OUVRAGES DE LA COLLECTION

A. I. MARKOUCHEVITCH. — *Fonctions d'une variable complexe. Problèmes contemporains* (272 p.). Traduit par L. NICOLAS, 1962.

N. N. BOGOLIOUBOV et Y. A. MITROPOLSKI. — *Les méthodes asymptotiques en théorie des oscillations non linéaires* (520 p.). Traduit par G. JACOBI, 1962.

Y. V. LINNIK. — *Décompositions des lois de probabilités* (294 p.). Traduit par M. L. GRUEL, 1962.

J. MIKUSINSKI et R. SIKORSKI. — *Théorie élémentaire des distributions* (108 p.). Traduit par S. KLARSFELD, 1964.

I. M. GELFAND, D. A. RAIKOV et G. E. CHILOV. — *Les anneaux normés commutatifs* (259 p.). Traduit par M. et J.-L. VERLEY, 1964.

A. GELFOND et Y. LINNIK. — *Méthodes élémentaires dans la théorie analytique des nombres* (234 p.). Traduit par M. et J.-L. VERLEY, 1965.

Y. A. I. MITROPOLSKI. — *Problèmes de la théorie asymptotique des oscillations non stationnaires* (547 p.). Traduit par G. CARVALLO, 1966.

V. I. ARNOLD et A. AVEZ. — *Problèmes ergodiques de la mécanique classique* (288 p.), 1967.

MONOGRAPHIES INTERNATIONALES DE MATHÉMATIQUES MODERNES

Sous la direction de S. MANDELBROJT

Professeur au Collège de France

Théorie des nombres

par **Z. I. BOREVITCH**

et **I. R. CHAFAREVITCH**

Traduit par

Myriam et Jean-Luc VERLEY

gV

UNIVERSITÉ DE GRENOBLE I

LABORATOIRE

DE MATHÉMATIQUES PURES

INSTITUT FOURIER

1967

GAUTHIER-VILLARS

PARIS

CHAPITRE PREMIER

CONGRUENCES

Ce chapitre est consacré à la théorie des congruences et à ses applications aux équations. Remarquons que si l'équation

$$F(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

où F est un polynôme à coefficients entiers, a une solution en nombres entiers, alors la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{2}$$

a une solution pour tout entier m. Pour chaque m, l'ensemble des classes résiduelles modulo m est fini et par suite la congruence (2) s'étudie directement. On obtient ainsi des conditions nécessaires pour que l'équation (1) soit résoluble en nombres entiers.

L'étude de la suffisance éventuelle de ces conditions est très difficile. L'affirmation : « une équation est résoluble si et seulement si pour chaque entier la congruence correspondante est résoluble » n'est pas vraie dans le cas général (cf. par exemple, exercice 4), mais est vraie pour plusieurs classes particulières d'équations. Dans ce chapitre, nous démontrerons ce résultat dans le cas où F est une forme quadratique, après avoir ajouté l'hypothèse supplémentaire (manifestement nécessaire) que l'équation (1) a une solution en nombres réels (si F est une forme, alors, par solution de $F = 0$, on entend solution non nulle).

La notion essentielle que nous étudierons tout d'abord dans ce chapitre est celle de nombre p-adique; nous appliquerons ensuite cette notion à la théorie des congruences. On sait, d'après la théorie élémentaire des nombres, que, si $m = p_1^{k_1} \ldots p_r^{k_r}$ ($p_1, \ldots, p_r$ étant des facteurs premiers distincts), la résolution de la congruence (2) est équivalente à la résolution des congruences

$$F(x_1, \ldots, x_n) \equiv 0 \left(\mathrm{mod}\ p_i^{k_i}\right)$$

pour tout $i = 1, 2, \ldots, r$. Ainsi, la résolubilité de la congruence (2) pour tout entier m est équivalente à la résolubilité de ces congruences modulo toutes les puissances des nombres premiers. Dans la suite, nous fixerons le nombre premier p et nous étudierons les congruences

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{3}$$

pour toutes les valeurs entières de k. En liaison avec ce problème, Hensel a introduit, pour chaque nombre premier p, un nouveau type de nombres appelés par lui nombres p-adiques et a démontré que la résolubilité des congruences (3) pour tout entier k est équivalente à la résolubilité de l'équation (1) dans l'ensemble des nombres p-adiques. Par suite, la résolubilité des congruences (2) pour tout entier m est équivalente à la résolubilité de l'équation (1) dans les ensembles de nombres p-adiques pour les nombres p premiers.

En utilisant la notion de nombre p-adique, on peut donc donner la forme suivante au théorème mentionné ci-dessus (ce chapitre est consacré à la démonstration de ce résultat) : si $F(x_1, \ldots, x_n)$ est une forme quadratique à coefficients entiers, l'équation (1) est résoluble en nombres entiers si et seulement si elle est résoluble en nombres réels et en nombres p-adiques, pour tout p.

Dans la formulation de ce théorème, appelé le théorème de Minkowski-Hasse, et dans beaucoup d'autres questions, les nombres p-adiques figurent sur le même plan que les nombres réels. De même que les nombres réels interviennent de manière naturelle dans l'étude des limites de nombres rationnels, les nombres p-adiques jouent un rôle analogue dans les questions liées à la division suivant les puissances successives du nombre premier p. Cette analogie entre les nombres p-adiques et les nombres réels sera précisée en montrant que les nombres p-adiques, tout comme les nombres réels, peuvent être obtenus par complétion à partir des nombres rationnels (pour d'autres métriques que la valeur absolue usuelle).

Faisons une dernière remarque : si F est une forme, la résolubilité en nombres entiers de l'équation (1) est bien entendu équivalente à l'existence d'une solution formée de nombres rationnels; ainsi, dans le théorème de Minkowski-Hasse, on peut parler de la résolubilité en nombres rationnels au lieu de la résolubilité en nombres entiers. Cette remarque évidente prend toute sa signification dans le résultat suivant : si F est un polynôme quelconque de degré 2, le théorème correspondant donne des conditions de résolubilité de l'équation (1) en nombres rationnels et non pas en nombres entiers. Par suite, dans l'étude des équations du deuxième degré nous ne nous limiterons pas à l'étude des solutions en nombres entiers mais examinerons également les solutions en nombres rationnels.

EXERCICES

1. Montrer que l'équation $15x^2 - 7y^2 = 9$ n'a pas de solutions en nombres entiers.

2. Montrer que l'équation $5x^3 + 11y^3 + 13z^3 = 0$ n'a pas d'autre solution en nombres entiers que la solution triviale $x = 0, y = 0, z = 0$.

3. Démontrer que les nombres entiers de la forme $8n + 7$ ne peuvent pas s'écrire comme somme de trois carrés de nombres entiers.

4. Utilisant les propriétés du symbole de Legendre, démontrer que la congruence

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod{m}$$

est résoluble pour tout entier m. Remarquer cependant qu'il est évident que l'équation $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ n'a pas de solution en nombres entiers.

5. Démontrer que l'équation linéaire $a_1x_1 + \ldots + a_nx_n = b$, où $a_1, \ldots, a_n, b$ sont des entiers, est résoluble en nombres entiers si et seulement si la congruence correspondante modulo m est résoluble pour tout entier m.

6. Démontrer le même résultat pour un système d'équations linéaires à coefficients entiers.

§ 1. — CONGRUENCES MODULO UN NOMBRE PREMIER

1) Équivalence des polynômes

Rappelons tout d'abord quelques propriétés des congruences modulo un nombre premier. Comme on le sait, les classes résiduelles modulo p forment un corps fini à p éléments qui sera constamment désigné dans la suite par $\mathbf{F}_p$; chaque congruence modulo p s'interprète comme une égalité dans ce corps. Tous les résultats de ce paragraphe et du suivant sont valables non seulement pour le corps $\mathbf{F}_p$, mais plus généralement pour tout corps fini; il suffit de remplacer à chaque fois le nombre p par le nombre $q = p^m$ d'éléments de ce corps. Nous nous limiterons cependant à l'étude des corps $\mathbf{F}_p$ et c'est seulement pour donner un contre-exemple après le théorème 3 que nous devrons faire appel à un corps fini qui ne soit pas de ce type.

Les corps résiduels modulo un nombre premier (et plus généralement tout corps fini) possèdent une série de propriétés qui les distinguent des corps usuels de l'algèbre élémentaire. Voici la plus importante d'entre elles, dont nous aurons souvent besoin : deux polynômes qui prennent des valeurs égales pour toutes les valeurs des variables n'ont pas nécessairement des coefficients égaux. Ainsi, d'après le petit théorème de Fermat, les polynômes x^p et x prennent des valeurs égales quand x parcourt tout le corps $\mathbf{F}_p$

mais leurs coefficients ne sont pas égaux (ce phénomène se produit dans tout corps fini : si $\alpha_1, \ldots, \alpha_q$ sont tous les éléments de ce corps, le polynôme $(x - \alpha_1) \ldots (x - \alpha_q)$ à coefficients non nuls prend seulement la valeur 0 quand x parcourt tout le corps fini considéré).

Nous écrirons

$$F(x_1, \ldots, x_n) \equiv G(x_1, \ldots, x_n) \pmod{p}$$

et nous dirons que les polynômes F et G sont *congrus* si leurs coefficients correspondants sont congrus modulo p. Si maintenant nous avons

$$F(c_1, \ldots, c_n) \equiv G(c_1, \ldots, c_n) \pmod{p}$$

pour tous les systèmes de valeurs $c_1, \ldots, c_n$, nous écrirons $F \sim G$ et nous dirons que les polynômes F et G sont *équivalents*. Il est clair que si $F \equiv G$, alors $F \sim G$, mais l'exemple des polynômes x et x^p montre que la réciproque n'est pas vraie en général.

Puisque les deux congruences $F \equiv 0 \pmod{p}$ et $G \equiv 0 \pmod{p}$ ont les mêmes solutions si $F \sim G$, il est naturel pour étudier une congruence de remplacer le polynôme considéré par un polynôme équivalent plus simple. Précisons cette question.

Si une inconnue x_i figure dans le polynôme F avec un exposant supérieur à p, alors, utilisant l'équivalence $x_i^p = x_i$ qui résulte du théorème de Fermat, nous pouvons remplacer x_i^p par x_i dans F. Puisque les équivalences s'additionnent et se multiplient terme à terme, on obtient facilement ainsi un polynôme équivalent à F et de degré en x_i strictement plus petit. On peut alors répéter ce processus jusqu'à obtention d'un polynôme équivalent à F dont le degré par rapport à chaque variable est strictement inférieur à p. Un tel polynôme sera dit *réduit*. Il est clair que par le remplacement de x_i^p par x_i le degré total de F (par rapport à l'ensemble des variables) diminue; nous obtenons ainsi le résultat suivant.

THÉORÈME 1. — *Tout polynôme* F *est équivalent à un polynôme réduit* F* *dont le degré total est inférieur ou égal au degré total de* F.

Montrons maintenant que le polynôme réduit équivalent à un polynôme donné est unique.

THÉORÈME 2. — *Deux polynômes réduits qui sont équivalents sont congrus.*

Ce théorème se démontre par récurrence sur le nombre de variables, exactement comme le théorème rappelé ci-dessus sur l'identité des polynômes. Bien entendu, il suffit de montrer que si F est un polynôme réduit équivalent à 0, alors $F \equiv 0 \pmod{p}$.

Considérons tout d'abord le cas $n = 1$. Si le degré de x est inférieur à p et $F(c) \equiv 0 \pmod{p}$ pour tout c, alors F a un nombre de racines supérieur à son degré et cela n'est possible que si tous les coefficients de F sont divisibles par p, i. e. $F \equiv 0 \pmod{p}$. Soit maintenant $n \geqslant 2$; nous écrirons F sous la forme

$$F(x_1, \ldots, x_n) = A_0(x_1, \ldots, x_{n-1}) + A_1(x_1, \ldots, x_{n-1})x_n + \cdots + A_{p-1}(x_1, \ldots, x_{n-1})x_n^{p-1}.$$

Considérons un système arbitraire de valeurs $x_1 = c_1, \ldots, x_{n-1} = c_{n-1}$ et posons

$$A_0(c_1, \ldots, c_{n-1}) = a_0, \ldots, A_{p-1}(c_1, \ldots, c_{n-1}) = a_{p-1}.$$

Ainsi

$$F(c_1, \ldots, c_{n-1}, x) = a_0 + a_1x_n + \ldots + a_{p-1}x_n^{p-1},$$

et nous avons obtenu un polynôme d'une seule variable x_n qui est équivalent à 0 puisque $F \sim 0$. Mais le théorème est démontré pour les polynômes d'une variable et par suite ce polynôme est congru à 0. Ainsi

$$\begin{aligned} A_0(c_1, \ldots, c_{n-1}) &\equiv 0 \pmod{p} \\ &\vdots \\ A_{p_1}(c_1, \ldots, c_{n-1}) &\equiv 0 \pmod{p}, \end{aligned}$$

i. e. $A_0 \sim 0, \ldots, A_{p-1} \sim 0$ (puisque $c_1, \ldots, c_{n-1}$ sont arbitraires). Puisque les polynômes $A_0, \ldots, A_{p-1}$ de $(n - 1)$ variables sont réduits, alors, par hypothèse de récurrence, on a

$$A_0 \equiv 0 \pmod{p}, \ldots, A_{p-1} \equiv 0 \pmod{p},$$

d'où $F \equiv 0 \pmod{p}$.

2) Théorèmes sur le nombre de solutions des congruences

Donnons déjà quelques conséquences des théorèmes 1 et 2.

THÉORÈME 3. — *Si la congruence* $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ *a une solution et si le degré total du polynôme* F *est strictement inférieur au nombre n des variables, alors cette congruence a au moins deux solutions.*

DÉMONSTRATION. — Supposons que le polynôme $F(x_1, \ldots, x_n)$ de degré r ait une solution unique

$$x_1 \equiv a_1 \pmod{p}, \ldots, x_n \equiv a_n \pmod{p}.$$

Posant $H(x_1, \ldots, x_n) = 1 - F(x_1, \ldots, x_n)^{p-1}$, nous avons, d'après les hypothèses faites sur F et le petit théorème de Fermat,

$$H(x_1, \ldots, x_n) \equiv \begin{cases} 1 \text{ si } x_1 \equiv a_1, \ldots, x_n \equiv a_n \pmod p \\ 0 \text{ sinon.} \end{cases}$$

Soit H* le polynôme réduit équivalent au polynôme H (cf. théorème 1); H* prend les mêmes valeurs que H. Mais il est facile, par ailleurs, de construire un polynôme réduit prenant les mêmes valeurs que H; c'est le polynôme

$$\prod_{i=1}^{n}(1 - (x_i - a_i)^{p-1}).$$

D'après le théorème 2, nous aurons donc

$$H^* \equiv \prod_{i=1}^{n}(1 - (x_i - a_i)^{p-1}) \pmod p \tag{1}$$

et, d'après le théorème 1, le degré de H* est inférieur au degré de H, i. e. inférieur à $r(p-1)$, alors que son degré, d'après (1), est égal à $n(p-1)$. Il en résulte $n(p-1) \leqslant r(p-1)$, ce qui contredit l'hypothèse $r < n$.

COROLLAIRE (théorème de Chevalley). — *Si* $F(x_1, \ldots, x_n)$ *est une forme de degré strictement inférieur à n, la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p$$

a une solution non nulle.

L'existence de cette solution résulte du théorème 3 puisque cette congruence admet trivialement la solution nulle.

Montrons qu'il est impossible d'améliorer l'inégalité $r < n$ dans le théorème de Chevalley; nous construirons à cet effet pour tout entier n une forme $F(x_1, \ldots, x_n)$ de degré n telle que la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p \tag{2}$$

n'ait que la solution nulle. Nous utiliserons le fait que, pour tout $n \geqslant 1$, il existe un corps fini Σ à p^n éléments contenant $\mathbf{F}_p$ comme sous-corps (voir appendice, § 3, théorème 2); soit $\omega_1, \ldots, \omega_n$ une base du corps Σ sur le corps $\mathbf{F}_p$. Considérons les combinaisons linéaires $x_1\omega_1 + \ldots + x_n\omega_n$ où, $x_1, \ldots, x_n$ prennent des valeurs quelconques dans $\mathbf{F}_p$. La norme

$$N_{\Sigma/\mathbf{F}_p}(x_1\omega_1 + \ldots + x_n\omega_n) = \varphi(x_1, \ldots, x_n)$$

est une forme de degré n en $x_1, \ldots, x_n$, à coefficients dans $\mathbf{F}_p$. Par définition de la norme $N(\alpha)$ d'un élément $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ $(x_i \in \mathbf{F}_p)$ (cf. appendice § 2, 2)), on a $N(\alpha) = 0$ si et seulement si $\alpha = 0$, i. e. $x_1 = \ldots = x_n = 0$. Ainsi, la forme φ est telle que l'équation $\varphi(x_1, \ldots, x_n) = 0$ admet seulement la solution nulle dans le corps $\mathbf{F}_p$. Remplaçons maintenant chaque coefficient de la forme φ, qui est une classe résiduelle modulo p, par un représentant de cette classe. Nous obtenons ainsi une forme $F(x_1, \ldots, x_n)$ à coefficients entiers, de degré n à n variables telle que la congruence (2) n'ait que la solution nulle.

Le théorème 3 est un cas particulier du résultat suivant.

THÉORÈME 4 (théorème de Warning). — *Si le degré du polynôme* $F(x_1, \ldots, x_n)$ *est strictement inférieur à n, le nombre de solutions de la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p$$

est divisible par p.

DÉMONSTRATION. — Supposons que la congruence considérée ait s solutions $A_i = (a_1^{(i)}, \ldots, a_n^{(i)})$, $i = 1, \ldots, s$. Posons, cette fois encore, $H = 1 - F^{p-1}$. Il est clair que

$$H(X) = \begin{cases} 1 \text{ si } X \equiv A_i \pmod p & i = 1, \ldots, s, \\ 0 \text{ dans les autres cas;} \end{cases}$$

ici, $X = (x_1, \ldots, x_n)$ (les congruences entre vecteurs à coordonnées entières signifient que les composantes correspondantes de ces vecteurs vérifient la congruence). Pour $A = (a_1, \ldots, a_n)$, formons le polynôme

$$D_A(x_1, \ldots, x_n) = \prod_{j=1}^{n}(1 - (x_j - a_j)^{p-1}). \tag{3}$$

Il est clair que

$$D_A(X) = \begin{cases} 1 \text{ si } X \equiv A \pmod p \\ 0 \text{ sinon.} \end{cases} \tag{4}$$

Posons

$$H^*(x_1, \ldots, x_n) = D_{A_1}(x_1, \ldots, x_n) + \ldots + D_{A_s}(x_1, \ldots, x_n). \tag{5}$$

La congruence (4) montre que H* prend les mêmes valeurs que H pour toutes les valeurs des variables $x_1, \ldots, x_n$, i. e. $H \sim H^*$. Puisque chacun des polynômes D_{A_i} est réduit, H* est aussi réduit; il résulte alors des théorèmes 1 et 2 que le degré de H* est inférieur au degré de H, lui-même strictement inférieur à $n(p-1)$. Mais dans chaque D_{A_i}, il y a un seul terme de degré $n(p-1)$, c'est le terme $(-1)^n (x_1 \ldots x_n)^{p-1}$. Puisque le degré de H* est strictement inférieur à $n(p-1)$, la somme de tous les termes de degré $p-1$ est nulle,

ce qui exige $s \equiv 0 \pmod p$. Ceci termine la démonstration du théorème 4.

Le théorème 3 résulte du théorème 4 : si $p \geqslant 2$, $s \not\equiv 0$ et $s \equiv 0 \pmod p$ entraînent $s \geqslant 2$.

