^2 + Q\eta^2).$$

Les deux théorèmes précédents indiquent seulement les diviseurs logiquement possibles de (X, Y, Z) pour l'ensemble des couples u, ν. Ils indiquent des conditions nécessaires mais non obligatoirement suffisantes pour obtenir un diviseur du nombre (X, Y, Z) correspondant à un couple déterminé (u, ν). Il nous faut maintenant considérer un couple u, ν donné et déterminer les facteurs premiers de (X, Y, Z) et leurs exposants.

Nous classerons ces facteurs premiers en 4 groupes :

1er *groupe*, ceux de P ;

2e *groupe*, ceux de Q ;

3e *groupe*, ceux de $P\xi^2 + Q\eta^2 = -R\zeta^2$,

En excluant chaque fois le facteur 2 s'il s'y trouve ;

4e *groupe*, le facteur 2.

Une première réponse nous est fournie par le théorème suivant.

THÉORÈME III. — *Pour qu'un facteur premier* ρ *de* D *divise* (X, Y, Z) *il faut et il suffit que*

ρ / ν	si	ρ / P	($\rho = 2$ compris)
ρ / u	si	ρ / Q	»
$\rho / \nu\xi - u\eta$	si	$\rho / P\xi^2 + Q\eta^2$	»

et enfin quand

$$\rho = 2 \text{ } / \text{ } PQ(P\xi^2 + Q\eta^2),$$

que

$$2 / u + \nu.$$

1) Pour qu'un facteur premier p de P divise (X, Y, Z) il faut et il suffit que p/ν,

car il faut et il suffit que

$$p \mid \begin{cases} Q\xi\rho^2 - 2Q\eta u\rho, \\ - Q\eta\rho^2, \\ Q\zeta\rho^2. \end{cases}$$

Or $p \nmid Q$ et $p \nmid \zeta$.
Donc p/ρ^2 et par suite p/ρ.
2)
3) Pour qu'un facteur premier ρ de $P\xi^2 + Q\eta^2$ divise (X, Y, Z). il faut et il suffit que

$$\rho \mid \rho\xi - u\eta. \tag{1}$$

On pourrait prendre la condition

$$\rho \mid D = P\xi u + Q\eta\rho \tag{2}$$

mais la précédente est plus simple.

31) **La condition est nécessaire.** — En effet les deux formes (1) et (2) sont équivalentes (mod ρ) car leur résultant est $P\xi^2 + Q\eta^2$ qui est nul (mod ρ).
On peut aussi remarquer que l'on a

$$u(P\xi^2 + Q\eta^2) - \xi(P\xi u + Q\eta\rho) = Q\eta(u\eta - \rho\xi),$$

ρ doit donc diviser $Q\eta$ $(u\eta - \rho\xi)$ et comme il est premier avec $Q\eta$ (voir lemme), on a nécessairement

$$\rho \mid \rho\xi - u\eta.$$

32) **La condition est suffisante.** — En effet posons

$$u \equiv \alpha\rho \pmod{p},$$

la condition (1) donne

$$\alpha \equiv \frac{\xi}{\eta} \pmod{p},$$

et l'on a bien

$$\begin{aligned} C &\equiv \rho^2(P\alpha^2 + Q) \equiv \rho^2(P\xi^2 + Q\eta^2) \\ D &\equiv \rho(P\xi\alpha + Q\eta) \equiv \rho(P\xi^2 + Q\eta^2) \end{aligned} \equiv 0 \pmod{p}.$$

4) Pour que $2/(X, Y, Z)$ il faut et il suffit que

$$2 \mid C = Pu^2 + Q\eta^2,$$

car $2 \nmid \xi, \eta, \zeta$ à la fois.

Cette divisibilité se simplifie

41) Si $2/Q$ elle est quivalente à $2/u$.

42) Si $2/P$ elle est équivalente à $2/\rho$.

43) Si $2 \nmid PQ$, on a

$$P \equiv Q \equiv 1 \pmod{p},$$

et

$$Pu^2 + Q\rho^2 \equiv u^2 + \rho^2,$$

et d'après le théorème de Format

$$u^2 + \rho^2 \equiv u + \rho.$$

44) Si $2/P\xi + Q\eta^2 = -R\zeta^2$.
ξ et η sont impairs (voir lemme) et les deux conditions

$$\left.\begin{array}{l} 2/u + \rho \\ 2/\rho\xi + u\eta \end{array}\right\} \text{ sont équivalentes.}$$

Ainsi le facteur 2 s'il entre dans les trois premiers groupes joue le même rôle que les autres facteurs, ce qui justifie l'addition « $\rho = 2$ compris ».

THÉORÈME IV. — *L'exposant d'un facteur premier de* (X, Y, Z) *se détermine à l'aide du système* (E).

$$\text{(E)} \qquad \begin{aligned} \xi X &= Q(\eta u - \rho\xi)^2 - u^2(P\xi^2 + Q\eta^2), \\ \eta Y &= P(\eta u - \rho\xi)^2 - \rho^2(P\xi^2 + Q\eta^2), \\ \xi\eta Z &= \zeta(\eta u - \rho\xi)(P\xi u - Q\eta\rho) + \zeta u\rho(P\xi^2 + Q\eta^2). \end{aligned}$$

1) et 2) Les facteurs premiers de P et Q ayant seulement l'exposant 1, il n'y a aucun doute.