3) Les formes quadratiques modulo un nombre premier

Appliquons les résultats précédents aux formes quadratiques. Le théorème suivant est une conséquence immédiate du théorème de Chevalley.

THÉORÈME 5. — *Soit $f(x_1, \ldots, x_n)$ une forme quadratique à coefficients entiers. Si $n \geqslant 3$, la congruence*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod p$$

a une solution non nulle.

Le cas des formes quadratiques à une seule variable ne présente guère d'intérêt (si $a \not\equiv 0 \pmod p$, la congruence $ax^2 \equiv 0 \pmod p$ a seulement la solution nulle).

Considérons le cas des formes quadratiques à deux variables. Nous supposerons $p \neq 2$ (pour $n = 2$, $p = 2$, il est facile d'étudier directement toutes les formes quadratiques possibles). La forme peut alors s'écrire

$$f(x, y) = ax^2 + 2bxy + cy^2.$$

Nous désignerons par d son déterminant $ac - b^2$.

THÉORÈME 6. — *La congruence*

$$f(x, y) \equiv 0 \pmod p \quad (p \neq 2) \tag{6}$$

a une solution non nulle si et seulement si — d est ou bien divisible par p ou bien est un résidu quadratique modulo p.

DÉMONSTRATION. — Il est clair que pour des formes f et f_1 équivalentes sur le corps $\mathbf{F}_p$ (voir appendice § 1, 1)), les congruences (6) ont simultanément une solution non nulle ou pas de solution non nulle. Puisque dans le passage d'une forme à une forme équivalente, son déterminant est multiplié par le carré d'un élément non nul du corps $\mathbf{F}_p$, nous pouvons, dans la démonstration du théorème 6, remplacer la forme f par une autre qui lui soit équivalente. Chaque forme est équivalente à une forme diagonale (appendice § 1, théorème 3); par suite, nous pouvons supposer que

$$f = ax^2 + cy^2, \qquad d = ac.$$

Si $a \equiv 0$ ou $c \equiv 0 \pmod p$, le théorème est évident. Si maintenant $ac \not\equiv 0 \pmod p$ et si la congruence (6) a une solution non nulle (x_0, y_0), alors, de la congruence

$$ax_0^2 + cy_0^2 \equiv 0 \pmod p$$

nous tirons

$$-ac \equiv \left(\frac{cy_0}{x_0}\right)^2 \pmod p$$

(la fraction $w = \frac{u}{v} \pmod p$ désigne le résultat de la division dans le corps $\mathbf{F}_p$, i. e. la solution de la congruence $vw \equiv u \pmod p$). Ainsi $\left(\frac{-d}{p}\right) = 1$. Réciproquement, si $\left(\frac{-d}{p}\right) = 1$ et $-ac \equiv u^2 \pmod p$, nous pouvons prendre

$$(x_0, y_0) = (u, a).$$

EXERCICES

1. Déterminer le polynôme réduit équivalent modulo p en monôme x^k.
2. Construire une forme cubique $F(x_1, x_2, x_3)$ telle que la congruence

$$F(x_1, x_2, x_3) \equiv 0 \pmod 2$$

n'admette que la solution nulle.

3. Avec les notations de la démonstration du théorème de Warning, montrer que, pour $p \neq 2$, les composantes des solutions A_i $(i = 1, \ldots, s)$ vérifient les congruences

$$\sum_{i=1}^{s} a_1^{(i)} \equiv \ldots \equiv \sum_{i=1}^{s} a_n^{(i)} \equiv 0 \pmod p.$$

4. Généralisant le théorème 4 et l'exercice 3, montrer, avec ces notations, que l'on a les congruences

$$\sum_{i=1}^{s} (a_1^{(i)})^k \equiv \ldots \equiv \sum_{i=1}^{s} (a_n^{(i)})^k \equiv 0 \pmod p$$

pour $k = 0, 1, \ldots, p-2$.

5. Démontrer que si $F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)$ sont des polynômes à coefficients entiers de degrés $r_1, \ldots, r_m$ tels que $r_1 + \ldots + r_m < n$ et si le système des congruences

$$\left.\begin{aligned} F_1(x_1, \ldots, x_n) &\equiv 0 \pmod p \\ &\cdots \\ F_m(x_1, \ldots x_n) &\equiv 0 \pmod p \end{aligned}\right\} \tag{7}$$

a au moins une solution, alors il en a au moins deux.

6. Avec les hypothèses de l'exercice 5, montrer que le nombre de solutions du système (7) est divisible par p.

7. Montrer que si f est une forme quadratique sur le corps $\mathbf{F}_p$ de rang $\geqslant 2$ et $a \not\equiv 0 \pmod{p}$, alors la congruence

$$f \equiv a \pmod{p}$$

est résoluble.

8. Utilisant les théorèmes 2 et 3 de l'appendice, montrer que deux formes quadratiques non singulières sur le corps $\mathbf{F}_p (p \neq 2)$ sont équivalentes si et seulement si le produit de leurs déterminants est un carré.

9. Définir le groupe des classes de Witt de formes quadratiques sur le corps $\mathbf{F}_p (p \neq 2)$ (cf. exercice 5 du § 1 de l'appendice).

10. Montrer que le nombre de solutions non nulles de la congruence $f(x, y) \equiv 0 \pmod{p}$, où f est une forme quadratique de déterminant $d \not\equiv 0 \pmod{p}$, est égal à

$$(p-1)\left(1 + \left(\frac{-d}{p}\right)\right).$$

11. Utilisant le théorème 7 du § 1 de l'appendice, montrer que si $f(x_1, \ldots, x_n)$ est une forme quadratique de déterminant $d \not\equiv 0 \pmod{p}$, $p \neq 2$, alors le nombre de solutions non nulles de la congruence $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ est égal à

$$p^{n-1} - 1 + (p-1)\left(\frac{(-1)^{\frac{n}{2}} d}{p}\right) p^{\frac{n}{2}-1} \qquad \text{pour } n \text{ pair}$$

$$p^{n-1} - 1 \qquad \text{pour } n \text{ impair}$$

12. Avec les hypothèses de l'exercice 11, trouver le nombre de solutions de la congruence

$$f(x_1, \ldots, x_n) \equiv a \pmod{p}.$$

§ 2. — SOMMES TRIGONOMÉTRIQUES

1) Congruences et sommes trigonométriques

Dans ce paragraphe, nous considérerons encore les congruences modulo un nombre premier, mais d'un point de vue différent. Les théorèmes du § 1 donnent des résultats sur le nombre de solutions d'une congruence en liaison avec le degré et le nombre de variables du polynôme. Ici, c'est la grandeur du nombre premier p qui joue un rôle essentiel.

Nous avons dit au début de ce chapitre que pour que l'équation

$$\mathrm{F}(x_1, \ldots, x_n) = 0$$

soit résoluble en nombres entiers, il est nécessaire que les congruences $\mathrm{F} \equiv 0 \pmod{m}$ soient résolubles pour tous les entiers m; en fait, on a vu qu'il suffisait de considérer les cas où m est une puissance de nombre premier.

Nous allons voir que pour une classe très importante de polynômes, les congruences $\mathrm{F} \equiv 0 \pmod{p}$ sont automatiquement résolubles pour tout entier p assez grand.

DÉFINITION. — Un polynôme $\mathrm{F}(x_1, \ldots, x_n)$ à coefficients rationnels est dit *absolument irréductible* s'il n'est décomposable en produit de polynômes non triviaux dans aucune extension du corps des nombres rationnels.

Le théorème fondamental est le suivant :

THÉORÈME A. — *Si* $\mathrm{F}(x_1, \ldots, x_n)$ *est un polynôme absolument irréductible à coefficients entiers, alors la congurence*

$$\mathrm{F}(x_1, \ldots, x_n) \equiv 0 \pmod{p} \qquad (1)$$

est résoluble pour tout nombre premier p supérieur à un certain nombre (dépendant du polynôme F).

On a un résultat analogue pour les solutions non nulles d'un polynôme homogène F et pour les systèmes de congruences (pour des notions appropriées d'irréductibilité absolue).

Le théorème A est trivial pour $n = 1$ (tout polynôme à une variable de degré supérieur à 1 se décompose dans le corps des nombres complexes et le théorème est trivial pour les polynômes du premier degré). Pour $n = 2$ déjà, la démonstration utilise des méthodes plus profondes de géométrie algébrique. Dans le cas $n = 2$, le théorème A a été obtenu par A. Weil (A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, *Act. Sci. Ind.*, 1041, Paris, Hermann, 1948). Des variantes de cette démonstration figurent dans les travaux de S. Lang (S. Lang, Abelian varietics, Interscience Tracts, n° 7, New York, 1959) et A. Mattuck et J. Tate (On the inequality of Castelnuovo-Severi, *Abh. Math. Sem. Univ. Hamb.*, 1958, B. **22**, H. 3-4, 295-299).

Le passage de $n = 2$ au cas général s'effectue beaucoup plus simplement. C'est fait dans les travaux de L. B. Nisnevitch (Sur le nombre de points des variétés algébriques dans les corps premiers finis, *Dokl. A. N. URSS*, 1954, **99**, n° 1, 17-20) et de S. Lang et A. Weil (Number of points of variety in finite fields, *Am. J. Math.*, 1954, **76**, n° 4, 819-827).

Les ouvrages ci-dessus démontrent en fait plus que le théorème A; ainsi, on montre que si on fixe le polynôme F, le nombre $\mathrm{N}(p)$ de solutions de la congruence (1) tend vers l'infini quand le nombre premier p tend vers l'infini. Plus précisément encore, on a évalué la rapidité de croissance du nombre $\mathrm{N}(p)$. La formulation exacte de ce résultat est la suivante :

THÉORÈME B. — *Le nombre* $\mathrm{N}(\mathrm{F}, p)$ *de solutions de la congruence* (1) *satisfait à l'inégalité*

$$|\mathrm{N}(\mathrm{F}, p) - p^{n-1}| < \mathrm{C}(\mathrm{F}) p^{n-1-\frac{1}{2}},$$

la constante $\mathrm{C}(\mathrm{F})$ *dépendant seulement du polynôme* F *et non de p.*

L'unique procédé de démonstration actuellement connu du théorème A est de le déduire du théorème B. Nous ne pourrons pas donner ici de démonstration des théorèmes A et B car il faut des outils algébriques beaucoup plus élaborés que ceux dont nous disposons dans ce livre. Cependant, nous exposerons une méthode qui permet de démontrer ces théorèmes dans des cas particuliers; nous choisirons ici un de ces cas particuliers.

Tout repose sur le fait qu'on peut représenter le nombre de solutions de l'équation (1) comme somme de certaines racines $p^{\text{ièmes}}$ de l'unité. Les sommes de ce type sont dites trigonométriques.

Posons quelques notations. Si $f(x)$ ou $f(x_1, \ldots, x_n)$ est une fonction à valeurs complexes dont les valeurs dépendent seulement des classes résiduelles des nombres $x_1, \ldots, x_n$ modulo p, nous désignerons par

$$\sum_x f(x) \qquad \text{ou} \qquad \sum_{x_1, \ldots, x_n} f(x_1, \ldots, x_n)$$

les sommes étendues à toutes les valeurs x ou $x_1, \ldots, x_n$ d'un système complet de résidus modulo p et par

$$\sum_x{}' f(x)$$

la somme étendue à toutes les valeurs x d'un système réduit de résidus.

Soit ζ une racine primitive $p^{\text{ième}}$ de 1 fixée. On voit alors facilement que

$$\sum_x \zeta^{xy} = \begin{cases} p & \text{si} \quad y \equiv 0 \pmod p \\ 0 & \text{si} \quad y \not\equiv 0 \pmod p. \end{cases} \tag{2}$$

Ces égalités vont nous permettre d'obtenir une expression très simple du nombre de solutions de la congruence (1).

Considérons la somme

$$S = \sum_{x_1, \ldots, x_n} \sum_x \zeta^{xF(x_1, \ldots, x_n)}.$$

Si les valeurs $x_1, \ldots, x_n$ constituent une solution de la congruence (1), on a, en accord avec (2),

$$\sum_x \zeta^{xF(x_1, \ldots, x_n)} = p\ ;$$

si maintenant $F(x_1, \ldots, x_n) \not\equiv 0 \pmod p$, on a, toujours d'après (2),

$$\sum_x \zeta^{xF(x_1, \ldots, x_n)} = 0.$$

Ainsi $S = Np$, en désignant par N le nombre de solutions de la congruence (1). Énonçons ce résultat sous forme d'un théorème :

THÉORÈME 1. — *Le nombre* N *de solutions de la congruence* (1) est donné par

$$N = \frac{1}{p} \sum_{x, x_1, \ldots, x_n} \zeta^{xF(x_1, \ldots, x_n)}. \tag{3}$$

Séparons les p^n termes de la somme (3) tels que $x \equiv 0 \bmod p$; chacun de ces termes est égal à 1 et on a donc

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \sum_{x_1, \ldots, x_n} \zeta^{xF(x_1, \ldots, x_n)} \tag{4}$$

Écrite ainsi, la formule donnant N suggère le théorème B. Il suffit seulement de démontrer (mais toute la difficulté est là !) que quand p croît, la somme des termes restants croît plus lentement que son terme principal.

2) Sommes de puissances

Nous appliquerons les résultats qui précèdent au cas où le polynôme F est de la forme

$$F(x_1, \ldots, x_n) = a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n}, \quad a_i \not\equiv 0 \pmod p.$$

Nous supposerons $n \geqslant 3$ puisque pour $n = 1$ ou $n = 2$ le nombre de solutions de la congruence $F \equiv 0 \pmod p$ se calcule trivialement.

En accord avec la formule (4), le nombre de solutions de la congruence

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod p$$

est donné par la formule

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \sum_{x_1, \ldots, x_n} \zeta^{x\left(a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n}\right)},$$

qui peut aussi s'écrire

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{x_i} \zeta^{a_i x_i^{r_i}}. \tag{5}$$

Cette formule nous conduit à l'étude des sommes de la forme

$$\sum_y \zeta^{ay^r} \qquad (a \not\equiv 0 \pmod p)\ ;$$

il est facile de vérifier que

$$\sum_y \zeta^{ay^r} = \sum_x m(x)\zeta^{ax}, \tag{6}$$

en désignant par $m(x)$ le nombre de solutions en y de la congruence

$$y^r \equiv x \pmod{p}.$$

Il est clair que $m(0) = 1$; nous allons calculer $m(x)$ pour $x \not\equiv 0 \pmod{p}$. Soit g une racine primitive modulo p; alors

$$x \equiv g^k \pmod{p}, \tag{7}$$

l'exposant k étant défini de manière unique modulo $p-1$. Posant $y \equiv g_3^u \pmod{p}$, la congruence $y^r \equiv x \pmod{p}$ est équivalente à la congruence

$$ru \equiv k \pmod{(p-1)}. \tag{8}$$

D'après la théorie générale des congruences du premier degré, la congruence (8) a $d = (r, p-1)$ solutions en u ou n'a aucune solution suivant que k est divisible par d ou pas. Par suite,

$$m(x) = \begin{cases} d & \text{si} \quad k \equiv 0 \pmod{d} \\ 0 & \text{si} \quad k \not\equiv 0 \pmod{d}. \end{cases} \tag{9}$$

Donnons une autre évaluation plus utilisable du nombre $m(x)$. Soit ε une racine primitive d'ordre d de 1 et définissons pour tous les nombres entiers x relativement premiers à p des fonctions χ_s ($s = 0, 1, \ldots, p-1$) en posant

$$\chi_s(x) = \varepsilon^{ks} \tag{10}$$

où k vérifie la congruence (7) (d'après l'égalité $\varepsilon^{p-1} = 1$, la valeur ε^{ks} ne dépend pas du choix de k). Si $k \equiv 0 \pmod{d}$, alors $\varepsilon^{ks} = 1$ pour tout $s = 0, 1, \ldots, d-1$ et par suite la somme

$$\sum_{s=0}^{d-1} \chi_s(x)$$

est égale à d. Si maintenant $k \not\equiv 0 \pmod{d}$ alors $\varepsilon^k \neq 1$ et par suite

$$\sum_{s=0}^{d-1} \varepsilon^{ks} = \frac{\varepsilon^{kd} - 1}{\varepsilon^k - 1} = 0.$$

Rapprochant ce résultat des égalités (9), nous obtenons (pour x non divisible par p) la formule

$$m(x) = \sum_{s=0}^{d-1} \chi_s(x)$$

L'expression donnée plus haut pour $m(x)$ permet d'écrire l'égalité (6) sous la forme

$$\sum_y \zeta^{ay^r} = 1 + \sum_x{}' \sum_{s=0}^{d-1} \chi_s(x)\zeta^{ax}. \tag{11}$$

Les fonctions χ_s introduits ci-dessus possèdent, c'est clair, la propriété

$$\chi_s(xy) = \chi_s(x)\chi_s(y) \tag{12}$$

et s'appellent les *caractères multiplicatifs modulo p*. Étendons-les à tous les entiers x en posant $\chi_s(x) = 0$ si x est divisible par p. Il est clair que, pour cette définition, la propriété (12) est conservée. Le caractère $\chi_0(n)$ dont la valeur pour px est égale à 1 s'appelle le *caractère unité*.

Séparons dans la somme (11) les termes qui correspondent au caractère unité χ_0. Puisque

$$1 + \sum_x{}' \zeta^{ax} = \sum_x \zeta^{ax},$$

l'égalité (11) peut s'écrire sous la forme

$$\sum_y \zeta^{ay^r} = \sum_{s=1}^{d-1} \sum_x \chi_s(x)\zeta^{ax} \tag{13}$$

(ici on peut considérer que x parcourt un système complet de résidus modulo p, puisque $\chi_s(x) = 0$ pour $x \equiv 0 \pmod{p}$).

Soient χ un des caractères χ_s et a un nombre entier. L'expression

$$\sum_x \chi(x)\zeta^{ax}$$

s'appelle *somme de Gauss* et se désigne par $\tau_a(\chi)$.

Les formules (5) et (13) nous permettent de formuler le théorème suivant.

THÉORÈME 2. — *Le nombre* N *de solutions de la congruence*

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} = 0 \pmod{p}, \qquad a_i \not\equiv 0 \pmod{p} \tag{14}$$

est donné par la formule

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} \tau_{a_i x}(\chi_{i,s}), \tag{15}$$

dans laquelle $d_i = (r_i, p-1)$, *les caractères* $\chi_{i,s}$ *étant définis par l'égalité* (10) *avec* $d = d_i$.

Remarquons que si un des d_i est égal à 1, i. e. si r_i relativement premier avec $p-1$, alors dans la formule (15) la somme intérieure correspondante sera nulle (comme somme indexée par l'ensemble vide) et par suite dans ce cas on a la formule $N = p^{n-1}$. Cela est d'ailleurs clair directement puisque pour chaque choix des valeurs $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ il existe une valeur x_i et une seule pour laquelle la congruence (14) est satisfaite.

Le théorème 2 prend tout son sens grâce au fait que le module de la somme de Gauss peut être calculé exactement. Nous montrerons dans le point suivant que

$$|\tau_a(\chi)| = \sqrt{p} \quad \text{pour} \quad a \not\equiv 0 \pmod p \quad \text{et} \quad \chi \neq \chi_0$$

(cf. aussi exercice 8).

Voyons ce que donne le théorème (2) en utilisant ce résultat. Il résulte de la formule (15) que

$$|N - p^{n-1}| \leqslant \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} |\tau_{a_i x}(\chi_{i,s})|$$

$$= \frac{1}{p}(p-1) \prod_{i=1}^{n} (d_i - 1) p^{\frac{1}{2}} = (p-1) p^{\frac{n}{2}-1} \prod_{i=1}^{n} (d_i - 1).$$

Nous obtenons ainsi le théorème.