3) L'utilité du système (E) est de mettre en évidence la forme $\rho\xi - u\eta$. Remarquons qu'un diviseur du 3e groupe ne divise pas $\xi\eta$. Donc s'il divise ξX, ηY, $\xi\eta Z$ il divisera (X, Y, Z). De plus on a

$$\text{(1)} \qquad P\xi u - Q\eta\rho \not\equiv 0 \pmod{\rho},$$

car de

$$\rho\xi - u\eta \equiv 0 \pmod{\rho}$$

on déduit

$$\frac{\rho}{u} \equiv \frac{\eta}{\xi},$$

et la non congruence (1) s'écrit

$$P\xi^2 - Q\eta^2 \not\equiv 0,$$

ce qui est puisque l'on a

$$P\xi^2 + Q\eta^2 \equiv 0,$$

et que

$$\rho \nmid 2P\xi^2 \quad \text{et} \quad 2Q\eta^2.$$

Ceci posé soient

$$R = r_1 r_2 \cdots \lambda_1 \lambda_2 \cdots,$$
$$\zeta = \rho_1^{\alpha_1} \rho_2^{\alpha_2} \cdots \lambda_1^{\beta_1} \lambda_2^{\beta_2} \cdots$$

les λ étant seuls communs à R et ζ d'où

$$R\zeta^2 = r_1 r_2 \cdots \lambda_1^{2\beta_1+1} \cdots \rho_1^{2\alpha_1} \cdots$$

31) Si nous posons

$$(311) \qquad \begin{matrix} \nu\xi - u\eta \equiv 0 \pmod{\rho^{\gamma}} \\ \nu\xi - u\eta \not\equiv 0 \pmod{\rho^{\gamma+1}} \end{matrix} \qquad (\gamma < \alpha),$$

nous aurons

$$\rho^{2\gamma} / X \text{ et } Y \quad \text{car} \quad \rho^{2\gamma} / (\nu\xi - u\eta)^2 \quad \text{et} \quad P\xi^2 + Q\eta^2,$$
$$\rho^{2\gamma} / Z \quad \text{car} \quad \rho^{\gamma} / \zeta \quad \text{et} \quad \nu\xi - u\eta.$$

De plus

$$\rho^{2\gamma+1} / P\xi^2 + Q\eta^2 \quad \text{et} \quad \nmid (\nu\xi - u\eta)^2.$$

Donc $\rho^{2\gamma+1} \nmid X\ Y$

$$(X, Y, Z) = \rho^{2\gamma} \cdots$$

312) Si $\gamma = \alpha$ on atteint la limite supérieure 2α pour l'exposant de ρ et l'on a encore

$$(X, Y, Z) = \rho^{2\gamma} \cdots$$

Il n'est pas inutile de montrer directement que ρ ne peut avoir un exposant supérieur à 2α.

En effet $\xi\eta Z$ contient ρ à l'exposant 2α pour la partie $\zeta(\eta u - \nu\xi)(P\xi u - Q\eta\nu)$ et à l'exposant $\alpha + 2\alpha$ pour la partie $\zeta u\nu\ (P\xi^2 + Q\eta^2)$ donc seulement à l'exposant 2α.

313) Si $\gamma > \alpha$ ξX a une partie divisible par $\rho^{2\gamma}$ et l'autre seulement par $\rho^{2\alpha}$ donc

$$(X, Y, Z) = \rho^{2\alpha} \dots$$

ce qui est en accord avec la limite supérieure donnée par le théorème II.

32) Si nous posons de même

$$(312) \qquad \begin{aligned} \nu\xi - u\eta &\equiv 0 \pmod{\lambda^{\delta}} \\ \nu\xi - u\mu &\not\equiv 0 \pmod{\lambda^{\delta+1}} \end{aligned} \qquad (\delta \leqslant \beta),$$

l'exposant de λ sera 2δ dans (X, Y, Z).

$$(X, Y, Z) = \lambda^{2\delta} \dots$$

313) Si l'on fait

$$\delta \geqslant \beta + 1,$$

on trouve immédiatement

$$(X, Y, Z) = 2^{2\beta+1} \dots$$

ce qui est encore en accord avec la limite supérieure.

33) Les r ne figurant qu'avec l'exposant 1 il n'y a aucun doute

4) La discussion relative au facteur 2 se conduit de façon analogue, mais elle est beaucoup plus délicate.

41) $2 \mid PQ(P\xi^2 + Q\eta^2)$. — Alors 2 n'entre dans D qu'à la puissance 1, il n'y a aucun doute.

42) $2/P$. — On a par suite (voir lemme).

$$D = 2^2 \cdots, \qquad P = 2P', \qquad P' \text{ impair},$$

et nous devons poser $\nu = 2S$.

On a alors

$$\frac{Y}{2} = \eta(P'u^2 + 2Qs^2) - 4s(P'\xi u + Q\eta s).$$

Comme u est impair puisque $(u, \nu) = 1$, $2 \nmid \frac{Y}{2}$ car η et P' sont impairs.

$$(X, Y, Z) = 2 \cdots$$

43) $2/Q$. — La conclusion est analogue.