THÉORÈME 3. — *Le nombre* N *de solutions de la congruence*

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod p$$

pour tous les p premiers ne divisant pas $a_1, \ldots, a_n$ *satisfait à l'inégalité*

$$|N - p^{n-1}| \leqslant C(p-1) p^{\frac{n}{2}-1} \tag{16}$$

avec

$$C = (d_1 - 1) \ldots (d_n - 1), \qquad d_i = (r_i, p-1).$$

Pour $n \geqslant 3$, on peut obtenir le théorème B, pour les polynômes de la forme considérée, à partir du théorème 3. En effet

$$|N - p^{n-1}| \leqslant C p^{\frac{n}{2}} \leqslant C p^{n-1-\frac{1}{2}}$$

Remarquons, en passant, que l'inégalité (16) que nous avons obtenue pour $n > 3$ est plus précise que l'inégalité du théorème B.

Remarque. — Pour démontrer le théorème 3, il suffirait, d'après (5), de connaître une estimation du module de la somme $\sum_x \zeta^{ax^r}$. On peut obtenir une telle estimation plus rapidement, sans utiliser les sommes de Gauss (voir exercices 9 à 12 dus à H. M. Korobof). Nous exposons ici la démonstration avec les sommes de Gauss car les sommes de Gauss ont de nombreuses autres applications en théorie des nombres.

3) Module des sommes de Gauss

Considérons l'ensemble $\mathcal{F}$ de toutes les fonctions $f(x)$ à valeurs complexes définies pour x entier rationnel et telles que $f(x) \equiv f(y)$ si $x \equiv y \pmod p$. Puisque chaque fonction $f(x) \in \mathcal{F}$ est définie par ses valeurs sur un système complet de résidus modulo p, alors $\mathcal{F}$ est un espace vectoriel de dimension p sur le corps des nombres complexes. Introduisons sur $\mathcal{F}$ un produit scalaire hermitien en posant

$$(f, g) = \frac{1}{p} \sum_x f(x) \overline{g(x)} \qquad (f, g \in \mathcal{F}).$$

Une simple vérification montre que, pour ce produit scalaire, les p fonctions

$$f_a(x) = \zeta^{-ax} \qquad (a \text{ résidu mod } p) \tag{17}$$

forment une base orthonormale dans $\mathcal{F}$. En effet, d'après (2),

$$(f_a, f_{a'}) = \frac{1}{p} \sum_x \zeta^{(a'-a)x} = \begin{cases} 1 & \text{pour} \quad a \equiv a' \pmod p \\ 0 & \text{pour} \quad a \not\equiv a' \pmod p. \end{cases}$$

Les fonctions (17) qui possèdent la propriété

$$f_a(x+y) = f_a(x) f_a(y)$$

sont appelées des *caractères additifs modulo p*. Cherchons les coordonnées d'un caractère multiplicatif χ dans la base (17). Soit

$$\chi = \sum_a \alpha_a f_a. \tag{18}$$

Alors

$$\alpha_a = (\chi, f_a) = \frac{1}{p} \sum_x \chi(x) \zeta^{ax} = \frac{1}{p} \tau_a(\chi). \tag{19}$$

Nous voyons ainsi que les sommes de Gauss $\tau_a(\chi)$ $\left(\text{à } \frac{1}{p} \text{ près}\right)$ sont les coordonnées du caractère multiplicatif χ dans la base des caractères additifs f_a.

Pour obtenir une importante relation entre les coordonnées α_a (et par suite entre les sommes de Gauss $\tau_a(\chi)$), multiplions l'égalité

$$\chi(x) = \sum_a \alpha_a f_a(x) \tag{20}$$

par χ_c, où $c \not\equiv 0 \pmod p$, et remplaçons l'indice de sommation a par ac :

$$\chi(cx) = \sum_a \chi(c)\alpha_{ac} f_{ac}(x) = \sum_a \chi(c)\alpha_{ac} f_a(cx).$$

Comparant ceci avec (20), nous obtenons

$$\alpha_a = \chi(c)\alpha_{ac}. \tag{21}$$

Supposant ici $a = 1$ et remarquant que $|\chi(c)| = 1$, nous trouvons

$$|\alpha_c| = |\alpha_1| \qquad \text{pour } c \not\equiv 0 \pmod p. \tag{22}$$

Supposons maintenant que le caractère χ est distinct du caractère unité χ_0. Alors on peut choisir le nombre c (relativement premier avec p) tel que $\chi(c) \neq 1$ et l'égalité (21) pour $a = 0$ donne

$$\alpha_0 = 0. \tag{23}$$

Démontrons maintenant le résultat annoncé donnant le module de la somme de Gauss.

THÉORÈME 4. — *Si χ est un caractère multiplicatif modulo p, différent du caractère unité χ_0 et a un nombre entier relativement premier avec p, alors*

$$|\tau_a(\chi)| = \sqrt{p}.$$

DÉMONSTRATION. — Considérons dans l'espace $\mathcal{F}$ le produit scalaire (χ, χ). Puisque $|\chi(x)| = 1$ pour $x \not\equiv 0 \pmod p$, alors

$$(\chi, \chi) = \frac{1}{p}\sum_x \chi(x)\overline{\chi(x)} = \frac{p-1}{p}.$$

D'autre part, en utilisant l'expression (18) et en tenant compte de (22) et (23) nous trouvons

$$(\chi, \chi) = \sum_a |\alpha_a|^2 = (p-1)|\alpha_c|^2.$$

La réunion de ces deux résultats nous donne l'égalité

$$|\alpha_c| = \frac{1}{\sqrt{p}} \qquad (c \not\equiv 0 \pmod p),$$

d'où le résultat, d'après la formule (19).

EXERCICES

1. Montrer que le théorème A n'est pas vrai pour les solutions non nulles du polynôme $F = x^2 + y^2$ mais que, par contre, le théorème B est vrai pour le polynôme $F = x^2 - y^2$. Bien entendu, ces polynômes ne sont pas absolument irréductibles.

2. Soit $\varphi(x)$ une fonction définie pour tous les nombres entiers x premiers avec p et prenant des valeurs complexes différentes de zéro. Montrer que si $\varphi(x) = \varphi(y)$ pour $x \equiv y \pmod p$ et $\varphi(xy) = \varphi(x)\varphi(y)$, alors cette fonction coïncide avec une des fonctions $\chi_s(x) = \varepsilon^{ks}$, ε étant une racine primitive $(p-1)$-ème de 1 (k est défini par la congruence (7)).

3. Démontrer que toute fonction $f(x)$ de la variable entière x à valeurs complexes non nulles qui dépend seulement de la classe résiduelle de x modulo p et telle que $f(x+y) = f(x)f(y)$ est de la forme $f(x) = \zeta^{tx}$, où t est un certain entier et ζ une racine d'ordre p de 1.

4. Soit $p \neq 2$. Démontrer que le caractère $x = \chi_1$ défini par l'égalité (10) pour $d = 2$ (et $s = 1$) coïncide avec le symbole de Legendre :

$$\chi(x) = \left(\frac{x}{p}\right)$$

(ce caractère est appelé le *caractère quadratique* modulo p).

5. Supposons $ab \not\equiv 0 \pmod p$ et soit χ le caractère quadratique modulo $p \neq 2$. Démontrer la relation

$$\tau_a(\chi)\tau_b(\chi) = \left(\frac{-ab}{p}\right)p$$

pour les deux sommes de Gauss $\tau_a(\chi)$ et $\tau_b(\chi)$.

6. Avec les mêmes notations, démontrer que

$$\sum_x{}' \tau_x(\chi) = 0.$$

7. Résoudre les exercices 10, 11 et 12 du paragraphe précédent en utilisant le théorème 2 et les résultats des exercices 5 et 6.

8. Soient χ un caractère multiplicatif modulo p, différent du caractère χ_0 et $a \not\equiv 0 \pmod p$. Montrer que

$$|\tau_a(\chi)|^2 = \tau_a(\chi)\overline{\tau_a(\chi)} = p\ ;$$

en déduire une nouvelle démonstration du théorème 4.

9. Soient $f(x)$ un polynôme à coefficients entiers et ζ une racine primitive d'ordre m de 1. On pose $S_a = \sum_{x \bmod m} \zeta^{af(x)}$. Démontrer que l'on a

$$\sum_{a \bmod m} |S_a|^2 = m \sum_{c \bmod m} N(c)^2,$$

en désignant par $N(c)$ le nombre de solutions de la congruence $f(x) \equiv c \pmod m$.

10. Soit ζ une racine primitive d'ordre p premier de 1 et posons $T_a = \sum_x{}' \zeta^{ax^r}$.

Démontrer que

$$\sum_a{}' |T_a|^2 = p(p-1)(d-1),$$

avec $d = (r, p-1)$.

11. Avec les mêmes notations, montrer que les sommes T_a, $a \not\equiv 0 \pmod p$, sont décomposables en d groupes de $\frac{p-1}{d}$ sommes égales entre elles. Utilisant ce résultat et celui de l'exercice 1, en déduire que

$$|T_a| < d\sqrt{p}, \qquad a \not\equiv 0 \pmod p.$$

12. Remarquant que $\sum_a{}' T_a = 0$, obtenir pour T_a l'estimation meilleure

$$|T_a| \leqslant (d-1)\sqrt{p}, \qquad a \not\equiv 0 \pmod p$$

(D'après la formule (5), cette estimation nous donne une autre démonstration du théorème 3).

13. Montrer que la congruence

$$3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod p.$$

a une solution non nulle pour tout p premier.

§ 3. — LES NOMBRES p-ADIQUES

1) Les nombres entiers p-adiques

Passons maintenant aux congruences modulo une puissance d'un nombre premier. Étudions un exemple. Soit la congruence

$$x^2 \equiv 2 \pmod{7^n}.$$

Pour $n = 1$, cette congruence a deux solutions :

$$x_0 = \pm 3 \pmod 7. \tag{1}$$

Soit maintenant $n = 2$. De

$$x^2 \equiv 2 \pmod{7^2}, \tag{2}$$

résulte $x^2 \equiv 2 \pmod 7$ et par suite on peut chercher les solutions de la congruence (2) sous la forme $x_0 + 7t_1$, x_0 étant un des nombres définis par la congruence (1). Nous rechercherons les solutions de la forme $x_1 = 3 + 7t_1$ (les solutions de la forme $-3 + 7t_1$ s'étudient de la même manière). Portant cette expression de x_1 dans (2), nous obtenons

$$\begin{aligned} (3 + 7t_1)^2 &\equiv 2 \pmod{7^2} \\ 9 + 6.7t_1 + 7^2t_1^2 &\equiv 2 \pmod{7^2} \\ 1 + 6t_1 &\equiv 0 \pmod 7 \\ t_1 &\equiv 1 \pmod 7. \end{aligned}$$

D'où la solution $x_1 \equiv 3 + 7.1 \pmod{7^2}$.

De même, pour $n = 3$, on pose $x_2 = x_1 + 7^2t_2$ et à partir de la congruence

$$(3 + 7 + 7^2t_2)^2 \equiv 2 \pmod{7^3}$$

on obtient $t_2 \equiv 2 \pmod 7$, i. e.

$$x_2 \equiv 3 + 7.1 + 7^2.2 \pmod{7^3}.$$

Il est facile de voir que ce procédé s'étend indéfiniment. On obtient ainsi une suite

$$x_0, x_1, \ldots, x_n, \ldots \tag{3}$$

qui possède les propriétés :

$$\begin{aligned} x_0 &\equiv 3 \pmod 7 \\ x_n &\equiv x_{n-1} \pmod{7^n} \\ x_n^2 &\equiv 2 \pmod{7^{n+1}}. \end{aligned}$$

Le procédé de construction de la suite (3) rappelle le procédé d'extraction de la racine carrée de 2. En effet, le calcul de $\sqrt{2}$ consiste en la construction d'une suite de nombres rationnels $r_1, r_2, \ldots, r_n, \ldots$ dont les carrés sont aussi proches que l'on désire de 2, par exemple

$$|r_n^2 - 2| < \frac{1}{10^n}.$$

Ici, on construit une suite de nombres entiers $x_0, x_1, \ldots, x_n, \ldots$ pour lesquels $x_n^2 - 2$ est divisible par 7^{n+1}. Cette analogie sera plus claire si nous convenons que deux nombres sont proches (plus exactement p-proches, p étant un nombre premier) quand leur différence est divisible par une puissance

de p suffisamment grande. On pourra dire alors que les carrés des nombres de la suite (3) sont, quand n croît, aussi 7-proches que l'on veut de 2.

La construction de la suite $\{r_n\}$ définit le nombre réel $\sqrt{2}$. On peut dire que la suite (3) définit également un nombre α d'une « nouvelle nature » et tel, par suite, que $\alpha^2 = 2$.

Attirons l'attention du lecteur sur le fait suivant. Si une suite de nombres rationnels $\{r'_n\}$ est telle que $|r_n - r'_n| < \frac{1}{10^n}$ pour tout n, alors sa limite sera encore $\sqrt{2}$. Nous supposerons donc également qu'une suite $\{x'_n\}$ telle que $x_n \equiv x'_n \pmod{7^{n+1}}$ définit le même « nouveau nombre » α (pour cette nouvelle suite $\{x'_n\}$, il est évident que l'on a aussi $x'^2_n \equiv 2 \pmod{7^{n+1}}$ et $x'_n \equiv x'_{n-1} \pmod 7$)).

Ces remarques nous conduisent à la définition suivante.

DÉFINITION. — *Soit p un nombre premier quelconque. Une suite de nombres entiers*

$$\{x_n\} = \{x_0, x_1, \ldots, x_n, \ldots\},$$

tels que

$$x_n \equiv x_{n-1} \pmod{p^n} \tag{4}$$

définit un nouvel objet appelé nombre entier p-adique. Par définition deux suites $\{x_n\}$ et $\{x'_n\}$ définiront le même nombre entier p-adique si et seulement si $x_n \equiv x'_n \pmod{p_{n+1}}$ pour tout $n \geqslant 0$.

Nous exprimerons le fait que la suite $\{x_n\}$ définit le nombre entier p-adique α par le symbole :

$$\{x_n\} \to \alpha.$$

Nous désignerons par $\mathbf{Z}_p$ l'ensemble de tous les nombres entiers p-adiques. Pour les distinguer des nombres entiers p-adiques, les nombres entiers habituels seront appelés entiers rationnels.

A chaque nombre entier rationnel x, nous associerons le nombre entier p-adique défini par la suite $\{x, x, \ldots, x, \ldots\}$ et nous désignerons par la même lettre x ce nombre entier p-adique. Deux entiers rationnels x et y distincts définissent deux entiers p-adiques distincts. En effet, leur égalité comme entiers p-adiques entraîne, pour tout n, la congruence $x \equiv y \pmod{p^n}$, ce qui exige $x = y$. Par suite, nous pourrons considérer l'ensemble $\mathbf{Z}$ des entiers rationnels comme un sous-ensemble de l'ensemble $\mathbf{Z}_p$ des nombres entiers p-adiques.

Pour concrétiser plus clairement l'ensemble $\mathbf{Z}_p$, donnons un procédé pour choisir une suite standard dans l'ensemble de toutes les suites définissant un nombre entier p-adique donné.

Soit un nombre entier p-adique défini par une suite $\{x_n\}$. Désignons par $\bar{x}_n$ le plus petit nombre positif ou nul congru à x_n modulo p^{n+1} :

$$x_n \equiv \bar{x}_n \pmod{p^{n+1}} \tag{5}$$

$$0 \leqslant \bar{x}_n < p^{n+1}. \tag{6}$$

La congruence (5) montre que

$$\bar{x}_n \equiv x_n \equiv x_{n+1} \equiv \bar{x}_{n+1} \pmod{p^n} ;$$

ainsi, la suite $\{\bar{x}_n\}$ définit un nombre entier p-adique, qui est le même que celui défini par la suite $\{x_n\}$. Une suite dont tous les termes satisfont aux conditions (4) et (6) sera dite *canonique*. Ainsi, chaque entier p-adique est défini par une suite canonique.

Il est facile de voir que deux suites canoniques différentes définissent des entiers p-adiques différents. En effet, si deux suites canoniques $\{\bar{x}_n\}$ et $\{\bar{y}_n\}$ définissent le même entier p-adique, alors, d'après les congruences

$$\bar{x}_n \equiv \bar{y}_n \pmod{p^{n+1}}$$

et les conditions $0 \leqslant \bar{x}_n < p^{n+1}$, $0 \leqslant \bar{y}_n < p^{n+1}$, on a $\bar{x}_n = \bar{y}_n$ pour tout $n \geqslant 0$. Ainsi, les nombres entiers p-adiques sont en correspondance biunivoque avec les suites canoniques. La condition (4) entraîne que

$$\bar{x}_{n+1} = \bar{x}_n + a_{n+1}p^{n+1},$$

et, puisque $0 \leqslant \bar{x}_{n+1} < p^{n+2}$, on a $0 \leqslant a_{n+1} < p$; toute suite canonique est donc de la forme

$$\{a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots\},$$

avec $0 \leqslant a_i < p$. Il est évident que, réciproquement, toute suite de cette forme est une suite canonique définissant un nombre entier p-adique. Il est facile de démontrer à partir de là que l'ensemble des suites canoniques et par conséquent l'ensemble des entiers p-adiques, ont la puissance du continu.

2) L'anneau des nombres entiers p-adiques

DÉFINITION. — *On appelle somme et produit de deux nombres entiers p-adiques α et β définis par les suites $\{x_n\}$ et $\{y_n\}$ les nombres entiers p-adiques définis respectivement par les suites $\{x_n + y_n\}$ et $\{x_n y_n\}$.*

Pour que cette définition ait un sens, il faut montrer que les suites $\{x_n + y_n\}$ et $\{x_n y_n\}$ définissent des nombres entiers p-adiques et que ces nombres dépendent seulement de α et β et non du choix des suites qui les définissent.

La démonstration de ces propriétés est triviale et nous l'omettrons.

Il est clair à partir de ces définitions que pour ces opérations, les entiers p-adiques forment un anneau commutatif contenant comme sous-anneau l'anneau $\mathbf{Z}$ des entiers rationnels.

La notion de divisibilité se définit ici comme dans tout anneau (voir appendice § 4-1)) : α est divisible par β s'il existe un entier p-adique γ tel que $\alpha = \beta\gamma$. Pour étudier les propriétés de divisibilité, il est important de connaître les entiers p-adiques qui admettent un inverse; ces nombres seront appelés diviseurs de l'unité, ou unités. Nous les appellerons aussi *unités p-adiques.*

THÉORÈME 1. — *Un nombre entier p-adique α défini par une suite $\{x_0, x_1, \ldots, x_n, \ldots\}$ est une unité si et seulement si $x_0 \not\equiv 0 \pmod p$.*

DÉMONSTRATION. — Supposons que α est une unité. Il existe alors un entier p-adique β tel que $\alpha\beta = 1$. Si β est défini par la suite $\{y_n\}$, la condition $\alpha\beta = 1$ signifie que

$$x_n y_n \equiv 1 \pmod{p^{n+1}}. \tag{7}$$

En particulier $x_0 y_0 \equiv 1 \pmod p$, d'où $x_0 \not\equiv 0 \pmod p$. Réciproquement supposons $x_0 \not\equiv 0 \pmod p$. Il résulte facilement de (4) que

$$x_n \equiv x_{n-1} \equiv \ldots \equiv x_0 \pmod p$$

d'où $x_n \not\equiv 0 \pmod p$. Par suite, pour tout n, on peut trouver y_n tel que la congruence (7) soit vérifiée. Puisque $x_n \equiv x_{n-1} \pmod{p^n}$ et $x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n}$, alors $y_n \equiv y_{n-1} \pmod{p_n}$. Cela signifie que la suite $\{y_n\}$ définit un nombre entier p-adique β, qui est l'inverse de α d'après (7) .

Ce théorème entraîne qu'un nombre entier rationnel a, considéré comme un élément de l'anneau $\mathbf{Z}_p$, est une unité si et seulement si $a \not\equiv 0 \pmod p$. Si cette condition est remplie, alors $a^{-1} \in \mathbf{Z}_p$; il en résulte que tout entier rationnel b est divisible par a dans $\mathbf{Z}_p$, i. e. tout nombre rationnel de la forme $\frac{b}{a}$ où a et b sont entiers et $a \not\equiv 0 \pmod p$ appartient à $\mathbf{Z}_p$. Les nombres rationnels de cette forme sont appelés *p-entiers.* Ils forment un anneau de manière évidente. On peut formuler ainsi ce résultat :

COROLLAIRE. — *L'anneau $\mathbf{Z}_p$ des nombres entiers p-adiques contient un sous-anneau isomorphe à l'anneau des nombres rationnels p-entiers.*

THÉORÈME 2. — *Tout entier p-adique α différent de 0 s'écrit de manière unique sous la forme*

$$\alpha = p^m \varepsilon \tag{8}$$

où ε est une unité de l'anneau $\mathbf{Z}_p$.

DÉMONSTRATION. — Si α est une unité, alors (8) est satisfait pour $m = 0$. Supposons que $\{x_n\} \to \alpha$ et que α n'est pas une unité, i. e. $x_0 \not\equiv 0 \pmod p$. Puisque $\alpha \neq 0$, les congruences $x_n \equiv 0 \pmod{p^{n+1}}$ ne peuvent pas avoir lieu pour tout n; soit m le plus petit entier tel que :

$$x_m \not\equiv 0 \pmod{p^{m+1}}. \tag{9}$$

Pour $s \geqslant 0$,

$$x_{m+s} \equiv x_{m-1} \equiv 0 \pmod{p^m}$$

et par suite le nombre $y_s = \frac{x_{m+s}}{p^m}$ est un entier. De la congruence

$$p^m y_s - p^m y_{s-1} = x_{m+s} - x_{m+s-1} \equiv 0 \pmod{p^{m+s}},$$

il résulte que

$$y_s \equiv y_{s-1} \pmod{p^s}$$

pour tout $s \geqslant 0$. La suite $\{y_s\}$ définit donc $\varepsilon \in \mathbf{Z}_p$. Puisque $y_0 = \frac{x_m}{p_m} \not\equiv 0 \pmod p$, il résulte alors du théorème 1 que ε est une unité. Enfin, la congruence $p^m y_s = x_{m+s} \equiv x_s \pmod{p^{s+1}}$ entraîne que $p^m \varepsilon = \alpha$, i. e. on a la décomposition (8).

Supposons maintenant que α admette une autre décomposition $\alpha = p^k \eta$ avec $k \geqslant 0$ et η une unité. Si $\{z_s\} \to \eta$, alors

$$p^m y_s \equiv p^k z_s \pmod{p^{s+1}} \tag{10}$$

pour tout $s \geqslant 0$ et, d'après le théorème 1, tous les y_s et z_s ne sont pas divisibles par p puisque ε et η sont des unités. Faisant $s = m$ dans la congruence (10), on obtient

$$p^m y_m \equiv p^k z_m \not\equiv 0 \pmod{p^{m+1}},$$

d'où l'inégalité $k \leqslant m$. Par symétrie, on a de même $m \leqslant k$, i. e. $k = m$. Remplaçons s par $s + m$ dans la congruence (10) et simplifions par p^m. Nous obtenons

$$y_{m+s} \equiv z_{m+s} \pmod{p^{s+1}},$$

et, puisque $y_{m+s} \equiv y_s \pmod{p^{s+1}}$ et $z_{m+s} \equiv z_s \pmod{p^{s+1}}$ d'après (4), on a bien, pour tout $s \geqslant 0$,

$$y_s \equiv z_s \pmod{p^{s+1}},$$

ce qui montre que $\varepsilon = \eta$.

COROLLAIRE 1. — *Un nombre entier p-adique α défini par une suite $\{x_n$ est divisible par p^k si et seulement si $x_n \equiv 0 \pmod{p^{n+1}}$ pour tout*

$$n = 0, 1, \ldots, k-1.$$

En effet, l'exposant m dans (8) a été défini comme le plus petit entie pour lequel on a (9).

COROLLAIRE 2. — *L'anneau $\mathbf{Z}_p$ n'a pas de diviseur de zéro.*

En effet, si $\alpha \neq 0$ et $\beta \neq 0$, alors on a les représentations $\alpha = p^m\varepsilon$ $\beta = p^k\eta$, ε et η étant des unités (ε et η ont donc des inverses ε^{-1} et η^{-1} da l'anneau $\mathbf{Z}_p$). Si $\alpha\beta = 0$, alors, multipliant l'égalité $p^{m+k}\varepsilon\eta = 0$ par $\varepsilon^{-1}\eta^-$ nous obtiendrions $p^{m+k} = 0$, ce qui est impossible.

DÉFINITION. — *Le nombre m qui figure dans la décomposition* (8) *d'u nombre entier p-adique α différent de zéro s'appelle la valuation p-adique α et se désigne par $\nu_p(\alpha)$.*

Si le nombre premier p est fixé sans ambiguïté, on appellera simpleme ce nombre la valuation de α et on le désignera par $\nu(\alpha)$. Pour que la fon tion $\nu(\alpha)$ soit définie pour tous les nombres entiers p-adiques, nous pos rons $\nu(0) = \infty$ (cette définition formelle est justifiée par le fait que 0 divisible par des puissances de p arbitrairement grandes).

Une démonstration immédiate donne les propriétés suivantes de la valu tion :

$$\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta) \qquad (1$$

$$\nu(\alpha + \beta) \geqslant \min(\nu(\alpha), \nu(\beta)) \qquad (1$$

$$\nu(\alpha + \beta) = \min(\nu(\alpha), \nu(\beta)), \quad \text{si} \quad \nu(\alpha) \neq (\beta). \qquad (1$$

Les propriétés de divisibilité des nombres entiers p-adiques s'exprime très simplement au moyen de la valuation. En particulier, on obtient fac lement, à partir du théorème 3 :

COROLLAIRE 3. — *Un nombre entier p-adique α est divisible par β si et seul ment si $\nu(\alpha) \geqslant \nu(\beta)$.*

Ainsi, l'arithmétique de l'anneau $\mathbf{Z}_p$ est très simple. Il y a un seul éléme premier (à un élément associé près), c'est le nombre p. Tout élément de différent de 0 est caractérisé par sa valuation et son unité.

En conclusion, nous étudierons les congruences dans l'anneau $\mathbf{Z}_p$. L congruence est définie ici comme pour les nombres entiers et plus généra ment pour tout anneau (cf. appendice § 4-1)) : $\alpha \equiv \beta \pmod{\gamma}$ signifie qu $\alpha - \beta$ est divisible par γ. Si $\gamma = p^n\varepsilon$, ε étant une unité, alors la congruenc modulo γ est équivalente à la congruence modulo p^n. Par suite, on peu se limiter à l'examen des congruences modulo p^n.

THÉORÈME 3. — *Tout nombre entier p-adique est congru à un nombre entier rationnel modulo p^n. Deux nombres entiers rationnels sont congrus modulo p^n dans l'anneau $\mathbf{Z}_p$ si et seulement s'ils sont congrus modulo p^n dans l'anneau $\mathbf{Z}$.*

DÉMONSTRATION. — Pour démontrer la première affirmation, établissons que si α est un nombre entier p-adique et $\{x_n\}$ une suite de nombres entiers rationnels qui le définit, alors

$$\alpha \equiv x_{n-1} \pmod{p^n}. \qquad (14)$$

Puisque x_{n-1} est défini par la suite $\{x_{n-1}, x_{n-1}, \ldots\}$, une suite définissant $\alpha - x_{n-1}$ est $\{x_0 - x_{n-1}, x_1 - x_{n-1}, \ldots\}$. Appliquons à l'entier p-adique $\alpha - x_{n-1}$ le corollaire 1 du théorème 2. Nous voyons que la congruence (14) équivaut aux congruences

$$x_n - x_{n-1} \equiv 0 \pmod{p^{k+1}}, \qquad k = 0, 1, \ldots, n-1,$$

dont la vérification découle de la condition (4) de la définition des entiers p-adiques.

Démontrons maintenant que pour deux entiers rationnels x et y, la congruence modulo p^n dans $\mathbf{Z}_p$ équivaut à la congruence modulo p^n dans $\mathbf{Z}$. Posons

$$x - y = p^m a, \qquad a \not\equiv 0 \pmod{p} \qquad (15)$$

(on suppose $x \neq y$). La congruence

$$x \equiv y \pmod{p^n}. \qquad (16)$$

dans l'anneau $\mathbf{Z}$ est équivalente à $n \leqslant m$. D'autre part (15) est la représentation (8) du nombre $x - y$ puisque a est une unité p-adique. Par suite $\nu_p(x - y) = m$ et la condition $n \leqslant m$ peut s'écrire sous la forme $\nu_p(x-y) \geqslant n$, ce qui est équivalent à la congruence (16) dans $\mathbf{Z}_p$ puisque $\nu(p^n) = n$ (cf. corollaire 3 du théorème 2).

COROLLAIRE. — *Le nombre des classes résiduelles modulo p^n dans $\mathbf{Z}_p$ est égal à p^n.*

3) Fractions p-adiques

Puisque l'anneau $\mathbf{Z}_p$ est sans diviseur de zéro (corollaire 2 du théorème 2), on peut l'inclure dans un corps en utilisant la construction du corps des fractions d'un domaine d'intégrité. Ici, cette construction nous conduit à étudier les fractions de la forme $\frac{\alpha}{p^k}$, où α est un entier p-adique quelconque et $k \geqslant 0$. La fraction est ici simplement un symbole commode pour désigner la paire (α, p^k).

DÉFINITION. — *Le symbole fractionnaire* $\frac{\alpha}{p^k}$, $\alpha \in \mathbf{Z}_p$, $k \geqslant 0$ *définit un nombre fractionnaire p-adique ou, plus simplement, un nombre p-adique. Deux fractions* $\frac{\alpha}{p^k}$ *et* $\frac{\beta}{p^m}$ *définissent le même nombre p-adique si* $\alpha p^m = \beta p^k$ *dans* $\mathbf{Z}$.

Nous désignerons par $\mathbf{Q}_p$ l'ensemble de tous les nombres p-adiques.

Tout nombre entier p-adique définit un élément $\frac{\alpha}{1} = \frac{\alpha}{p^0}$ de $\mathbf{Q}_p$. Il est clair que des nombres entiers p-adiques différents définissent des nombres p-adiques différents de $\mathbf{Q}_p$. Par suite, nous pouvons considérer $\mathbf{Z}_p$ comme un sous-ensemble de l'ensemble $\mathbf{Q}_p$.

Les opérations dans $\mathbf{Q}_p$ sont définies par les règles :

$$\frac{\alpha}{p^k} + \frac{\beta}{p^m} = \frac{\alpha p^m + \beta p^k}{p^{k+m}}$$

$$\frac{\alpha}{p^k} \cdot \frac{\beta}{p^m} = \frac{\alpha\beta}{p^{k+m}}.$$

Une vérification triviale montre que le résultat des opérations ci-dessus ne dépend pas du choix des fractions qui définissent les éléments correspondants de $\mathbf{Q}_p$ et que $\mathbf{Q}_p$ est un corps pour ces opérations, le *corps des nombres p-adiques*. Il est évident que la caractéristique du corps $\mathbf{Q}_p$ est nulle et par suite il contient le corps des nombres rationnels.

THÉORÈME 4. — *Tout nombre p-adique* $\xi \neq 0$ *est représentable de manière unique sous la forme*

$$\xi = p^m \varepsilon, \qquad (1$$

où m est un entier rationnel et ε *une unité de* $\mathbf{Z}_p$.

DÉMONSTRATION. — Soit $\xi = \frac{\alpha}{p^k}$, $\alpha \in \mathbf{Z}_p$. D'après le théorème 2, $\alpha = p^l \varepsilon$, $l \geqslant 0$, où ε est une unité de l'anneau $\mathbf{Z}_p$. Ainsi $\xi = p^m \varepsilon$ avec $m = l - k$. L'unicité de la représentation (17) découle de l'affirmation correspondante pour les nombres entiers p-adiques démontrée dans le théorème 2.

La notion de valuation introduite ci-dessus se généralise facilement aux nombres p-adiques. Nous poserons

$$\nu_p(\xi) = m,$$

où m est l'exposant dans la représentation (17). On vérifie facilement que les propriétés (11), (12) et (13) sont encore valables dans le corps $\mathbf{Q}_p$. Il est clair que le nombre p-adique ξ est un nombre entier p-adique si et seulement si $\nu_p(\xi) \geqslant 0$.

4) Convergence dans le corps des nombres p-adiques

Dans le sous-paragraphe 1), nous avons attiré l'attention sur l'analogie qui existe entre les nombres entiers p-adiques et les nombres réels : les uns et les autres sont définis par des suites de nombres rationnels.

Puisque chaque nombre réel est, comme on le sait, la limite de toute suite de nombres rationnels qui le définit, il est intuitif de penser qu'il en sera de même pour les nombres p-adiques pour une notion de convergence appropriée. Pour définir la limite d'une suite de nombres réels, on s'appuie essentiellement sur la notion de proximité : deux nombres réels ou rationnels sont considérés comme proches si la valeur absolue de leur différence est suffisamment petite. Pour définir la convergence dans le corps des nombres p-adiques, il faut donc définir la notion de nombres p-adiques proches.

Dans l'exemple du début de ce paragraphe, nous avons déjà parlé de la p-proximité de deux nombres entiers rationnels x et y en entendant par là que la différence $x - y$ est divisible par des puissances de p suffisamment grandes. Ainsi, apparaît une nouvelle analogie entre les nombres réels et p-adiques pour la notion de proximité. Si on utilise la notion de p-valuation ν_p, il est clair que la p-proximité de x et y sera caractérisée par la valeur du nombre $\nu_p(x - y)$. Cela signifie que deux nombres p-adiques quelconques ξ et η (non nécessairement entiers) doivent être considérés comme proches si la valeur $\nu_p(x - y)$ est suffisamment grande. En d'autres termes, les nombres p-adiques « petits » sont caractérisés par de grandes valeurs de leurs valuations.

Après ces remarques préparatoires, passons à une définition précise.

DÉFINITION. — *Une suite*

$$\{\xi_n\} = \{\xi_0, \xi_1, \ldots, \xi_n, \ldots\}$$

de nombres p-adiques est dite convergente vers un nombre p-adique ξ (*ce que nous noterons* $\lim_{n\to\infty} \xi_n = \xi$ *ou* $\{\xi_n\} \to \xi$) *si*

$$\lim_{n\to\infty} \nu_p(\xi_n - \xi) = \infty.$$

On peut donner à la définition ci-dessus un aspect moins surprenant en considérant, au lieu de l'exposant ν_p défini sur le corps $\mathbf{Q}_p$, une autre fonction, à valeurs réelles positives, qui tend vers 0 lorsque l'exposant tend vers l'infini. Par exemple, choisissant un nombre réel ρ tel que $0 < \rho < 1$, posons

$$\varphi_\rho(\xi) = \begin{cases} \rho^{\nu_p(\xi)} & \text{si} \quad \xi \neq 0 \\ 0 & \text{si} \quad \xi = 0. \end{cases} \qquad (18)$$

DÉFINITION. — *La fonction* $\varphi_p(\xi)$, $\xi \in \mathbf{Q}_p$, *définie la formule* (18) *s'appel*
une métrique p-adique. La valeur du nombre $\varphi_p(\xi)$ *s'appelle la grandeur d*
nombre p-adique ξ *pour cette métrique.*

Comme pour la valuation, nous dirons fréquemment que la fonction
est une métrique et nous la désignerons par φ.

Il résulte facilement des propriétés (11) et (12) de l'exposant que
métrique possède les propriétés :

$$\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta) \qquad (1$$

$$\varphi(\xi + \eta) \leqslant \max(\varphi(\xi), \varphi(\eta)). \qquad (2$$

Cette dernière inégalité entraîne d'ailleurs

$$\varphi(\xi + \eta) \leqslant \varphi(\xi) + \varphi(\eta). \qquad (2$$

Les propriétés (19) et (21) et la propriété $\varphi(\xi) > 0$ pour $\xi \neq 0$ montre
que la notion de métrique introduite ci-dessus pour les nombres *p*-adiqu
est analogue à la notion de valeur absolue sur le corps des nombres ré
(ou de module sur le corps des nombres complexes).

A l'aide de la métrique φ_p, la définition de la convergence dans le corps
devient : la suite $\{ \xi_n \}$, $\xi_n \in \mathbf{Q}_p$, converge vers le nombre *p*-adique ξ si

$$\lim_{n\to\infty} \varphi_p(\xi_n - \xi) = 0.$$

On peut facilement formuler et démontrer pour le corps $\mathbf{Q}_p$ les théorèm
habituels de l'analyse sur les limites des suites. Montrons par exemple q
si $\{ \xi_n \} \to \xi$ et $\xi \neq 0$, alors $\left\{ \frac{1}{\xi_n} \right\} \to \frac{1}{\xi}$. Tout d'abord, à partir d'un certa
rang, i. e. $n \geqslant n_0$, nous aurons $\nu(\xi_n - \xi) > \nu(\xi)$, d'où, d'après (13),

$$\nu(\xi_n) = \min(\nu(\xi_n - \xi), \nu(\xi)) = \nu(\xi);$$

en particulier $\nu(\xi_n) \neq \infty$, i. e. $\xi_n \neq 0$ et par suite $\frac{1}{\xi_n}$ a un sens pour tout $n \geqslant$
De plus,

$$\nu\left(\frac{1}{\xi_n} - \frac{1}{\xi}\right) = \nu(\xi - \xi_n) - \nu(\xi_n) - \nu(\xi) = \nu(\xi_n - \xi) - 2\nu(\xi) \to \infty$$

pour $n \to \infty$, ce qui démontre notre affirmation.

THÉORÈME 5. — *Si le nombre entier p-adique* α *est défini par une suite* $\{ x_n$
de nombres entiers rationnels, alors cette suite converge vers α. *Tout nombr*
p-adique ξ *est limite d'une suite de nombres rationnels.*

DÉMONSTRATION. — De la congruence (14) résulte que $\nu_p(x_n - a) \geqslant n + 1$. Par suite $\nu(x_n - \alpha) \to \infty$ pour $n \to \infty$, donc $x_n \to \alpha$. Considérons maintenant une fraction *p*-adique $\xi = \frac{\alpha}{p^k}$. Puisque

$$\nu\left(\frac{x_n}{p^k} - \xi\right) = \nu\left(\frac{x_n - \alpha}{p^k}\right) = \nu(x_n - \alpha) - k \to \infty$$

pour $n \to \infty$, ξ est la limite de la suite de nombres rationnels $\left\{ \frac{x_n}{p^k} \right\}$.

De toute suite bornée de nombres réels on peut toujours, comme on le sait, extraire une sous-suite convergente. On a une propriété analogue pour les nombres *p*-adiques.