44) $2/R\xi^2$. — Rappelons que

$$2 \nmid PQ\xi\eta u\nu$$

et que nous devons poser

$$\nu\xi - u\eta \equiv 0 \pmod 2.$$

Mais ici on a

$$P\xi u - Q\eta\nu \equiv 0 \pmod 2,$$

tandis que dans le cas 3 analogue on avait

$$P\xi u - Q\eta\nu \not\equiv \pmod \rho.$$

La discussion est plus délicate à cause de l'exposant inconnu *a priori* γ de 2 dans $P\xi u - Q\eta\nu$.

Nous nous reportons au système (E) que nous récrivons

$$(E) \qquad \begin{cases} \xi X = Q(\eta u - \nu\xi)^2 - u^2(P\xi^2 + Q\eta^2), \\ \eta Y = P(\eta u - \nu\xi)^2 - \nu^2(P\xi^2 - Q\eta^2), \\ \xi\eta Z = \zeta(\eta u - \nu\xi)(P\xi u - Q\eta\nu) + \zeta u\nu(P\xi^2 + Q\eta^2). \end{cases}$$

441) $2 \mid \zeta$, $2/R$. — $R = 2R'$, R' impair.

Alors

$$4 \nmid P\xi^2 + Q\eta^2 \qquad \text{et} \qquad 4 \mid (\nu\xi - u\eta)^2.$$

Donc

$$(X, Y, Z) = 2 \cdots$$

442) $\zeta = 2^\alpha \cdots$ $2 \nmid R$. — D'où $2\ R\zeta^2 = 2^{2\alpha+1} \cdots$

Posons

$$(4421) \qquad \begin{matrix} \nu\xi - u\eta \equiv 0 & \pmod{2^\beta} \\ \nu\xi - u\eta \not\equiv 0 & \pmod{2^{\beta+1}} \end{matrix} \qquad (\beta < \alpha),$$

ξX contient 2 avec l'exposant 2β dans le terme $Q(\nu\xi - u\eta)^2$ et 2α dans le terme $P\xi^2 + Q\eta^2$ donc seulement avec l'exposant 2β car $\beta < \alpha$.

$\eta Y \cdots$

$\xi\eta Z$ contient 2 avec l'exposant $\alpha + \beta + \gamma$ dans le 1er terme et 3α dans le 2e, donc avec l'exposant 2β au moins

$$(X, Y, Z) = 2^{2\beta} \cdots$$

4422) Soit maintenant $\beta = \alpha$.

$(\eta u - \nu\xi)^2$ et $P\xi^2 + Q\eta^2$ ont 2 avec l'exposant 2α ; Q et u^2 sont impairs. Donc ξX a 2 avec un exposant au moins égal à $2\alpha + 1$.

Il en est de même pour ηY et de même pour $\eta\xi Z$. Comme l'exposant de 2 ne peut dépasser $2\alpha + 1$ d'après le théorème II, on a bien

$$(X, Y, X) = 2^{2\alpha+1}.$$

Il n'est pas inutile de démontrer directement que ξX ou ηY ont le facteur 2 seulement à l'exposant $2\alpha + 1$.

En effet de

$$P\xi^2 + Q\eta^2 = 2^{2\alpha} \cdots,$$

on tire

$$P + Q \equiv 0 \pmod 4,$$

puisque ξ^2 et η^2 impairs sont $\equiv 1 \pmod 4$.

Le quotient de $P\xi^2 + Q\eta^2$ par $2^{2\alpha}$ est impair.

a) il est $\equiv -1 \pmod 4$.

b) il est $\equiv 1 \pmod 4$.

D'autre part, P et Q impairs ayant une somme nulle (mod 4). sont l'un $\equiv 1 \pmod 4$, l'autre $\equiv (-1) \pmod 4$. Soit, par exemple

$$P \equiv 1 \qquad \text{et} \qquad Q \equiv -1 \pmod 4.$$

u^2 et ν^2 carrés de nombres imapirs sont $\equiv 1 \pmod 4$.

Le quotient de $(\eta u - \nu\xi)^2$ par $2^{2\alpha}$, carré impair est $\equiv 1$ (mod 4).

Dans le cas *a*) le quotient de ηY par $2^{2\alpha}$ est congru à

$$1 - (-1) \equiv 2 \pmod 4.$$

Dans le cas *b*) le quotient de ξX par $2^{2\alpha}$ est congru à

$$-1 - 1 \equiv -2 \pmod 4.$$

Dans les deux cas ξX et ηY divisés par $2^{2\alpha}$ le sont encore par 2 et non par 4, pour l'un d'eux.

4423) Si l'on posait $\beta > \alpha$, ξX comprendrait une partie divisible par $2^{2\beta}$ et l'autre seulement par $2^{2\alpha}$ et par suite on a

$$(X, Y, Z) = 2^{2\alpha} \cdots,$$

ce qui est en accord avec la limite supérieure.

443) $\zeta = 2^\alpha$, $R = 2$ d'où $2R\zeta^2 = 2^{2\alpha+2} \cdots$

Posons

$$(4431) \qquad \begin{aligned} \nu\xi - u\eta &\equiv 0 \pmod{2^\beta} \\ \nu\xi - u\eta &\not\equiv 0 \pmod{2^{\beta+1}} \end{aligned} \qquad (\beta < \alpha),$$

ξX contient 2 avec l'exposant 2β dans le terme Q $(\nu\xi - u\eta)^2$ et avec l'exposant $2\alpha + 1$ dans le terme $P\xi^2 = Q\eta^2$ donc avec l'exposant 2β.

$\eta Y \dots$

$\xi\eta Z$ contient 2 avec l'exposant $\alpha + \beta + \gamma$ dans un terme et $3\alpha + 1$ dans l'autre, donc au moins avec l'exposant 2β.

Donc

$$(X, Y, Z) = 2^{2\beta} \dots$$

4432) Pour $\beta \geqslant \alpha + 1$).

$(\eta u - \nu\xi)^2$ contient 2 avec un exposant supérieur ou égal à $2\alpha + 2$ et $P\xi^2 + Q\eta^2$ seulement avec l'exposant $2\alpha + 1$. Donc

$$(X, Y, Z) = 2^{2\alpha+1} \dots .$$

Ce théorème IV indique donc quel est l'exposant d'un facteur premier dans (X, Y, Z). Il est à remarquer que certains diviseurs de D ne peuvent être p. g. c. d. de X, Y, Z pour aucun couple u, ν. Ce sont en particulier ceux qui contiennent un facteur ρ à un exposant impair.

Nous terminerons ce chapitre en indiquant quelques exemples schématiques et numériques.

Exemple schématique

Soient, par exemple

$$\begin{aligned} P &= p_1 p_2, \\ Q &= q_1 q_2 q_3, \\ R &= r_1 r_2 \lambda, \\ \zeta &= \lambda \rho_1 \rho_2^2, \end{aligned}$$

aucun facteur n'étant 2.

Pour que

$$(X, Y, Z) = p_1 q_1 q_2 r_1 \lambda^2 \rho^2,$$

il faut et il suffit que le couple u, ν satisfasse au double système

$$\text{(C)} \qquad \left\{ \begin{aligned} u &\equiv 0 \pmod{q_1, q_2}, \\ \nu &\equiv 0 \pmod{p_1}, \\ \nu\xi - u\eta &\equiv 0 \pmod{r_1, \lambda_1, \rho_1}, \end{aligned} \right.$$

et

$$(N)\qquad \begin{cases} u \not\equiv 0 \pmod{q_3}, \\ v \not\equiv 0 \pmod{p_2}, \\ v\xi - u\eta \not\equiv 0 \pmod{r_2, \text{ mod } \lambda^2, \text{ mod } \rho_1^2, \text{ mod } \rho_2} \\ u + v \not\equiv 0 \pmod{d_2}. \end{cases}$$

En effet d'après le théorème III, seuls les facteurs q_1, q_2, p_1, r_1, λ et ρ, figurent dans (X, Y, Z).

D'après le théorème IV ils y figurent avec l'exposant voulu.

Exemple numérique

$$3X^2 + 5Y^2 - 2Z^2 = 0.$$

Nous partons de la solution

$$\xi = 1, \quad \eta = 1, \quad \zeta = 2.$$

Le système est alors

$$\begin{cases} X = 3u^2 + 5v^2 - 2u(3u + 5v), \\ Y = 3u^2 + 5v^2 - 2v(3u + 5v), \\ Z = 2(3u^2 + 5v^2), \end{cases}$$

et nous avons

$$D = 2 \cdot 3 \cdot 5 \cdot 8 = 2^4 \cdot 3 \cdot 5.$$

D a 5.2.2 = 20 diviseurs donnés par le tableau

1	2	4	8	16
1	3			
1	5			

Le système de congruences (C) est alors

$$(C)\qquad \begin{cases} v \equiv 0 \pmod 3, \\ u \equiv 0 \pmod 5, \\ v - u \equiv 0 \pmod 2. \end{cases}$$

Le système (E) s'écrit

$$\begin{aligned} X &= 5(v - u)^2 - 8u^2, \\ Y &= 3(v - u)^2 - 8v^2, \\ Z &= 2(u - v)(3u - 5v) + 16uv. \end{aligned}$$

Posons $v - u + 2S$.

1) Si S est impair, (X, Y, Z) est divisible par 4 et non par 8.

2) Si S est pair, (X, Y, Z) est divisible par 8 et non par 16, car u et v ne sont pas tous deux pairs.

(X, Y, Z) prend seulement 12 valeurs données par le tableau

$$\begin{matrix} 1 & 4 & 8 \\ 1 & 3 & \\ 1 & 5 & \end{matrix}$$

ce qui est en accord avec le théorème IV.

Ainsi à chaque couple u, v est attaché un double système (C) et (N) déterminé par les théorèmes III et IV.

Pour chaque couple u, v nous savons calculer (X, Y, Z). Nous remplaçons le système incomplet unique (S) par un nombre limité de systèmes analogues correspondants aux différentes valeurs de (X, Y, Z).

L'exemple suivant en montre bien le mécanisme.