DÉFINITION. — *Une suite* $\{ \xi_n \}$ *de nombres p-adiques est dite bornée si toutes les valeurs* $\varphi_p(\xi_n)$ *sont bornées supérieurement ou, ce qui revient au même, si tous les nombres* $\nu_p(\xi_n)$ *sont bornés inférieurement.*

THÉORÈME 6. — *De toute suite bornée de nombres p-adiques (en particulier, de toute suite de nombres entiers p-adiques) on peut extraire une sous-suite convergente.*

DÉMONSTRATION. — Démontrons tout d'abord le théorème pour une suite $\{ \alpha_n \}$ de nombres entiers *p*-adiques. Puisque dans l'anneau $\mathbf{Z}_p$ le nombre de classes résiduelles modulo *p* est fini (corollaire du théorème 3), il existe dans la suite α_n une infinité de termes congrus modulo *p* à un même nombre entier rationnel x_0. Extrayant tous ces termes, nous obtenons une suite $\{ \alpha_n^{(1)} \}$ dont tous les termes satisfont à la congruence

$$\alpha_n^{(1)} \equiv x_0 \pmod{p}.$$

De la même manière, on extrait de la suite $\alpha_n^{(1)}$ une suite $\alpha_n^{(2)}$ telle que

$$\alpha_n^{(2)} \equiv x_1 \pmod{p^2},$$

où x_1 est un certain nombre entier rationnel. Continuant ce processus indéfiniment, nous obtenons pour tout *k* une suite $\{ \alpha_n^{(k)} \}$ qui est une sous-suite de la suite précédente $\{ \alpha_n^{(k-1)} \}$ et dont les termes vérifient la congruence

$$\alpha_n^{(k)} \equiv x_{k-1} \pmod{p^k}$$

pour un certain entier rationnel x_{k-1}. Puisque $x_k \equiv \alpha_n^{(k+1)} \pmod{p^{k+1}}$ et puisque la suite $\{ \alpha_n^{(k+1)} \}$ est extraite de la suite $\{ \alpha_n^{(k)} \}$, alors

$$x_k \equiv x_{k-1} \pmod{p^k}$$

pour tout $k \geqslant 1$. La suite $\{ x \}$ définit par suite un certain nombre en
p-adique α. Formons maintenant la « suite diagonale » $\{ \alpha_n^{(n)} \}$. Il est c
que c'est une sous-suite extraite de la suite α_n; montrons que $\{ \alpha_n^{(n)} \}$ -
En effet, d'après (14), nous avons : $\alpha \equiv x_{n-1} \pmod{p^u}$; d'autre part

$$\alpha_n^{(n)} \equiv x_{n-1} \pmod{p^n}$$

et par suite $\alpha_n^{(n)} \equiv \alpha \pmod{p^n}$, i. e. $v(\alpha_n^{(n)} - \alpha) \geqslant n$. Ainsi $v(\alpha_n^{(n)} - \alpha)$ -
pour $n \to \infty$, i. e. $\{ \alpha_n^{(n)} \} \to \alpha$.

Démontrons le théorème dans le cas général. Si pour une suite de n
bres p-adiques $\{ \xi_n \}$ on a $v(\xi_n) \geqslant -k$ (k étant un entier rationnel), a
pour $\alpha_n = \xi_n p^k$, on aura $v(\alpha_n) \geqslant 0$ et α_n est un nombre entier p-adi
D'après ce qui précède, on peut extraire de la suite $\{ \alpha_n \}$ de nombres en
p-adiques une suite convergente $\{ \alpha_{n_i} \}$. Mais alors, la suite $\{ \xi_{n_i} \} = \{ \alpha_{n_i}$
est une sous-suite convergente de $\{ \xi_n \}$. Ceci termine la démonstration

Les nombres p-adiques vérifient également le critère de Cauchy :
suite

$$\{ \xi_n \}, \qquad \xi_n \in \mathbf{Q}_p,$$

est convergente si et seulement si

$$\lim_{m,n \to \infty} v(\xi_m - \xi_n) = \infty.$$

La nécessité de cette condition est claire. Pour démontrer la suffisa
remarquons tout d'abord que (23) entraîne que la suite (22) est bor
En effet, la condition (23) entraîne l'existence d'un n_0 tel que $v(\xi_m - \xi_{n_0})$
pour tout $m \geqslant n_0$. Mais alors, d'après la propriété (12), pour tout $m \geqslant$
on a l'inégalité

$$v(\xi_m) = v\big((\xi_m - \xi_{n_0}) + \xi_{n_0}\big) \geqslant \min\big(0, v(\xi_{n_0})\big) ;$$

ainsi (22) est bornée. D'après le théorème 6, on peut extraire de (22)
sous-suite $\{ \xi_{n_i} \}$ convergente vers un certain nombre ξ. Soit M un nom
quelconque, arbitrairement grand; d'après (23) et la définition de la con
gence, il existe un entier naturel N tel que $v(\xi_m - \xi_n) \geqslant M$ pour $m, n \geqslant$
et $v(\xi_{n_i} - \xi) \geqslant M$ pour $n \geqslant N$. Par suite

$$v(\xi_m - \xi) \geqslant \min\big(v(\xi_m - \xi_{n_i}), \quad v(\xi_{n_i} - \xi)\big) \geqslant M$$

pour tout $m \geqslant N$. Par suite, $\lim_{m \to \infty} v(\xi_m - \xi) = \infty$, i. e. la suite (22)
convergente.

On peut donner une forme plus forte au critère de convergence dans

corps des nombres p-adiques. Si la suite (22) satisfait à la condition (23), il est clair que

$$\lim_{n \to \infty} v(\xi_{n+1} - \xi_n) = \infty. \tag{24}$$

Montrons maintenant que la condition (24) entraîne (23). En effet, si $v(\xi_{n+1} - \xi_n) \geqslant M$ pour tout $n \geqslant N$, d'après (12), l'égalité

$$\xi_m - \xi_n = \sum_{i=n}^{m-1} (\xi_{i+1} - \xi_i), \qquad m > n \geqslant N,$$

entraîne

$$v(\xi_m - \xi_n) \geqslant \min_{i=n, \ldots, m-1} v(\xi_{i+1} - \xi_i) \geqslant M,$$

i. e. $v(\xi_m - \xi_n) \to \infty$ pour $m, n \to \infty$. Ainsi, on a :

THÉORÈME 7. — *Pour qu'une suite $\{ \xi_n \}$ de nombres p-adiques soit convergente, il faut et il suffit que*

$$\lim_{n \to \infty} v(\xi_{n+1} - \xi_n) = \infty.$$

L'existence d'une notion de convergence dans le corps $\mathbf{Q}_p$ nous permet de parler de fonctions p-adiques continues d'une variable p-adique. Une fonction $F(\xi)$ sera dite continue pour $\xi = \xi_0$ si pour toute suite $\{ \xi_n \}$ convergente vers ξ_0, la suite des valeurs $\{ F(\xi_n) \}$ converge vers $F(\xi_0)$. La définition pour des fonctions de plusieurs variables est analogue. De même que dans l'analyse réelle, on démontre facilement les théorèmes usuels sur les opérations arithmétiques appliquées aux fonctions p-adiques continues. En particulier, il est facile de vérifier que tout polynôme d'un nombre quelconque de variables à coefficients p-adiques est une fonction p-adique continue. Nous utiliserons par la suite ce résultat simple (§ 5, 1)).

Pour terminer, donnons quelques résultats sur les séries p-adiques.

DÉFINITION. — *Si la suite des sommes partielles*

$$S_n = \sum_{i=0}^{n} \alpha^i$$

d'une série

$$\sum_{i=0}^{\infty} \alpha_i = \alpha_0 + \alpha_1 + \ldots + \alpha_n + \ldots, \tag{25}$$

à termes p-adiques, converge vers un nombre p-adique α, on dit que cette série converge et que sa somme est égale à α.

Le théorème 7 entraîne immédiatement le critère suivant de convergen des séries.

THÉORÈME 8. — *Pour que la série* (25) *soit convergente, il faut et il su que son terme général tende vers zéro, i. e. que* $v(\alpha_n) \to \infty$ *pour* $n \to \infty$.

Il est clair que l'on peut additionner, soustraire et multiplier par nombre p-adique constant des séries p-adiques.

THÉORÈME 9. — *La convergence et la somme d'une série ne changent si on permute l'ordre des termes.*

Nous laissons au lecteur la démonstration très simple de ce théorè

On montre dans les cours classiques d'analyse dans le domaine réel la propriété exprimée par le théorème 9 caractérise les séries absolum convergentes. Ainsi, toutes les séries p-adiques convergentes sont « abs ment convergentes ». Il en résulte facilement que dans le corps des nom p-adiques on peut multiplier les séries convergentes selon les règles usu de l'analyse classique.

Si le nombre entier p-adique α est défini par la suite canonique

$$\{a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots\} \qquad \text{(cf. § 1)},$$

alors, en accord avec le théorème 5, il est égal à la somme de la série con gente

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$$
$$0 \leqslant a_n \leqslant p - 1 \qquad (n = 0, 1. \ldots).$$

Puisque des suites canoniques différentes définissent des nombres en p-adiques différents, la représentation de α comme somme d'une séri type (26) est unique. Réciproquement, il est évident que toute séri type (26) converge vers un certain nombre entier p-adique.

La représentation des nombres entiers p-adiques par des séries du type rappelle l'écriture des nombres réels sous forme de fractions décim infinies.

Si on considère plus généralement la série

$$b_0 + b_1 p + \ldots + b_n p^n + \ldots$$

où les b_i sont des entiers rationnels quelconques, il est clair qu'elle conv vers un certain entier p-adique α (puisque $v(b_n p^n) \geqslant n$). Pour obten représentation du nombre α comme somme d'une série du type (26), il remplacer successivement chaque coefficient b_n par le reste de sa divi par p, en faisant rentrer le quotient partiel obtenu dans le terme suiva Cette remarque est très importante pour effectuer des opérations dans l' neau $\mathbf{Z}_p$, car en ajoutant, soustrayant ou multipliant des séries (26) suiv les règles usuelles de l'analyse on obtient des séries du type (27).

Il résulte facilement du théorème 1 qu'un entier p-adique représenté comme somme de la série (26) est une unité de $\mathbf{Z}_p$ si et seulement si $a \neq 0$. Réuni au théorème 4, cela nous donne le résultat suivant

THÉORÈME 10. — Tout nombre p-adique $\xi \neq 0$ s'écrit de manière unique sous la forme

$$\xi = p^m(a_0 + a_1 p + \ldots + a_n p^n + \ldots) \tag{28}$$

avec

$$m = v_p(\xi), \quad 1 \leqslant a_0 \leqslant p - 1, \quad 0 \leqslant a_n \leqslant p - 1 \quad (n = 1, 2, \ldots).$$

EXERCICES

1. Posant $x_n = 1 + p + \ldots + p^{n-1}$, montrer que dans le corps des nombres p-adiques, la suite $\{x_n\}$ converge vers $\frac{1}{1-p}$.

2. Soient $p \neq 2$ et c un résidu quadratique modulo p. Montrer qu'il existe deux nombres p-adiques distincts dont les carrés sont égaux à c.

3. Soit c un entier rationnel non divisible par p. Montrer que la suite $\{c^{p^n}\}$ est convergente dans le corps $\mathbf{Q}_p$. Soit γ la limite de cette suite; montrer que

$$\gamma \equiv c \pmod{p} \qquad \text{et} \qquad \gamma^{p-1} = 1.$$

4. Utilisant l'exercice précédent, montrer que le polynôme $t^{p-1} - 1$ se décompose en facteurs linéaires dans le corps $\mathbf{Q}_p$.

5. Dans le corps des nombres p-adiques, écrire le nombre -1 comme somme d'une série du type (26).

6. Dans le corps des nombres 5-adiques, écrire le nombre $-\frac{2}{3}$ comme somme d'une série du type (26).

7. Pour $p \neq 2$, montrer qu'il n'existe pas d'autre racine $p^{\text{ième}}$ de 1 que 1 dans le corps des nombres p-adiques.

8. Dans le corps $\mathbf{Q}_p$, montrer que, dans la représentation d'un nombre rationnel $\neq 0$ comme somme d'une série (28), les coefficients sont périodiques (à partir d'un certain rang). Réciproquement, toute série du type (28) telle que $a_{m+k} = a_k$ pour $k \geqslant k_0$ $(m > 0)$ a pour somme un nombre rationnel.

9. Pour les polynômes sur le corps des nombres p-adiques, démontrer le test d'irréductibilité d'Eisenstein : le polynôme $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ à coefficients entiers p-adiques est irréductible si, a_0 n'étant pas divisible par p et tous les autres coefficients étant divisibles par p, le terme constant a_n n'est pas divisible par p^2.

10. Montrer qu'il existe des extensions finies de degré quelconque du corps des nombres p-adiques.

11. Démontrer, que pour des nombres premiers p et q distincts, les corps $\mathbf{Q}_p$ et $\mathbf{Q}_q$ ne sont pas isomorphes. Démontrer également qu'aucun des corps $\mathbf{Q}_p$ n'est isomorphe au corps des nombres réels.

12. Démontrer que le seul automorphisme du corps des nombres p-adiques est l'identité (c'est également vrai pour le corps des nombres réels).

§ 4. — CARACTÉRISATION AXIOMATIQUE DU CORPS DES NOMBRES p-ADIQUES

Le corps des nombres p-adiques est un des instruments fondamentaux la théorie des nombres. Les paragraphes suivants de ce chapitre ser consacrés à quelques applications. Cependant, nous nous écarterons ici l'esprit fondamental de ce chapitre en situant les corps de nombres p-adiq dans la théorie générale des corps.

1) Les corps métriques

Nous avons déjà souligné l'analogie qui existe entre les nombres p-adiq et les nombres réels. Nous exposerons ici une axiomatique des corps m ques qui comprend ces deux exemples comme cas particuliers. Cette méth dans le cas particulier des nombres réels, coïncide avec la méthod construction des nombres réels à partir des suites de Cauchy, due à Ca

L'extension de la méthode de Cantor à d'autres corps repose su remarques suivantes. La notion essentielle ici est celle de convergence d suite de nombres rationnels. Cette notion s'appuie elle-même sur la no de valeur absolue (on dit qu'une suite de nombres rationnels $\{ r_n \}$ conv vers un nombre rationnel r si la valeur absolue $| r_n - r |$ tend vers zé Remarquons que l'on utilise ici seulement des propriétés simples de la va absolue. Par suite, si on suppose l'existence sur un corps k d'une fonct à valeurs réelles possédant les mêmes propriétés fondamentales que la va absolue, on peut définir dans k une notion de convergence et, en appliq la méthode de Cantor, construire un nouveau corps.

DÉFINITION. — *Soit k un corps. Une fonction φ définie sur les éléme du corps k et à valeurs réelles s'appelle une métrique si elle possède les priétés suivantes*

1^o $\quad \varphi(\alpha) > 0 \quad$ pour $\quad \alpha \neq 0, \quad \varphi(0) = 0;$

2^o $\quad \varphi(\alpha + \beta) \leqslant \varphi(\alpha) + \varphi(\beta);$

3^o $\quad \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta).$

Un corps k muni d'une métrique s'appelle un corps métrique (et est pa désigné par (k, φ)). De cette définition découlent facilement les propri suivantes :

$$\varphi(\pm 1) = 1 ;$$
$$\varphi(-\alpha) = \varphi(\alpha) ;$$

$$\varphi(\alpha - \beta) \leqslant \varphi(\alpha) + \varphi(\beta) ;$$
$$\varphi(\alpha \pm \beta) \geqslant | \varphi(\alpha) - \varphi(\beta) | ;$$
$$\varphi\left(\frac{\alpha}{\beta}\right) = \frac{\varphi(\alpha)}{\varphi(\beta)} \quad (\beta \neq 0).$$

Donnons des exemples de métriques :

1^o la valeur absolue dans le corps des nombres rationnels;

2^o la valeur absolue dans le corps des nombres réels;

3^o le module dans le corps des nombres complexes;

4^o la métrique p-adique φ_p, définie au § 3-4), sur le corps $\mathbf{Q}_p$ des nombres p-adiques;

5^o la fonction $\varphi(\alpha)$ définie sur un corps quelconque k par les conditions

$$\varphi(0) = 0, \qquad \gamma(\alpha) = 1 \qquad \text{si} \qquad \alpha \neq 0.$$

Une telle métrique est dite triviale.

Si on considère la restriction au corps $\mathbf{Q}$ des rationnels de la métrique φ_p définie sur $\mathbf{Q}_p$, on obtient une nouvelle métrique sur $\mathbf{Q}$. Cette métrique, que nous désignerons encore par φ_p, s'appelle métrique p-adique du corps $\mathbf{Q}$.

Sa valeur sur un nombre rationnel $x = p^{\nu_p(x)} \frac{a}{b}$ (a et b non divisible par p) est donnée par

$$\varphi_p(x) = \rho^{\nu_p(x)}, \tag{1}$$

où ρ est un nombre réel fixé satisfaisant à la condition $0 < \rho < 1$. Nous verrons ci-dessous que la construction de Cantor appliquée au corps des nombres rationnels muni de la métrique p-adique (au lieu de la valeur absolue) nous conduit au corps $\mathbf{Q}_p$ des nombres p-adiques.

Dans tout corps métrique (k, φ), on peut définir une notion de convergence : une suite $\{ \alpha_n \}$ d'éléments de k est dite convergente vers un élément $\alpha \in k$ si $\varphi(\alpha_n - \alpha) \to 0$ pour $n \to \infty$. On dit encore que α est la limite de $\{ \alpha_n \}$ et on écrit

$$\{ \alpha_n \} \to \alpha \qquad \text{ou} \qquad \alpha = \lim_{n \to \infty} \alpha_n.$$

DÉFINITION. — *Une suite $\{ \alpha_n \}$ d'éléments d'un corps métrique k est dite de Cauchy pour la métrique φ si $\varphi(\alpha_n - \alpha_m) \to 0$ pour $n, m \to \infty$.*

Il est clair que toute suite convergente est de Cauchy. En effet, si $\{ \alpha_n \} \to \alpha$, alors, d'après l'inégalité

$$\varphi(\alpha_n - \alpha_m) = \varphi(\alpha_n - \alpha + \alpha - \alpha_m) \leqslant \varphi(\alpha_n - \alpha) + \varphi(\alpha_m - \alpha),$$
$$\varphi(\alpha_n - \alpha_m) \to 0 \ (\text{car } \varphi(\alpha_n - \alpha) \to 0 \quad \text{et} \quad \varphi(\alpha_m - \alpha) \to 0).$$

La réciproque n'est pas vraie pour tous les corps métriques; elle est vr pour le corps réel et pour les corps p-adiques, d'après le critère de C chy (§ 3, 4)), mais n'est pas vraie pour le corps des rationnels muni d valeur absolue ou d'une métrique p-adique.

DÉFINITION. — *Un corps métrique est dit complet si toute suite de Cau est convergente.*

La méthode de Cantor consiste à plonger le corps non complet nombre rationnels (en prenant la valeur absolue comme métrique) dan corps complet des nombres rationnels. On montre qu'un tel plongemen possible pour tout corps métrique, en transcrivant presque littéralemen construction introduite par Cantor.

Fixons la terminologie suivante. On dira qu'un corps métrique (k est un sous-corps d'un corps métrique (k_1, φ_1) si $k \subset k_1$ et si $\varphi(x) =$ pour $x \in k$. De plus, un sous-ensemble d'un corps k sera dit partout d dans k si tout élément de k est limite d'une suite d'éléments de ce ensemble. On a alors le théorème 1.

THÉORÈME 1. — *Pour tout corps métrique k, il existe un corps mét complet $\bar{k}$ contenant k comme sous-corps partout dense.*

Pour énoncer le théorème suivant, nous avons encore besoin d définition.