Soit l'équation

$$X^2 + Y^2 - 5Z^2 = 0,$$

avec la solution initiale

$$\xi = 1, \qquad \eta = 2 \qquad \text{et} \qquad \zeta = 1,$$

d'où nous tirons le système (S)

$$\begin{aligned} X &= u^2 + v^2 - 2u(u + 2v), \\ Y &= 2(u^2 + v^2) - 2v(u + 2v), \\ Z &= u^2 + v^2. \end{aligned}$$

On a ici

$$D = 2 \cdot 5 = 10.$$

Les congruences (C) sont ici

$$(C) \qquad \begin{cases} u + v \equiv 0 \pmod 2, \\ v - 2u \equiv 0 \pmod 5, \end{cases}$$

et l'on aura

$$(X, Y, Z) = \begin{cases} 1 \\ 2 \\ 5 \\ 10 \end{cases} \quad \text{si} \quad u + v \begin{cases} \not\equiv 0 \\ \equiv 0 \\ \not\equiv 0 \\ \equiv 0 \end{cases} \quad \text{et} \quad v - 2u \begin{cases} \not\equiv 0 \\ \not\equiv 0 \\ \equiv 0 \\ \equiv 0, \end{cases}$$

et le système (S) doit être remplacé par les 4 analogues.

1) X, Y, Z tant que

$$\begin{cases} v + u \not\equiv 0, \\ v - 2u \not\equiv 0. \end{cases}$$

2) $\frac{X}{2}, \frac{Y}{2}, \frac{Z}{2}$ tant que

$$\begin{cases} v + u \equiv 0, \\ v - 2u \not\equiv 0. \end{cases}$$

3) $\frac{X}{5}, \frac{Y}{5}, \frac{Z}{5}$ tant que

$$\begin{cases} v + u \not\equiv 0, \\ v + 2u \equiv 0. \end{cases}$$

4) $\frac{X}{10}, \frac{Y}{10}, \frac{Z}{10}$ tant que

$$\begin{cases} v + u \equiv 0, \\ v - 2u \equiv 0. \end{cases}$$

Les systèmes 2), 3) et 4) contiennent sous forme apparente un dénominateur qui disparaît si l'on tient compte des congruences (C). On peut résoudre ces congruences en introduisant un nouveau couple S, t devant satisfaire bien entendu aux non congruences (N) et à la condition $(u, v)) = 1$.

Pour préciser transformons le système (3).

On doit avoir

$$\begin{cases} v - 2u \equiv 0 \pmod 5, \\ v + u \not\equiv 0 \pmod 2, \\ (u + v) = 1. \end{cases}$$

Posons

$$\begin{aligned} v - 2u &= 5S, \\ u &= t, \end{aligned}$$

d'où

$$v = 5S + 2t.$$

On a $(u, v) = 1$ si $5 \nmid t$ et si $(S, t) = 1$.

On a $2 \nmid v + u$ si u et v sont de parités différentes.

Le système (E) donne

$$\begin{aligned} X &= 25S^2 - 5t^2, \\ 2Y &= 25S^2 - 5(5S + 2t)^2, \\ 2Z &= 5S(3t + 10S) + 5t(5S + 2t), \end{aligned}$$

ou après division par 5

$$\begin{cases} X = 5S^2 - t^2, \\ Y = -10S^2 - 10St - 2t^2, \\ Z = 5S^2 + 4St + t^2, \end{cases}$$

qui est primitif, les S et t satisfaisant aux conditions imposées.

Vérifions les résultats précédents en employant la méthode générale.

Soit le système (S)

$$(S) \qquad \begin{cases} X = -\xi P u^2 - 2\eta Q u v + \xi Q v^2, \\ Y = \quad \eta P u^2 - 2\xi P u v + \eta Q v^2, \\ Z = \quad \zeta P u^2 + \qquad\qquad \zeta Q v^2. \end{cases}$$

En résolvant par rapport à u^2, uv, v^2 nous obtenons

$$\begin{aligned} Du^2 &= AX + A'Y + A''Z, \\ Duv &= BX + B'Y + B''Z, \\ Dv^2 &= CX + C'Y + C''Z, \end{aligned}$$

où

$$D = 4PQR\zeta^3.$$

De plus nous avons

$$\begin{aligned} (A, A', A'') &= 2\zeta Q, \\ (B, B', B'') &= 2\zeta PQ, \\ (C, C', C'') &= 2\zeta P. \end{aligned}$$

Donc (X, Y, Z) divise

$$2PR\zeta^2 u^2, \qquad 2R\zeta^2 uv, \qquad 2QR\zeta^2 v^2.$$

Le p. p. c. m. de ces 3 coefficients est $2PQR\zeta^2$.
Donc

$$(X, Y, Z) \,/\, 2PQR\zeta^2.$$

Nous retrouvons la borne supérieure de (X, Y, Z).
Ensuite les 3 congruences du second degré sont

$$\begin{matrix} -P\xi\alpha^2 - 2Q\eta\alpha + Q\xi \\ P\eta\alpha^2 - 2P\xi\alpha - Q\eta \\ P\zeta\alpha^2 \qquad\quad + P\zeta \end{matrix} \equiv 0 \pmod{\rho},$$

L'élimination de α^2 entre la 1re et la 2e donne

$$2Q\eta\alpha - 2Q\xi \equiv 0.$$

Or $\rho \nmid 2Q$ puisque ρ est un diviseur du 3e groupe.
Donc

$$\eta\alpha - \xi \equiv 0 \pmod{\rho}.$$

En tirant le nombre α de cette congruence et le portant dans le système (T), on obtient

$$\begin{aligned} -P\xi^3 - 2Q\xi\eta^2 + Q\xi\eta^2 &= -\xi(P\xi^2 + Q\eta^2) \equiv 0, \\ P\eta\xi^2 - 2P\xi\eta - Q\eta^3 &= -\eta(P\xi^2 + Q\eta^2) \equiv 0, \\ &\quad \zeta(P\xi^2 + Q\eta^2) \equiv 0. \end{aligned}$$

Le système (T) est donc satisfait.

Nous terminerons ce chapitre en dégageant cette idée fondamentale :

Il suffit d'une seule représentation pour obtenir toutes les solutions, les simplifications que l'on a apportées ont été obtenues par des transformations homographiques portant sur le couple u, v.

CHAPITRE III

ÉQUATION $aX^2 + bY^2 + cZ^2 + dT^2 = 0$.

Comme précédemment nous partirons d'une solution particulière connue et nous nous proposons d'en déduire la solution générale.

Soit donc ξ, η, ζ, τ la solution connue. La méthode déjà employée donne la solution

$$(S) \qquad \begin{cases} X = \xi C - 2uD, \\ Y = \eta C - 2vD, \\ Z = \zeta C - 2wD, \\ T = \tau C, \end{cases} \qquad \text{avec} \qquad (u, v, w) = 1,$$

en posant

$$C = au^2 + bv^2 + cw^2,$$
$$D = a\xi u + b\eta v + c\zeta w.$$

THÉORÈME I. — *Les facteurs premiers de* (X, Y, Z, T) *sont les mêmes que ceux de* (C, 2D).

1) Soit p un facteur premier de (C, 2D). Alors p divise X, Y, Z et T.

2) Soit maintenant ρ en facteur premier de (X, Y, Z, T) supposé non diviseur de (C,2D). Les seules hypothèses à faire sont :

1° ρ C *et* $\not|$ 2D. — On doit nécessairement avoir

$$\rho \mid u, v, w \quad \text{à la fois,}$$

ce qui n'est pas car $(u, v, w) = 1$.

2° ρ/2D *et* $\not|$ C. — On doit avoir

$$\rho \mid \xi, \eta, \zeta, \tau \quad \text{à la fois,}$$

ce qui est impossible puisque $(\xi, \eta, \zeta, \tau) = 1$.

3° $\rho \nmid 2DC$. — Alors ρ divisant T divise τ et l'équation

$$a\xi^2 + b\eta^2 + c\zeta^2 + d\tau^2 = 0$$

s'écrit

$$a\xi^2 + b\eta_1^2 + c\zeta^2 \equiv 0 \pmod{\rho}. \tag{1}$$

Les congruences

$$X \equiv Y \equiv Z \equiv 0 \pmod{\rho}$$

donnent

$$\frac{C}{2D} \equiv \frac{u}{\xi} \equiv \frac{\nu}{\eta_1} \equiv \frac{w}{\zeta} \pmod{\rho}, \tag{2}$$

et en reportant dans la congruence (1) on a

$$au^2 + bo^2 + cw^2 = C \equiv 0,$$
$$a\xi u + b\eta_1 \nu + c\zeta w = D \equiv 0.$$

Cette contradiction démontre le théorème.

Pour être rigoureux remarquons que les congruences (2) ont une forme illusoire, par exemple pour ρ/ξ. Le résultat énoncé est encore valable.

En effet l'hypothèse $\rho \nmid 2D$ conduit à ρ/u pour que ρ/X.

C et D se réduisent à

$$\left.\begin{matrix} b\nu^2 + cw^2 \\ b\eta_1 \nu + b\zeta w \end{matrix}\right| \equiv 0 \pmod{\rho},$$

et les congruences (2) aux suivantes

$$\frac{C}{2D} \equiv \frac{\nu}{\eta_1} \equiv \frac{w}{\zeta} \pmod{\rho}.$$

Les autres cas ρ/η et ζ par exemple ou ρ/ξ, η et ζ se traitent de façon analogue.

Le théorème I est donc tout à fait général.

Théorème II. — *Tout facteur premier de* (C, 2D) *admet abcd pour reste quadratique.*

Comme $(u, \nu, w) = 1$, l'un au moins des 3 nombres u, ν, w est premier avec p ; soit w tel que

$$p \nmid w.$$

Nous pouvons poser

$$\left.\begin{aligned} u &\equiv \alpha w \\ v &\equiv \beta w \end{aligned}\right\} \pmod p,$$

et les congruences.

$$\left.\begin{aligned} C &= au^2 + bv^2 + cu^2 \\ D &= a\xi u + b\eta v + c\zeta w \end{aligned}\right\} \equiv 0 \pmod p$$

deviennent

$$\left.\begin{aligned} w^2(a\alpha^2 + b\beta^2 + c) \\ w(a\xi\alpha + b\eta\beta + c\zeta) \end{aligned}\right\} \equiv 0,$$

ou

$$\left.\begin{aligned} a\alpha^2 + b\beta^2 + c \\ a\xi\alpha + b\beta\eta + c\zeta \end{aligned}\right\} \equiv 0, \tag{1}$$

puisque $p \nmid w$.

L'élimination de α entre ces deux congruences (1) donne

$$b(a\xi^2 + b\eta^2)\beta^2 + 2bc\eta\zeta\beta + c(a\xi^2 + b\eta^2) \equiv 0 \pmod p, \tag{B}$$

Cette congruence (B) du second degré n'est possible que si son discriminant Δ

$$\Delta = -4abc(a\xi^2 + b\eta^2 + c\zeta^2)\xi^2,$$

est reste quadratique de p (voir CAHEN, *Théorie des Nombres*, II, 93).