DÉFINITION. — *Soient (k_1, φ_1) et (k_2, φ_2) deux corps métriques isomor entre eux. Un isomorphisme $\sigma : k_1 \to k_2$ est dit bicontinu ou topologiq pour toute suite $\{ \alpha_n \}$ d'éléments de k_1 convergente vers α pour la métriq la suite $\sigma(\alpha_n)$ converge vers $\sigma(\alpha)$ pour la métrique φ_2 et réciproquement.*

THÉORÈME 2. — *Le corps $\bar{k}$ introduit dans le théorème 1 est défini de ma unique, à un isomorphisme topologique près laissant fixe les élément corps k.*

DÉFINITION. — *Le corps $\bar{k}$, dont l'existence et l'unicité sont établie les théorèmes 1 et 2 s'appelle le complété du corps k.*

Il est clair que le corps des nombres réels est le complété du corps nombres rationnels $\mathbf{Q}$, muni de la valeur absolue comme métrique. S munit le corps des nombres rationnels de la métrique p-adique (1), alo complété de ce corps métrique est le corps $\mathbf{Q}_p$ des nombres p-adiques effet, d'après la deuxième partie du théorème 5 du § 3, $\mathbf{Q}$ est partout d dans $\mathbf{Q}_p$ et le critère de convergence de Cauchy (théorème 7, § 3) mo que $\mathbf{Q}_p$ est complet. Nous avons ainsi obtenu une nouvelle définition axio tique du corps des nombres p-adiques.

Le corps des nombres p-adiques est le complété du corps des nom rationnels muni de la métrique p-adique (1).

Passons à la démonstration rapide des théorèmes 1 et 2, en omettant les passages qui reproduisent textuellement les raisonnements classiques du cas réel.

DÉMONSTRATION DU THÉORÈME 1. — Nous dirons que deux suites de Cauchy $\{ x_n \}$ et $\{ y_n \}$ d'éléments du corps métrique (k, φ) sont équivalentes si la suite $\{ x_n - y_n \}$ tend vers zéro. Nous désignerons par $\bar{k}$ l'ensemble de toutes les classes d'équivalence de suites de Cauchy pour cette relation. Définissons de la manière suivante des opérations dans $\bar{k}$: si α et β sont deux classes et $\{ x_n \} \in \alpha$, $\{ y_n \} \in \beta$ alors nous appellerons somme (resp. produit) des classes α et β la classe de la suite $\{ x_n + y_n \}$ (resp. $\{ x_n y_n \}$). Il est facile de démontrer que $\{ x_n + y_n \}$ et $\{ x_n y_n \}$ sont effectivement des suites de Cauchy et que leurs classes ne dépendent pas du choix des suites $\{x_n\}$ et $\{ y_n \}$ dans les classes α et β.

Une vérification évidente montre que $\bar{k}$ est un anneau avec unité; la classe nulle et la classe unité sont les classes des suites $(0, 0, \ldots)$ et $(1, 1, 1, \ldots)$.

Démontrons que $\bar{k}$ est un corps. Si α est une classe différente de zéro et $\{ x_n \} \in \alpha$, alors il est facile de voir que tous les x_n sont différents de zéro à partir d'un certain rang (par exemple pour $n \geqslant n_0$). Considérons la suite $\{ y_n \}$ définie par

$$y_n = \begin{cases} 1 & \text{pour} \quad n < n_0 \\ \dfrac{1}{x_n} & \text{pour} \quad n \geqslant n_0. \end{cases}$$

On vérifie facilement que $\{ y_n \}$ est une suite de Cauchy et que sa classe est l'inverse de la classe α.

Définissons maintenant une métrique sur le corps $\bar{k}$. Remarquons pour cela que, comme il est facile de le vérifier, si $\{ x_n \}$ est une suite de Cauchy d'éléments du corps k, alors $\{ \varphi(x_n) \}$ est une suite de Cauchy de nombres réels, donc est convergente vers un certain nombre réel qui ne dépend que de la classe d'équivalence de $\{ x_n \}$. Nous poserons $\varphi(\alpha) = \lim_{n \to \infty} \varphi(x_n)$ si α est la classe contenant la suite $\{ x_n \}$. Il est facile de vérifier que la fonction φ ainsi définie est une métrique et par suite $(\bar{k}, \varphi)$ est un corps métrique.

Associons à tout élément a du corps k la classe contenant la suite $\{ a, a, \ldots \}$. Nous obtenons une application de k dans $\bar{k}$ qui réalise un isomorphisme conservant la métrique du corps métrique k sur un sous-corps du corps $\bar{k}$. Nous ne distinguerons pas un élément de k de son image dans $\bar{k}$, i. e. nous considérerons que $k \subset \bar{k}$. Il est clair que k est partout dense dans $\bar{k}$. En effet, si α est une classe contenant la suite de Cauchy $\{ x_n \}$, alors $\{ x_n \} \to \alpha$.

Il nous reste à démontrer que le corps $\bar{k}$ est complet. Soit α_n une suite de Cauchy d'éléments du corps $\bar{k}$. Puisque α_n est limite d'une suite d'éléments du corps k, il existe un élément $x_n \in k$ tel que $\varphi(\alpha_n - x_n) < \frac{1}{n}$.

La suite $\{ \alpha_n \}$ étant de Cauchy, la suite $\{ x_n \}$ d'éléments du corps k l'est aussi. Soit α la classe de la suite $\{ x_n \}$. On vérifie alors facilement que $\{ \alpha_n \} \to \alpha$, ce qui termine la démonstration.

DÉMONSTRATION DU THÉORÈME 2. — Soient $\bar{k}$ et $\bar{k}_1$ deux corps complets contenant k comme sous-corps partout dense. Montrons qu'il existe une correspondance biunivoque entre les corps $\bar{k}$ et $\bar{k}_1$, en laissant le soin au lecteur de vérifier que cette correspondance est un isomorphisme métrique.

Soit α un élément du corps $\bar{k}$. Par hypothèse, il existe une suite $\{ x_n \}$ d'éléments du corps k telle que $\{ x_n \} \to \alpha$. Puisque la suite $\{ x_n \}$ est convergente, c'est une suite de Cauchy et cette propriété est conservée si nous la considérons comme une suite d'éléments du corps $\bar{k}_1$. Ce corps étant complet, cette suite est convergente dans $\bar{k}_1$ vers une limite que nous désignerons par α_1. Il est facile de vérifier que si $\{ y_n \}$ est une autre suite d'éléments de k convergente vers α dans $\bar{k}$ alors la limite de $\{ y_n \}$ dans le corps $\bar{k}_1$ est encore le même élément α_1. Ainsi, l'élément α_1 du corps $\bar{k}_1$ est défini sans ambiguïté par l'élément α du corps $\bar{k}$. La correspondance $\alpha \to \alpha_1$ est ainsi un isomorphisme.

2) Les métriques du corps des nombres rationnels

On se propose ici de montrer que les seules métriques possibles sur le corps $\mathbf{Q}$ des nombres rationnels sont la métrique usuelle et les métriques p-adiques (pour p entier premier quelconque).

La définition de la métrique p-adique φ_p sur le corps $\mathbf{Q}$ fait intervenir le choix d'un nombre réel ρ auquel on impose seulement les conditions $0 < \rho < 1$ (cf. égalités (1) et (18) du § 3). Ainsi, il existe une infinité de métriques associées au même nombre premier p, mais toutes ces métriques définissent la même notion de convergence sur $\mathbf{Q}$ et par suite les complétés pour toutes ces métriques coïncident et sont tous égaux au corps $\mathbf{Q}_p$ des nombres p-adiques.

Montrons que, de même, pour tout choix de α réel tel que $0 < \alpha \leqslant 1$, la fonction

$$\varphi(x) = |x|^\alpha \tag{2}$$

est une métrique du corps R. En effet, il est clair que φ satisfait aux conditions 1° et 3° de définition d'une métrique. Soit $|x| \geqslant |y|$, $x \neq 0$; alors

$$|x+y|^\alpha = |x|^\alpha \left|1 + \frac{y}{x}\right|^\alpha \leqslant |x|^\alpha \left(1 + \left|\frac{y}{x}\right|^\alpha\right)$$
$$\leqslant |x|^\alpha \left(1 + \left|\frac{y}{x}\right|\right) \leqslant |x|^\alpha \left(1 + \left|\frac{y}{x}\right|^\alpha\right) = |x|^\alpha + |y|^\alpha,$$

i. e. la condition 2° est satisfaite.

D'après (2), la convergence dans $\mathbf{Q}$ définie par cette métrique coïncide avec la convergence pour la valeur absolue et par suite les complétés pour toutes ces métriques sont le corps des nombres réels.

THÉORÈME 3 (théorème d'Ostrowski). — *Les métriques du type* (2) *et les métriques p-adiques pour tout entier premier p sont les seules métriques non triviales du corps* $\mathbf{Q}$ *des nombres rationnels.*

DÉMONSTRATION. — Soit φ une métrique non triviale du corps des nombres rationnels. Deux cas sont possibles : ou bien il existe au moins un entier naturel $a > 1$ tel que $\varphi(a) > 1$ ou bien $\varphi(n) \leqslant 1$ pour tout entier naturel. Considérons tout d'abord le premier cas. Puisque

$$\varphi(n) = \varphi(1 + 1 + \ldots + 1) \leqslant \varphi(1) + \ldots + \varphi(1) = n \tag{3}$$

on peut poser

$$\varphi(a) = a^\alpha \tag{4}$$

où le nombre réel α est tel que $0 < \alpha \leqslant 1$.

Décomposons tout entier naturel N suivant les puissances de a :

$$N = x_0 + x_1 a + \ldots + x_{k-1} a^{k-1}$$

avec

$$0 \leqslant x_i \leqslant a - 1 \quad (0 \leqslant i \leqslant k-1), \quad x_{k-1} \geqslant 1.$$

Par suite, on a pour N l'inégalité

$$a^{k-1} \leqslant N < a^k.$$

D'après les propriétés de la métrique et les formules (3) et (4) nous obtenons

$$\varphi(N) \leqslant \varphi(x_0) + \varphi(x_1)\,\varphi(a) + \ldots + \varphi(x_{k-1})\,\varphi(a)^{k-1}$$
$$\leqslant (a-1)(1 + a^\alpha + \ldots + a^{(k-1)\alpha})$$
$$= (a-1)\frac{a^{k\alpha} - 1}{a^\alpha - 1} < (a-1)\frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1)}{a^\alpha - 1} a^\alpha \cdot a^{(k-1)\alpha}$$
$$\leqslant \frac{(a-1)a^\alpha}{a^\alpha - 1} N^\alpha = C N^\alpha,$$

i. e.

$$\varphi(N) < CN^{\alpha},$$

la constante C étant indépendante de N. Remplaçant N par N^m dans cette inégalité, nous obtenons, pour tout m,

$$\varphi(N)^m = \varphi(N^m) < CN^{m\alpha},$$

d'où

$$\varphi(N) < \sqrt[m]{C}\cdot N^{\alpha}.$$

Faisant tendre m vers l'infini, nous obtenons l'inégalité

$$\varphi(N) \leqslant N^{\alpha}. \tag{5}$$

Posons maintenant $N = a^k - b$, avec $0 < b \leqslant a^k - a^{k-1}$. D'après 2°, nous avons

$$\varphi(N) \geqslant \varphi(a^k) - \varphi(b) = a^{\alpha k} - \varphi(b).$$

D'après ce qu'on a vu,

$$\varphi(b) \leqslant b^{\alpha} \leqslant (a^k - a^{k-1})^{\alpha},$$

d'où

$$\varphi(N) \geqslant a^{\alpha k} - (a^k - a^{k-1})^{\alpha} = \left(1 - \left(1 - \frac{1}{a}\right)^{\alpha}\right)a^{\alpha k} = C_1 a^{\alpha k} > C_1 N^{\alpha},$$

où la constante C_1 est indépendante de N. Soit de nouveau m un entier naturel quelconque. En remplaçant N par N^m dans la dernière inégalité, nous obtenons

$$\varphi(N)^m = \varphi(N^m) > C_1 N^{\alpha m},$$

d'où

$$\varphi(N) > \sqrt[m]{C_1}\cdot N^{\alpha},$$

et par suite, pour $m \to \infty$, on a

$$\varphi(N) \geqslant N^{\alpha}. \tag{6}$$

La réunion de (5) et (6) nous montre que $\varphi(N) = N^{\alpha}$ pour tout entier naturel N. Soit maintenant $x = \pm \frac{N_1}{N_2}$ un nombre rationnel quelconque $\neq 0$ (N_1 et N_2 sont des entiers naturels). Alors

$$\varphi(x) = \varphi\left(\frac{N_1}{N_2}\right) = \frac{\varphi(N_1)}{\varphi(N_2)} = \frac{N_1^{\alpha}}{N_2^{\alpha}} = |x|^{\alpha}.$$

Ainsi, nous avons démontré que si $\varphi(\alpha) > 1$ pour au moins un entier naturel a, alors la métrique φ est de la forme (2).

Passons maintenant à l'étude du cas

$$\varphi(n) \leqslant 1 \tag{7}$$

pour tout entier naturel n.

Si nous avions $\varphi(p) = 1$ pour tout nombre premier p, alors, d'après la propriété 3°, nous aurions aussi $\varphi(n) = 1$ pour tout entier naturel; cela contredit la non-trivialité de la métrique φ. Ainsi, il existe un p premier tel que $\varphi(p) < 1$. Supposons que pour un autre nombre premier q, $q \neq p$, on ait $\varphi(q) < 1$ et choisissons des entiers k et l tels qu'on ait les inégalités

$$\varphi(p)^k < \frac{1}{2}, \qquad \varphi(q)^l < \frac{1}{2}.$$

Puisque p^k et q^l sont premiers entre eux, il existe des entiers rationnels u et v tels que $up^k + vq^l = 1$. D'après (7), nous avons $\varphi(u) \leqslant 1$ et $\varphi(v) \leqslant 1$, d'où

$$1 = \varphi(1) = \varphi(up^k + vq^l) \leqslant \varphi(u)\varphi(p)^k + \varphi(v)\varphi(q)^l < \frac{1}{2} + \frac{1}{2}.$$

La contradiction obtenue montre qu'il n'existe qu'un nombre premier p tel que

$$\varphi(p) = \rho < 1.$$

Puisque $\varphi(q) = 1$ pour tous les autres nombres premiers, il est clair que $\varphi(a) = 1$ pour tout entier a relativement premier avec p. Soit $x = p^m \frac{a}{b}$ un nombre rationnel non nul (a et b premiers à p). Alors

$$\varphi(x) = \varphi(p^m)\frac{\varphi(a)}{\varphi(b)} = \varphi(p)^m = \rho^m.$$

Ainsi, dans ce cas, la métrique φ coïncide avec la métrique p-adique (1).

Ceci termine la démonstration du théorème 3.

EXERCICES

1. Montrer que sur un corps fini, il existe une métrique et une seule (la métrique triviale).

2. Deux métriques φ et ψ sur un corps k sont dites *équivalentes* si elles définissent la même notion de convergence sur k, i. e. si les conditions $\varphi(x_n - x) \to 0$ et $\psi(x_n - x) \to 0$ sont équivalentes. Démontrer que φ et ψ sont équivalentes si et seulement si les conditions $\varphi(x) < 1$ et $\psi(x) < 1$ ($x \in k$) sont équivalentes.

3. Démontrer que si φ et ψ sont des métriques équivalentes d'un corps k, alors il existe un nombre réel δ tel que $\varphi(x) = (\psi(x))^{\delta}$ pour tout $x \in k$.

4. Une métrique φ sur un corps k est dite *non archimédienne* si elle vérifie la condition suivante, plus forte que la condition 2° de 1) :

2° $$\varphi(\alpha + \beta) \leqslant \max(\varphi(\alpha), \varphi(\beta))$$

(si cette condition n'est pas réalisée, la métrique φ est dite archimédienne). Montrer qu'une métrique φ est non archimédienne si et seulement si $\varphi(x) \leqslant 1$ pour tout entier naturel n (plus précisément, pour tout multiple naturel de l'élément unité du corps k).

5. Montrer que toute métrique d'un corps de caractéristique $p \neq 0$ est non archimédienne.

6. Soit k_0 un corps et $k = k_0(t)$ le corps des fractions rationnelles sur k. Tout élément $u \in k$, $u \neq 0$, peut s'écrire sous la forme

$$u = t^m \frac{f(t)}{g(t)} \quad (f(0) \neq 0,\ g(0) \neq 0)$$

où f et g sont des polynômes. Montrer que la fonction

$$\varphi(u) = \rho^m \ (0 < \rho < 1), \qquad \varphi(0) = 0 \tag{8}$$

est une métrique sur le corps k.

7. Démontrer que le complété du corps $k = k_0(t)$ pour la métrique (8) est isomorphe au corps des séries formelles généralisées $k_0\{t\}$ formé par toutes les séries formelles du type

$$\sum_{n=m}^{\infty} a_n t^n \qquad (a_n \in k_0,\ m \in \mathbf{Z})$$

avec les opérations habituelles sur les séries.

§ 5. — CONGRUENCES ET NOMBRES ENTIERS p-ADIQUES

1) Congruences et équations dans l'anneau $\mathbf{Z}_p$

Au début du § 3, nous avons étudié la résolution de la congruence $x^2 \equiv$ (mod 7^n) pour $n = 1, 2, \ldots$ et cela nous a conduit à la notion de nombre entier p-adique. Cela suggère un important lien entre les nombres p-adiques et les congruences.

THÉORÈME 1. — *Soit* $F(x_1, \ldots, x_n)$ *un polynôme à coefficients entiers rationnels. Les congruences*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{1}$$

sont résolubles pour tout entier $k \geqslant 1$ *si et seulement si l'équation*

$$F(x_1, \ldots, x_n) = 0 \tag{2}$$

est résoluble dans l'anneau des nombres entiers p-adiques.

DÉMONSTRATION. — Supposons que l'équation (2) ait une solution $\alpha_1, \ldots, \alpha_n$ dans les nombres entiers p-adiques. Pour tout k, il existe alors des nombres entiers rationnels $x_1^{(k)}, \ldots, x_n^{(k)}$, tels que

$$\alpha_1 \equiv x_1^{(k)} \pmod{p^k}, \ \ldots, \ \alpha_n \equiv x_n^{(k)} \pmod{p^k}. \tag{3}$$

Il en résulte que

$$F\left(x_1^{(k)}, \ldots, x_n^{(k)}\right) \equiv F(\alpha_1, \ldots, \alpha_n) \equiv 0 \pmod{p^k},$$

i. e. $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ est une solution de la congruence (1).

Supposons maintenant que la congruence (1) a une solution $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ pour tout k. Extrayons de la suite des nombres entiers rationnels $\left\{x_1^{(k)}\right\}$ une sous-suite p-adiquement convergente (théorème 6, § 3). Extrayons de nouveau une sous-suite convergente de la suite $\left\{x_2^{(k_i)}\right\}$; en répétant n fois ce processus, nous obtenons une sous-suite $\{l_1, l_2, \ldots\}$ de la suite des entiers telle que chacune des suites $\left\{x_i^{(l_1)}, x_i^{(l_2)}, \ldots\right\}$, soit p-adiquement convergente. Posons

$$\lim_{n \to \infty} x_i^{(l_m)} = \alpha_i.$$

Montrons que $(\alpha_1, \ldots, \alpha_n)$ est une solution de la congruence (2). Puisque le polynôme $F(x_1, \ldots, x_n)$ est une fonction continue, alors

$$F(\alpha_1, \ldots, \alpha_n) = \lim_{m \to \infty} F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right).$$

D'autre part, d'après la construction de la suite,

$$F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right) \equiv 0 \pmod{p^{l_m}},$$

d'où

$$\lim_{m \to \infty} F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right) = 0.$$

Ainsi $F(\alpha_1, \ldots, \alpha_n) = 0$ et le théorème 1 est démontré.

Considérons maintenant le cas où $F(x_1, \ldots, x_n)$ est une forme à coefficients entiers rationnels et supposons que l'équation $F(x_1, \ldots, x_n) = 0$ a une solution non nulle $(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ dans les nombres entiers p-adiques. Posons $m = \min(\nu_p(\bar{\alpha}_i), \ldots, \nu_p(\bar{\alpha}_n))$. Alors les $\bar{\alpha}_i$ s'écrivent sous la forme

$$\bar{\alpha}_i = p^m \alpha_i \qquad (i = 1, \ldots, n)$$

tous les α_i étant entiers et l'un au moins d'entre eux n'étant pas divisible par p. Il est évident que $(\alpha_1, \ldots, \alpha_n)$ est encore une solution de l'équation $F(x_1, \ldots, x_n) = 0$. Les nombres $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ satisfaisant aux condi-

tions (3) donnent, comme nous l'avons vu, une solution de la congruence (1) et l'un d'entre eux n'est pas divisible par p.