Ce Δ s'écrit, en utilisant la solution fondamentale

$$\begin{aligned} a\xi^2 + b\eta^2 + c\zeta^2 + d\tau^2 &= 0, \\ \Delta &= 4abcd\xi^2\tau^2. \end{aligned}$$

Comme 4, ξ^2, τ^2 sont restes et que le quotient de deux restes est encore reste, il en résulte que $abcd$ est reste de p.

Le théorème II admet une réciproque. En effet, la condition — Δ reste de p — est nécessaire pour qu'une congruence du second degré soit possible ; elle est d'ailleurs suffisante sous certaines conditions qu'il nous faut préciser.

THÉORÈME. — *Soit p un facteur premier admettant $abcd$ pour reste. Nous pouvons toujours déterminer u, v, w de telle sorte que*

$$p \mid (X, Y, Z, T)$$

la condition $(u, v, w) = 1$ étant remplie.

Rappelons d'abord que la congruence

$$A\alpha^2 + 2B\alpha + C \equiv 0 \pmod{p}, \tag{1}$$

donne

$$A(A\alpha^2 + 2B\alpha + C) \equiv 0,$$

ou

$$(A\alpha + B)^2 - \Delta \equiv 0, \tag{2}$$

et que la congruence (2) entraîne la congruence (1) certainement si

$$A \not\equiv 0.$$

Il y a simplement une discussion à faire si

$$A \equiv 0.$$

Cela posé, le fait que $abcd$ est reste de p entraîne la possibilité de la congruence (B)

$$b(a\xi^2 + b\eta^2)\beta^2 + 2bc\eta\zeta\beta + c(a\xi^2 + b\eta^2) \equiv 0, \tag{B}$$

sauf peut être si

$$p \mid b(a\xi^2 + b\eta^2).$$

1er Cas : $p \nmid b(a\xi^2 + \rho\eta^2)$. — Soit β l'une des 2 racines de la congruence (B).

Déterminons α de telle sorte que l'on ait

$$D' = a\xi\alpha + b\eta\beta + c\zeta \equiv 0 \pmod{p.},$$

ce qui est toujours possible si $p/a\xi$.

En posant

$$C' = a\alpha^2 + b\beta^2 + c,$$

on a

$$a\xi^2 C' + D'^2 - 2a\xi\alpha D' = B.$$

11) $p \nmid a\xi$. — Par suite $p \nmid a\xi^2$ et l'on a bien p/C'.
Donc p/C et D.

12) p/a. — Nous allons étudier ce cas.

13) p/ξ. — Au lieu de partir de la congruence (B), nous partirons de congruences analogues en intervertissant ξ, η ou ζ, qui nous conduirons au résultat voulu sauf si

$$p \mid \xi, \eta \text{ et } \zeta \text{ à la fois.}$$

Mais un tel p divise X, Y, Z et divisera T si

$$p \mid au^2 + bv^2 + bv^2 + cw^2$$

($p \nmid \tau$ car $(\xi, \eta, \zeta, \tau) = 1$).

Cette congruence à 3 variables est toujours possible, comme nous le montrerons à la fin de cette démonstration.

2e Cas : p/b. — Alors C et D se réduisent à

$$\begin{matrix} au^2 + Cw^2 \\ a\xi u + C\zeta w \end{matrix} \equiv 0,$$

résolubles par

$$u \equiv w \equiv 0 \pmod{p}.$$

Si l'on prend v premier avec (u, w) on a bien

$$(u, v, w) = 1.$$

Le raisonnement s'étend à p/a ce qui résout le cas 12).

3e Cas : $p/a\xi^2 + b\eta^2$. — Nous prendrons $w \equiv 0$.

$$\frac{\xi}{u} \equiv \frac{\eta}{v} \pmod{p},$$

ce qui entraîne, puisque

$$a\xi^2 + b\eta^2 \equiv 0,$$

les 2 congruences

$$\begin{matrix} au^2 + bv^2 \\ a\xi u + b\eta v \end{matrix} \equiv 0,$$

et par suite

$$C \equiv D \equiv 0 \pmod{p}.$$

On peut toujours prendre.

$$(u, v, w) = 1.$$

Il nous reste à montrer que la congruence à 3 variables

$$(C) \qquad au^2 + bv^2 + cw^2 \equiv 0 \pmod{p}$$

est toujours possible.

1) *Si* p/b, par exemple, nous nous reporterons au 2e cas déjà étudié.

2) *Si* — ab, par exemple est reste de p la congruence

$$au^2 + bv^2 \equiv 0 \pmod{p}$$

est possible avec $(u, v) \not\equiv 0$.

En prenant $w \equiv 0$ on aura $C \equiv 0$ et on pourra toujours avoir $(u, v, w) = 1$.

3) Dans le cas le plus défavorable aucune des hypothèses précédentes n'est vérifiée.

Soit

$$p = 2n + 1.$$

Les n nombres

$$-au^2c, \qquad u = 1, 2, \cdots, n$$

sont non restes quadratiques de p et aucune des congruences

$$au^2 + cw^2 \equiv 0,$$
$$u = 1, 2, \cdots, n,$$

n'est possible.

Soit alors $v = 1$.

Les n nombres

$$-acu^2, \qquad u = 1, 2, \cdots, n,$$

forment les n non restes quadratiques (mod p). Parmi les n nombres

$$-acu^2 - bc, \; u = 1, 2, \cdots, n$$

il y en a alors qui sont restes.

(Exercice proposé en particulier dans le livre déjà cité de M. Cahen, II, 102).

La congruence

$$au^2 + b + cw^2 \equiv 0$$

a son discriminant

$$-c(au^2 + b) = -acu^2 - bc$$

reste de p pour au moins une valeur de u et comme $v = 1$ on a bien

$$(u, v, w) = 1.$$

Pour être absolument rigoureux il nous faut considérer le cas de $p = 2$.

Mais alors

$$u^2 \equiv u \cdots \pmod 2,$$

d'après le théorème de Fermat et l'on a

$$au^2 + bv^2 + cw^2 \equiv au + bv + cw \pmod 2,$$

forme linéaire qui peut toujours être nulle (mod 2) avec $(u, v, w) = 1$.

De ce théorème III découle une conséquence très importante.

THÉORÈME IV. — (X, Y, Z, T) *admet avec une infinité de diviseurs lorsqu'on fait varier* u, v, w.

En effet, il y a une infinité de nombres premiers admettant *abcd* pour reste quadratique et *a fortiori* une infinité de nombres composés (Cahen, t. II, 366...).

Dans ce livre on trouvera la démonstration du fait que p appartient à certaines progressions

$$\begin{matrix} \rho_i + 4\delta x \\ \rho_i + 2\delta x \end{matrix} \qquad \text{où} \qquad \delta = abcd,$$

x variant de $-\infty$ à $+\infty$ et ρ_i ayant certaines valeurs déterminées.

Comme $(\rho_i, 2\delta) = 1$ d'après un théorème de Lejeune-Dirichlet, chacune de ces progressions contient une infinité de nombres premiers.

Exemple : Ce théorème IV est complètement différent du théorème relatif à 3 variables ; il n'est donc pas inutile de le vérifier sur un exemple simple.

Soit l'équation

$$X^2 + Y^2 + Z^2 - T^2 = 0,$$

où X, Y, Z, T peuvent représenter les 3 arêtes et la diagonale d'un parallélépipède droit à base rectangle.

Prenons la solution initiale

$$\xi = \eta = 0, \qquad \zeta = \tau = 1.$$

Nous obtenons la solution

$$\text{(S)} \qquad \begin{cases} X = & 2uw, \\ Y = & 2vw, \\ Z = u^2 + v^2 + w^2 - & 2ww, \\ T = u^2 + v^2 + w^2, & \end{cases}$$

Ici nous avons

$$C = u^2 + v^2 + w^2, \qquad D = w.$$

Puisque

$$(C, D) = (u^2 + v^2, w),$$

tout nombre premier p de la forme $4h + 1$ décomposable en une somme de deux carrés peut être diviseur de (C, D) pour u, v convenablement choisis avec

$$(u, v) \not\equiv 0 \pmod{p}$$

et

$$w \equiv 0 \pmod{p},$$

et

$$(u, v, w) = 1.$$

Il y en a bien une infinité (cas particulier très simple du théorème de Lejeune-Dirichlet).

Ceci est bien en accord avec les théorèmes II et IV à savoir *abcd* ici — 1 est reste quadratique de tout nombre premier de la forme $4h + 1$ et non reste de tout nombre premier de la forme $4h - 1$.

NOTES

I. *Sur les points multiples* (page 8). — Dans cette étude, nous avons écarté implicitement la considération de la rationnalité des points multiples.

1° Comme ces points sont en nombre limité, et faciles à obtenir, l'étude directe de leur rationnalité est immédiate.

2° D'autre part, les transformations birationnelles que nous avons employées, cessent d'être uniformément réversibles aux points multiples. Il faut donc étudier spécialement la rationnalité des points multiples.

Il est facile de former des courbes de genre O, dépourvues de points simples rationnels, et possédant, cependant, des points multiples rationnels.

Soit par exemple l'hyperbole

$$x^2 - 3y^2 + z^2 = 0$$

sans points rationnels (d'après le théorème rappelé page 13).

Son inverse par rapport au cercle de centre O, de rayon 1 est la quartique

$$Z^2(X^2 - 3Y^2) + (X^2 + Y^2)^2 = 0$$

qui n'a pas de point simple rationnel et dont l'origine, point double, est un point rationnel.

II. Théorème I (page 9). — La réciproque du théorème I concernant l'existence d'une représentation entière pour les courbes de genre O ayant une infinité de points entiers n'est nullement nécessaire en cet endroit. Elle résultera en effet du théorème II dont la première démonstration en indique l'existence et dont la deuxième permet de l'obtenir par voie de récurrence.

III. *Références.* — Signalons encore les travaux suivants que nous avons utilisés, sans toutefois leur faire d'emprunt direct :

1) HILBERT et HURWITZ. — *Ueber die diophantischen Gleichungen var Geschlecht Null* (*Acta Math.*, t. 14, 1891).

2) MAILLET. — *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers* (*Journal de l'Ecole Polyt.*, 1919).

3) CARMICHAEL. — *Analyse indéterminée* (éditée par les Presses Universitaires de France).

et enfin

4) DIKSON. — *History on the Theorie of Numbers.*

Où l'on trouvera tous renseignements bibliographiques.