Supposons que, réciproquement, la congruence (1) pour F homogène a pour tout k une solution $(x_1^{(k)}, \ldots, x_n^{(k)})$ telle qu'au moins un des nombres $x_i^{(k)}$ ne soit pas divisible par p. Il est clair qu'il existe un indice $i = i$ tel que le nombre $x_{i_0}^{(m)}$ ne soit pas divisible par p pour une infinité de valeurs de m. Par suite, nous pouvons choisir la suite $\{l_1, l_2, \ldots\}$ de telle sorte qu'aucun des $x_{i_0}^{(l_m)}$ ne soit divisible par p. Mais alors, l'égalité $\alpha_{i_0} = \lim_{m\to\infty} x_{i_0}^{(l_m)}$ entraîne que α_{i_0} n'est pas divisible par p d'où $\alpha_{i_0} \neq 0$. On a donc démontré le théorème suivant.

THÉORÈME 2. — *Soit* $F(x_1, \ldots, x_n)$ *une forme à coefficients entiers rationnels. Pour que l'équation* $F(x_1, \ldots, x_n) = 0$ *ait une solution non triviale dans l'anneau* $\mathbf{Z}_p$, *il faut et il suffit que, pour tout entier* m, *la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$$

ait une solution dont une au moins des composantes n'est pas divisible par p.

Il est évident qu'on peut aussi considérer dans les théorèmes 1 et 2 des polynômes à coefficients entiers p-adiques.

2) Sur la résolubilité de certaines congruences

Le théorème 1, démontré dans le point précédent, ramène la question de la résolubilité de l'équation (2) dans les nombres entiers p-adiques à la résolubilité de la suite infinie des congruences (1). La question de savoir s'il suffit d'examiner seulement un nombre fini de ces congruences est, dans le cas général, assez compliquée. Nous nous bornerons ici à examiner un cas particulier.

THÉORÈME 3. — *Soient* $F(x_1, \ldots, x_n)$ *un polynôme à coefficients entiers p-adiques et* $(\gamma_1, \ldots, \gamma_n)$ *des nombres entiers p-adiques tels que l'on ait, pour un certain* i $(1 \leqslant i \leqslant n)$:

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{2\delta+1}},$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{\delta}}$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$$

(δ *étant un entier naturel*). *Alors, il existe des entiers p-adiques* $\theta_1, \ldots, \theta_n$ tels que

$$F(\theta_1, \ldots, \theta_n) = 0$$

et

$$\theta_1 \equiv \gamma_1 \pmod{p^{\delta+1}}, \ldots, \theta_n \equiv \gamma_n \pmod{p^{\delta+1}}.$$

DÉMONSTRATION. — Considérons le polynôme

$$f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n).$$

Pour démontrer le théorème, il suffit d'établir l'existence d'un nombre entier p-adique α tel que $f(\alpha) = 0$ et $\alpha \equiv \gamma_i \pmod{p^{\delta+1}}$ (si on trouve un tel α, alors on peut poser $\theta_j = \gamma_j$ pour $j \neq i$ et $\theta_i = \alpha$). Posant $\gamma_i = \gamma$, construisons par récurrence une suite

$$\alpha_0, \alpha_1, \ldots, \alpha_m, \ldots \tag{3'}$$

de nombres p-adiques congrus à δ modulo $p^{\delta+1}$ et tels que

$$f(\alpha_m) \equiv 0 \pmod{p^{2\delta+1+m}} \tag{4}$$

pour tout $m \geqslant 0$. Pour $m = 0$, on peut prendre $\alpha_0 = \gamma$; supposons que pour un certain $m \geqslant 1$ on ait construit des nombres $\alpha_0, \ldots, \alpha_{m-1}$ satisfaisant aux conditions ci-dessus et tels, en particulier, que $\alpha_{m-1} \equiv \gamma \pmod{p^{\delta+1}}$ et $f(\alpha_{m-1}) \equiv 0 \pmod{p^{2\delta+m}}$. Ordonnons le polynôme $f(x)$ suivant les puissances de $x - \alpha_{m-1}$:

$$f(x) = \beta_0 + \beta_1(x - \alpha_{m-1}) + \beta_2(x - \alpha_{m-1})^2 + \ldots \qquad (\beta_i \in \mathbf{Z}_p).$$

Par hypothèse de récurrence, $\beta_0 = f(\alpha_{m-1}) = p^{2\delta+m}A$, A étant un entier p-adique. De plus, puisque $\alpha_{m-1} \equiv \gamma \pmod{p^{\delta+1}}$, alors $\beta_1 = f'(\alpha_{m-1}) = p^{\delta}B$ où le nombre $B \in \mathbf{Z}_p$ n'est pas divisible par p. Posant $x = \alpha_{m-1} + \xi p^{m+\delta}$, on a

$$f(\alpha_{m-1} + \xi p^{m+\delta}) = p^{2\delta+m}(A + B\xi) + \beta_2 p^{2\delta+2m}\xi^2 + \ldots$$

Posons maintenant $\xi = \xi_0 \in \mathbf{Z}_p$ tel que $A + B\xi_0 \equiv 0 \pmod{p}$ (puisque $B \not\equiv 0 \pmod{p}$, la congruence $A + B\xi \equiv 0 \pmod{p}$ est résoluble). Remarquant que $k\delta + km \geqslant 2\delta + 1 + m$ pour $k \geqslant 2$, nous obtenons

$$f(\alpha_{m-1} + \xi_0 p^{m+\delta}) \equiv 0 \pmod{p^{2\delta+1+m}}.$$

Nous pourrons alors poser $\alpha_m = \alpha_{m-1} + \xi_0 p^{m+\delta}$. Puisque $m + \delta \geqslant \delta + 1$, alors $\alpha_m \equiv \gamma \pmod{p^{\delta+1}}$. Par construction, $\nu_p(\alpha_m - \alpha_{m-1}) \geqslant m + \delta$ et par suite la suite (3') trouvée est convergente; nous désignerons sa limite par α. Il est évident que $\alpha \equiv \gamma \pmod{p^{\delta+1}}$. Il résulte alors de (4) que $\lim_{m\to\infty} f(\alpha_m) = 0$; d'autre part, d'après la continuité du polynôme, $\lim_{m\to\infty} f(\alpha_m) = f(\alpha)$, d'où

$$f(\alpha) = 0.$$

COROLLAIRE. — *Soient* $F(x_1, \ldots, x_n)$ *un polynôme à coefficients entier p-adiques et* $\gamma_1, \ldots, \gamma_n$ *des entiers p-adiques tels que, pour un certain* $i (1 \leqslant i \leqslant$ *on ait*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p}$$

$$F'_{x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p};$$

alors il existe des entiers p-adiques $\theta_1, \ldots, \theta_n$ *tels que*

$$F(\theta_1, \ldots, \theta_n) = 0$$

et

$$\theta_1 \equiv \gamma_1 \pmod{p}, \ldots, \theta_n \equiv \gamma_n \pmod{p}.$$

Ainsi, toute solution $c_1, \ldots, c_n$ de la congruence $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ peut être prolongée en une solution de l'équation $F(x_1, \ldots, x_n) = 0$ dan l'anneau $\mathbf{Z}_p$, sauf, peut-être, celles pour lesquelles on a simultanément

$$\left.\begin{aligned} F'_{x_1}(c_1, \ldots, c_n) &\equiv 0 \pmod{p} \\ &\vdots \\ F'_{x_n}(c_1, \ldots, c_n) &\equiv 0 \pmod{p} \end{aligned}\right\}$$

Ce dernier résultat a une importante application à la question dont nou avons parlé au début du § 2. Nous avons vu que la résolubilité de l congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{m}$$

pour tout entier m est liée à la satisfaction d'une infinité de condition Dans le cas d'un module premier, les théorèmes A et B, formulés au débu du § 2-1) nous permettent de ramener ces conditions à un nombre fini d vérifications. Nous pouvons énoncer un résultat pour les entiers quelconques comme nous l'avons déjà remarqué, il suffit de considérer des modules qu sont des puissances de nombres premiers et pour des modules de la forme p^k $(k = 1, 2, \ldots)$, la résolubilité des congruences (1) est équivalente, d'après le théorème 1 à la résolubilité de l'équation $F = 0$ dans l'anneau $\mathbf{Z}_p$ des nombres entiers p-adiques.

En s'appuyant sur les théorèmes A et B formulés (mais non démontrés) dans le § 2-1) et sur le théorème 3 de ce paragraphe, nous pouvons établir le résultat suivant.

THÉORÈME C. — *Si* $F(x_1, \ldots, x_p)$ *est un polynôme absolument irréductible à coefficients entiers rationnels, alors l'équation* $F(x_1, \ldots, x_n) = 0$ *est résoluble dans l'anneau* $\mathbf{Z}_p$ *des nombres entiers p-adiques pour tout nombre premier p plus grand qu'un certain nombre ne dépendant que du polynôme* F.

Par suite, pour tous les nombres premiers p, sauf un nombre fini, la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{5}$$

est résoluble pour tous les entiers k.

Le théorème C réduit ainsi la question de la résolubilité de toutes les congruences (5) à la question de la résolubilité de l'équation $F = 0$ dans l'anneau $\mathbf{Z}_p$ pour seulement un nombre fini d'entiers p. Nous n'étudierons pas ici la résolubilité de l'équation $F = 0$ dans l'anneau $\mathbf{Z}_p$ (cela sera fait, dans le cas d'un polynôme de deuxième degré au § 6).

Donnons une idée de la démonstration du théorème 6. En utilisant la valeur du nombre de solutions de la congruence (2), § 2, exprimée par le théorème B, montrons que le nombre de solutions de cette congruence pour p assez grand est supérieur au nombre de solutions du système de congruences

$$\left.\begin{aligned} F(x_1, \ldots, x_n) &\equiv 0 \pmod{p} \\ F'_{x_n}(x_1, \ldots, x_n) &\equiv 0 \pmod{p} \end{aligned}\right\} \tag{6}$$

Il nous faut pour cela obtenir une nouvelle estimation du nombre de solutions d'une congruence.

LEMME. — *Si aucun des coefficients du polynôme* $F(x_1, \ldots, x_n)$ *n'est divisible par p, alors le nombre* $N(p)$ *de solutions de la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{7}$$

satisfait à l'inégalité

$$N(p) \leqslant Lp^{n-1}, \tag{8}$$

dans lequel la constante L *est égale au degré total du polynôme* F.

Démontrons le lemme par récurrence sur n. Pour $n = 1$, il résulte du fait que le nombre de racines, dans le corps $\mathbf{F}_p$, d'un polynôme non nul ne peut pas dépasser son degré.

Si $n > 1$, nous considérerons $F(x_1, \ldots, x_n)$ comme un polynôme de $x_1, \ldots, x_{n-1}$ dont les coefficients sont des polynômes de x_n. Désignons par $f(x_n)$ le plus grand commun diviseur de ces coefficients modulo p. Alors

$$F(x_1, \ldots, x_n) \equiv f(x_n) F_1(x_1, \ldots, x_n) \pmod{p}$$

et par suite le polynôme $F_1(x_1, \ldots, x_{n-1}, a)$ n'est congru identiquement à zéro modulo p pour aucune valeur de a. Soient l et L_1 les degrés des polynômes f et F_1. Il est clair que f et F_1 peuvent être choisis tels que $l + L_1 \leqslant L$. Évaluons maintenant le nombre de solutions $(c_1, \ldots, c_n)$ de la congruence (7)

et portons notre attention sur la valeur de x_n dans cette solution. Considéron tout d'abord les solutions telles que

$$f(c_n) \equiv 0 \pmod{p}. \qquad (9$$

Si la congruence (9) est satisfaite, la congruence (7) est automatiquemen satisfaite pour tout $c_1, \ldots, c_{n-1}$. Puisque le nombre de valeurs de c_n modulo satisfaisant à la condition (9) ne dépasse pas L, le nombre de valeurs de congruence (7) pour lesquelles on a (9) ne dépasse pas Lp^{n-1}. Considéron maintenant les solutions $(c_1, \ldots, c_n)$ telles que $f(c_n) \not\equiv 0 \pmod{p}$. Il est cla que toutes ces solutions satisfont à la congruence $F_1(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ Puisque $F_1(x_1, \ldots, x_{n-1}, c_n)$ n'est pas identiquement congru à 0 modulo alors, par hypothèse de récurrence, le nombre $N(p, c_n)$ de solutions de l congruence $F(x_1, \ldots, x_{n-1}, c_n) \equiv 0 \pmod{p}$ satisfait à l'inégalité

$$N(p, c_n) \leqslant L_1 p^{n-2}.$$

Puisque c_n peut prendre au plus p valeurs, le nombre des solutions consi dérées ne dépasse pas $L_1 p^{n-1}$. Ainsi, le nombre de toutes les solutions de l congruence (7) ne dépasse pas $lp^{n-1} + L_1 p^{n-1} \leqslant Lp^{n-1}$, c. q. f. d.

DÉMONSTRATION DU THÉORÈME C. — Nous pouvons supposer qu le polynôme F dépend effectivement de la variable x_n. Considérons comme un polynôme de x_n dont les coefficients sont des polynômes d $x_1, \ldots, x_{n-1}$. L'irréductibilité absolue de F entraîne alors que le discr minant $D_{x_n}(x_1, \ldots, x_{n-1})$ du polynôme F considéré comme polynôme de x n'est pas un polynôme de $x_1, \ldots, x_{n-1}$ identiquement nul, car sinon F sera divisible par le carré d'un certain polynôme. Considérons les nombre premiers p qui ne divisent pas tous les coefficients de $D_{x_n}(x_1, \ldots, x_{n-}$ et évaluons dans ce cas, le nombre $N_1(p)$ de solutions de système d congruences (6). Si $(c_1, \ldots, c_n)$ est une solution du système (6), alors est une racine commune modulo p des polynômes

$$F(c_1, \ldots, c_{n-1}, x_n) \quad \text{et} \quad F'_{x_n}(c_1, \ldots, c_{n-1}, x_n),$$

d'où

$$D_{x_n}(c_1, \ldots, c_{n-1}) \equiv 0 \pmod{p}.$$

D'après le lemme, le nombre de systèmes $(c_1, \ldots, c_{n-1})$ qui satisfont à cette congruence ne dépasse pas $K_1 p^{n-2}$, K_1 étant une constante dépendant seulement du polynôme F. Pour $c_1, \ldots, c_{n-1}$ donnés la valeur c_n est définie par la congruence

$$F(c_1, \ldots, c_{n-1}, x_n) \equiv 0 \pmod{p}$$

et par suite le nombre de ces valeurs ne dépasse pas le degré m du polynôme F par rapport à la variable x_n. Ainsi le nombre $N_1(p)$ de solutions du système (6) ne dépasse pas Kp^{n-2}, avec $K = mK_1$. Démontrons maintenant que le nombre $N(p)$ de solutions de la congruence (7), pour p assez grand, est supérieur au nombre $N_1(p)$ de solutions du système (6). En effet, il résulte du théorème B que

$$N(p) > p^{n-1} - Cp^{n-1-\frac{1}{2}},$$

et nous venons de démontrer que $N_1(p) < Kp^{n-2}$. Par suite,

$$N(p) - N_1(p) > p^{n-1} - Cp^{n-1-\frac{1}{2}} - Kp^{n-2} = p^{n-2}(p - Cp^{\frac{1}{2}} - K),$$

et cela entraîne $N(p) > N_1(p)$ pour p assez grand. Ainsi, pour p assez grand, la congruence $F \equiv 0 \pmod{p}$ a une solution $\gamma_1, \ldots, \gamma_n$ telle que

$$\frac{\partial F}{\partial x_n}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p}.$$

D'après le corollaire du théorème 3, il en résulte que l'équation $F = 0$ est résoluble dans l'anneau $\mathbf{Z}_p$ pour tout p assez grand.

EXERCICES

1. Démontrer que si m et p sont premiers entre eux, toute unité p-adique ε telle que $\varepsilon \equiv 1 \pmod{p}$ est une puissance $m^{\text{ième}}$ dans $\mathbf{Q}_p$.

2. Soit $m = p^\delta m_0$, $(m_0, p) = 1$ et soit ε une unité p-adique telle que $\varepsilon \equiv 1 \pmod{p^{\delta+1}}$. Montrer que ε est une puissance $m^{\text{ième}}$ dans $\mathbf{Q}_p$.

3. Démontrer que, pour $p \neq 2$, la résolubilité de la congruence $\alpha x^p \equiv \beta \pmod{p^2}$ par des entiers p-adiques α et β non divisibles par p entraîne la résolubilité de l'équation $\alpha x^p = \beta$ dans le corps $\mathbf{Q}_p$.

4. Soit la forme $G = \varepsilon_1 x_1^p + \ldots + \varepsilon_n x_n^p$, dont les coefficients sont des unités p-adiques $p \neq 2$). Montrer que si la congruence $G \equiv 0 \pmod{p^2}$ a une solution telle que la valeur de l'une au moins des inconnues ne soit pas divisible par p, alors l'équation $G = 0$ a une solution non nulle dans le corps $\mathbf{Q}_p$.

5. Considérons une forme $G = \alpha_1 x_1^p + \ldots + \alpha_n x_n^p$ dont les coefficients sont des nombres entiers p-adiques non divisibles par p^p.

Démontrer que l'équation $G = 0$ a une solution non nulle dans le corps $\mathbf{Q}_p$ si la congruence $G \equiv 0 \pmod{p^{p+2}}$ a une solution telle que toutes les valeurs des inconnues ne soient pas divisibles par p.

(Dans le cas $p \neq 2$, il suffit que la congruence $G \equiv 0 \pmod{p^{p+1}}$ soit résoluble).

6. Considérons une forme quadratique $F = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ dont les coefficients sont des entiers p-adiques ($p \neq 2$) non divisibles par p^2. Démontrer que si la congruence $F \equiv 0 \pmod{p^2}$ a une solution telle que toutes les valeurs des inconnues ne soient pas divisibles par p, alors l'équation $F = 0$ a une solution, non nulle dans $\mathbf{Q}_p$.

7. Soit la forme $F = \alpha_1 x_1^m + \ldots + \alpha_n x_n^m$, où les α_i sont des entiers p-adiqu non nuls; posons $r = v_p(m)$, $s = \max(v_p(\alpha_1), \ldots, v_p(\alpha_n))$ et $N = 2(r+s)+$ Montrer que l'équation $F = 0$ a une solution non nulle dans le corps $\mathbf{Q}_p$ si seulement si la congruence $F \equiv 0 \pmod{p^N}$ a une solution telle que la valeur l'une au moins des inconnues ne soit pas divisible par p.

8. Montrer que la forme $3x^3 + 4y^3 + 5z^3$ représente zéro dans le corps pour tout p (cf. exercice 13 du § 2).

9. Soit $F(x_1, \ldots, x_n)$ un polynôme à coefficients entiers p-adiques et dés gnons par c_m le nombre de solutions de la congruence $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$

La série $\varphi(t) = \sum_{m=0}^{\infty} c_m t^m$ est appelée la série de Poincaré du polynôme F et conjecture que sa somme est une fonction rationnelle de t. Trouver la série Poincaré du polynôme $F = \varepsilon_1 x_1^2 + \ldots + \varepsilon_n x_n^2$ où les ε_i sont des unités p-adiqu et vérifier que la fonction $\varphi(t)$ est rationnelle.

10. Trouver la série de Poincaré d'un polynôme $F(x_1, \ldots, x_n)$ à coefficien entiers qui possède la propriété suivante : pour toute solution de la congruen $F \equiv 0 \pmod{p}$, il existe un certain indice i ($i = 1, 2, \ldots, n$) tel que $\frac{\partial F}{\partial x_i} \not\equiv 0 \pmod{p}$

11. Déterminer la série de Poincaré du polynôme $F(x, y) = x^2 - y^3$.

§ 6. — FORMES QUADRATIQUES A COEFFICIENTS p-ADIQUES

Dans ce paragraphe et le suivant, nous appliquerons la théorie des no bres p-adiques à la représentation des nombres rationnels et p-adiques des formes quadratiques. Nous aurons besoin des résultats algébriques s les formes quadratiques exposés dans le § 1 de l'appendice.

1) Les carrés dans le corps des nombres p-adiques

Pour étudier les formes quadratiques sur un corps, il est important savoir quels éléments du corps sont des carrés. C'est pourquoi nous comm cerons par l'étude des carrés dans le corps $\mathbf{Q}_p$ des nombres p-adiques.

Nous savons (théorème 4, § 3) que tout nombre p-adique $\alpha \neq 0$ s'éc de manière unique $\alpha = p^m \varepsilon$, où ε est une unité p-adique (i. e. une un dans l'anneau $\mathbf{Z}_p$ des entiers p-adiques). Si α est le carré d'un nomb p-adique $\gamma = p^k \varepsilon_0$, alors $m = 2k$ et $\varepsilon = \varepsilon_0^2$. Par suite, il est nécessaire connaître quelles sont les unités de $\mathbf{Z}_p$ qui sont des carrés.

THÉORÈME 1. — *Soit $p \neq 2$. Pour qu'une unité p-adique*

$$\varepsilon = c_0 + c_1 p + c_2 p^2 + \ldots \qquad (0 \leqslant c_i < p,\ c_0 \neq 0) \qquad (1$$

soit un carré, il faut et il suffit que le nombre c_0 soit un résidu quadratiqu modulo p.

DÉMONSTRATION. — Si $\varepsilon = \eta^2$ et $\eta \equiv b \pmod{p}$ (b entier rationnel), alors $c_0 \equiv b^2 \pmod{p}$. Réciproquement, si $c_0 \equiv b^2 \pmod{p}$, alors, considérant le polynôme $F(x) = x^2 - \varepsilon$, nous obtenons : $F(b) \equiv 0 \pmod{p}$ et

$$F'(b) = 2b \not\equiv 0 \pmod{p}.$$

D'après le corollaire du théorème 3 du § 5, il existe $\eta \in \mathbf{Z}_p$ tel que $F(\eta) = 0$ et $\eta \equiv b \pmod{p}$. Ainsi $\varepsilon = \eta^2$ et le théorème est démontré.

COROLLAIRE 1. — *Pour $p \neq 2$, toute unité p-adique congrue à 1 mod p est un carré dans $\mathbf{Q}_p$.*

COROLLAIRE 2. — *Pour $p \neq 2$, l'indice $(\mathbf{Q}_p^* : \mathbf{Q}_p^{*2})$ du sous-groupe $\mathbf{Q}_p^{*2}$ des carrés dans le groupe multiplicatif du corps des nombres p-adiques est égal à 4.*

En effet, si une unité ε n'est pas un carré, alors le rapport de deux des nombres 1, ε, p, $p\varepsilon$ n'est jamais un carré dans le corps $\mathbf{Q}_p$. De plus, tout nombre p-adique différent de 0 est représentable comme produit d'un des nombres 1, ε, p, $p\varepsilon$ par un carré.

Pour $p \neq 2$, nous poserons, pour toute unité (1),

$$\left(\frac{\varepsilon}{p}\right) = \begin{cases} +1 & \text{si } \varepsilon \text{ est un carré dans } R_p \\ -1 & \text{sinon.} \end{cases}$$

D'après le théorème 1, nous avons

$$\left(\frac{\varepsilon}{p}\right) = \left(\frac{c_0}{p}\right),$$

où $\left(\frac{c_0}{p}\right)$ est le symbole de Legendre. Si ε est un entier rationnel premier avec p, alors il est clair que le symbole $\left(\frac{\varepsilon}{p}\right)$ introduit ici coïncide avec le symbole de Legendre. Il est facile d'ailleurs de voir que, pour des unités p-adiques ε et η, on a

$$\left(\frac{\varepsilon\eta}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{\eta}{p}\right).$$

Revenons sur le cas $p = 2$.

THÉORÈME 2. — *Pour qu'une unité 2-adique ε soit un carré (dans le corps $\mathbf{Q}_2$), il faut et il suffit que $\varepsilon \equiv 1 \pmod{8}$.*

DÉMONSTRATION. — La nécessité résulte du fait que le carré d'un nombre impair est toujours congru à 1 modulo 8. Pour démontrer la suffisance de cette condition, considérons le polynôme $F(x) = x^2 - \varepsilon$ et appliquons-lui le

corollaire du théorème 3, § 5 pour $\delta = 1$ et $\gamma = 1$. Puisque $F(1) \equiv 0 \pmod 8$, $F'(1) = 2 \not\equiv 0 \pmod 4$, alors, d'après ce théorème, il existe $\eta \equiv 1 \pmod 4$ tel que $F(\eta) = 0$ i. e. $\varepsilon = \eta^2$.

COROLLAIRE. — *L'indice* $(\mathbf{Q}_2^* : \mathbf{Q}_2^{*2})$ *du sous-groupe des carrés dans le groupe multiplicatif du corps des nombres 2-adiques est égal à 8.*

En effet, d'après le théorème 2, le système des résidus 1, 3, 5, 7 modulo 8 est un système de représentants des classes résiduelles du quotient du groupe des unités 2-adiques par le sous-groupe de ses carrés. Ajoutant à ces nombres les produits 2.1, 2.3, 2.5, 2.7, nous obtenons un système complet de représentants des classes du groupe quotient du groupe $\mathbf{Q}_2^*$ par le sous-groupe $\mathbf{Q}_2^{*2}$.

2) Représentation de zéro par des formes quadratiques p-adiques

Comme dans tout corps, une forme quadratique non singulière sur le corps $\mathbf{Q}_p$ peut s'écrire, par une transformation linéaire de la variable, sous la forme

$$\alpha_1 x_1^2 + \ldots + \alpha_n x_n^2 \qquad (\alpha_i \neq 0)$$

(cf. appendice § 1-1)). Si $\alpha_i = p^{2k_i}\varepsilon_i$ ou $\alpha_i = p^{2k_i+1}\varepsilon_i$ (ε_i unité dans $\mathbf{Z}_p$) alors, par la transformation $y_i = p^{k_i}x_i$, on se ramène à une forme dont tous les coefficients sont des entiers p-adiques divisibles au plus une seule fois par p. Ainsi toute forme quadratique non singulière sur $\mathbf{Q}_p$ est équivalente à une forme du type

$$F = F_0 + pF_1 = \varepsilon_1 x_1^2 + \ldots + \varepsilon_r x_r^2 + p(\varepsilon_{r+1}x_{r+1}^2 + \ldots + \varepsilon_n x_n^2), \quad (2)$$

où les ε_i sont des unités p-adiques.

Dans la recherche des représentations de zéro, nous pouvons supposer $r \geqslant n - r$. En effet, il est clair que la forme pF est équivalente à la forme $F_1 + pF_0$. Puisque F et pF représentent simultanément zéro ou pas, à la place de la forme $F_0 + pF_1$, nous pouvons considérer la forme $F_1 + pF_0$.

Considérons d'abord le cas $p \neq 2$.

THÉORÈME 3. — *Soit $p \neq 2$ et $0 < r < n$. La forme* (2) *représente zéro dans le corps $\mathbf{Q}_p$ si et seulement si une au moins des formes F_0 ou F_1 représente zéro.*

DÉMONSTRATION. — Supposons que la forme (2) représente zéro :

$$\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 + p(\varepsilon_{r+1}\xi_{r+1}^2 + \ldots + \varepsilon_n\xi_n^2) = 0. \quad (3)$$

Il est clair que nous pouvons supposer que tous les ξ_i sont entiers et que l'un au moins d'entre eux n'est pas divisible par p. Si $\xi_1 \not\equiv 0 \pmod p$, alors, passant à la congruence modulo p dans (3), on a :

$$F_0(\xi_1, \ldots, \xi_r) \equiv 0 \pmod p ;$$

$$\frac{\partial F_0}{\partial x_1}(\xi_1, \ldots, \xi_r) = 2\varepsilon_1\xi_1 \not\equiv 0 \pmod p.$$

D'après le corollaire du théorème 3 § 5, la forme F_0 représente zéro. Supposons maintenant que toutes les valeurs $\xi_1, \ldots, \xi_r$ sont divisibles par p, d'où $\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 \equiv 0 \pmod{p^2}$. Passons à la congruence modulo p^2 dans (3). Simplifiant cette congruence par p, nous obtenons

$$F_1(\xi_{r+1}, \ldots, \xi_n) \equiv 0 \pmod p$$

où l'un au moins des $\xi_{r+1}, \ldots, \xi_n$ n'est pas divisible par p. En appliquant à nouveau le corollaire du théorème 3 du § 5, nous en concluons que, dans ce cas, la forme F_1 représente zéro. Puisque la suffisance de la condition est évidente, la démonstration du théorème 3 est terminée.

Nous avons incidemment obtenu le résultat suivant.

COROLLAIRE 1. — *Si $\varepsilon_1, \ldots, \varepsilon_r$ sont des unités p-adiques, alors, pour $p \neq 2$, la forme $f = \varepsilon_1 x_1^2 + \ldots + \varepsilon_r x_r^2$ représente zéro dans $\mathbf{Q}_p$ si et seulement si la congruence $f(x_1, \ldots, x_r) \equiv 0 \pmod p$ a une solution non triviale dans $\mathbf{Z}_p$.*

COROLLAIRE 2. — *Sous les mêmes hypothèses, si $r \geqslant 3$, alors la forme $f(x_1, \ldots, x_r)$ représente toujours zéro dans $\mathbf{Z}_p$.*

En effet, d'après le théorème 5, § 1, la congruence $f(x_1, \ldots, x_r) \equiv 0 \pmod p$ a une solution non triviale.

Dans la démonstration du théorème 3, nous n'avons pas complètement utilisé l'égalité (3) : nous avons seulement eu besoin des congruences $F \equiv 0 \pmod p$ et $F \equiv 0 \pmod{p^2}$. Ainsi, il résulte de la résolubilité de la deuxième de ces congruences que l'une des formes F_0 ou F_1 et par suite F, représente zéro. Nous avons donc

COROLLAIRE 3. — *Pour $p \neq 2$, la forme* (2) *représente zéro si et seulement si la congruence $F \equiv 0 \pmod{p^2}$ a une solution telle que la valeur d'une au moins des inconnues ne soit pas divisible par p.*

Passons maintenant à l'étude des formes quadratiques sur le corps des nombres 2-adiques. Dans ce cas, le théorème 3 et tous ses corollaires sont faux. Par exemple, pour la forme $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$, l'équation $f = 0$ n'a pas de solution non triviale dans $\mathbf{Q}_2$ (puisque déjà la congruence $f \equiv 0 \pmod 8$ n'a pas de solution dont l'une des inconnues soit impaire). Pourtant, la forme $f + 2x_5^2$ représente zéro dans $\mathbf{Q}_2$ (théorème 5).

THÉORÈME 4. — *Dans le corps des nombres 2-adiques, la forme* (2) (avec $p = 2$) *représente zéro si et seulement si la congruence* $F \equiv 0 \pmod{16}$ *admet une solution dont l'une des inconnues est impaire.*

DÉMONSTRATION. — Soit $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{16}$, l'un au moins des nombres entiers p-adiques ξ n'étant pas divisible par 2. Supposons tout d'abord que $\xi_i \not\equiv 0 \pmod 2$ pour au moins un $i \leqslant r$; soit par exemple $\xi_1 \not\equiv 0 \pmod 2$. Puisque $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod 8$ et $\frac{\partial F}{\partial x_1}(\xi_1, \ldots, \xi_n) \not\equiv$ (mod 4), alors, d'après le théorème 3 § 5 (avec $\delta = 1$) la forme F représente zéro. Supposons maintenant que $\xi_1, \ldots, \xi_r$ sont divisibles par 2, i. e. $\xi_i = 2\eta_i$ $(1 \leqslant i \leqslant r)$, les η_i étant des entiers 2-adiques. Simplifiant par 2 la congruence

$$4\sum_{i=1}^{r} \varepsilon_i \eta_i^2 + 2\sum_{i=r+1}^{n} \varepsilon_i \xi_i^2 \equiv 0 \pmod{16},$$

nous obtenons

$$\sum_{i=r+1}^{n} \varepsilon_i \xi_i^2 + 2\sum_{i=1}^{r} \varepsilon_i \eta_i^2 \equiv 0 \pmod 8,$$

l'un des $\xi_{r+1}, \ldots, \xi_n$ n'étant pas divisible par 2. Comme ci-dessus, cette congruence entraîne que la forme $F_1 + 2F_0$ représente zéro. Mais la forme 2[illegible] qui lui est équivalente représente alors aussi zéro, d'où la suffisance de la condition. La réciproque est évidente.

Dans la démonstration du théorème 4, nous avons aussi obtenu le résultat suivant.

COROLLAIRE. — *Si pour la forme* (2) *(avec* $p = 2$*), la congruence* $F \equiv$ (mod 8) *a une solution dont l'une au moins des inconnues* $x_1, \ldots, x_r$ [illegible] *impaire, alors cette forme représente zéro dans le corps* $\mathbf{Q}_2$.

THÉORÈME 5. — *Dans le corps* $\mathbf{Q}_p$ *des nombres p-adiques, toute forme quadratique non singulière de cinq ou plus de cinq variables représente toujours zéro.*

DÉMONSTRATION. — On peut supposer que la forme donnée est du type (2) avec $r \geqslant n - r$. Puisque $n \geqslant 5$, alors $r \geqslant 3$. Supposons $p \neq 2$. Dans ce cas, d'après le corollaire 2 du théorème 3, la forme F_0 représente zéro, ce qui entraîne que la forme F représente zéro.

Soit maintenant $p = 2$. Si $n - r > 0$, considérons la forme « partielle »

$$f = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + 2\varepsilon_n x_n^2.$$

Une telle forme représente toujours zéro dans $\mathbf{Q}_2$. En effet, puisque $\varepsilon_1 + \varepsilon_2 = 2\alpha$ (α entier 2-adique), alors

$$\varepsilon_1 + \varepsilon_2 + 2\varepsilon_n \alpha^2 \equiv 2\alpha + 2\alpha^2 = 2\alpha(1 + \alpha) \equiv 0 \pmod 4,$$

i. e. $\varepsilon_1 + \varepsilon_2 + 2\varepsilon_n \alpha^2 = 4\beta$, β entier 2-adique. Posant $x_1 = x_2 = 1$, $x_3 = 2\beta$, $x_n = \alpha$, nous avons

$$\varepsilon_1 . 1^2 + \varepsilon_2 . 1^2 + \varepsilon_3 (2\beta)^2 + 2\varepsilon_n \alpha^n \equiv 4\beta + 4\beta^2 \equiv 0 \pmod 8.$$

D'après le corollaire du théorème 4, la forme f représente zéro; mais alors F représente aussi zéro. Dans le cas où $n = r$, on prend pour forme « partielle »

$$f = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + \varepsilon_4 x_4^2 + \varepsilon_5 x_5^2.$$

Si $\varepsilon_1 + \varepsilon_2 \equiv \varepsilon_3 + \varepsilon_1 \equiv 2 \pmod 4$, posons $x_1 = x_2 = x_3 = x_4 = 1$ et si par exemple $\varepsilon_1 + \varepsilon_2 \equiv 0 \pmod 4$ posons $x_1 = x_2 = 1$, $x_3 = x_4 = 0$. Dans les deux cas

$$\varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + \varepsilon_4 x_4^2 = 4\gamma,$$

γ entier 2-adique. Posant $x_5 = 2\gamma$, nous obtenons

$$f \equiv 4\gamma + 4\gamma^2 \equiv 0 \pmod 8.$$

Le corollaire du théorème 4 montre que, dans ce cas, le théorème est démontré.

D'après le théorème 6, § 1 de l'appendice, le théorème 5 entraîne ce qui suit.

COROLLAIRE 1. — *Dans le corps* $\mathbf{Q}_p$, *toute forme quadratique non singulière de quatre ou plus de quatre variables représente tous les nombres p-adiques.*

COROLLAIRE 2. — *Soit* $F(x_1, \ldots, x_n)$ *une forme quadratique non singulière à coefficients entiers rationnels. Si* $n \geqslant 5$, *pour tout entier m la congruence* $F(x_1, \ldots, x_n) \equiv 0 \pmod m$ *a une solution non triviale.*

En effet, puisque la forme F représente zéro dans $\mathbf{Q}_p$, pour tout entier $s \geqslant 1$, la congruence $F \equiv 0 \pmod{p^s}$ a une solution pour laquelle une au moins des inconnues n'est pas divisible par p.

3) Formes binaires

Les formes quadratiques binaires constituent un important exemple de la théorie générale des formes quadratiques. Nous considérerons ici le problème de la représentation des nombres du corps $\mathbf{Q}_p$ par une forme quadratique binaire du type

$$x^2 - \alpha y^2, \qquad \alpha \neq 0, \qquad \alpha \in \mathbf{Q}_p \tag{4}$$

(Il est évident que le cas général d'une forme binaire quelconque s'y réduit par transformation des variables et multiplication de la forme par un certain nombre p-adique).

Nous désignerons par H_α l'ensemble de tous les nombres p-adiques dif
rents de zéro représentables par la forme (4). Cet ensemble est toujou
un groupe pour la multiplication. En effet, si $\beta = x^2 - ay^2$, $\beta_1 = x_1^2 - a$
alors, comme le montre un calcul évident,

$$\beta\beta_1 = (xx_1 + \alpha yy_1)^2 - \alpha(xy_1 + yx_1)^2,$$

$$\beta^{-1} = \left(\frac{x}{\beta}\right)^2 - \alpha\left(\frac{y}{\beta}\right)^2.$$

Donnons une autre démonstration de ce fait, basée sur l'étude de l'extensi
quadratique $\mathbf{Q}_p(\sqrt{\alpha})$ du corps $\mathbf{Q}_p$ (à condition que α ne soit pas un ca
dans $\mathbf{Q}_p$).

L'égalité $\beta = x^2 - ay^2$ est équivalente au fait que β est la norme
nombre $\xi = x + y\sqrt{\alpha}$ dans $\mathbf{Q}_p(\sqrt{\alpha})$. Mais si $\beta = N(\xi)$ et $\beta_1 = N(\xi_1)$, al

$$\beta\beta_1 = N(\xi_1\xi) \qquad \text{et} \qquad \beta^{-1} = N(\xi^{-1}).$$

Si α est un carré dans $\mathbf{Q}_p$, la forme (4) représente zéro et par suite tous
nombres de $\mathbf{Q}_p$. Par suite, H_α coïncide avec tout le groupe multiplicatif
corps $\mathbf{Q}_p$.

Puisque la forme (4) représente tous les carrés du corps $\mathbf{Q}_p$ (pour $y =$
alors $\mathbf{Q}_p^{*2} \subset H_\alpha$. Mais, d'après les corollaires des théorèmes 1 et 2, l'
dice $(\mathbf{Q}_p^* : \mathbf{Q}_p^{*2})$ est fini et par suite H_α a un indice fini dans $\mathbf{Q}_p^*$.

THÉORÈME 6. — *Si le nombre $\alpha \in \mathbf{Q}_p^*$ n'est pas un carré, alors* $(\mathbf{Q}_p^* : H_\alpha) =$

DÉMONSTRATION. — Remarquons d'abord que la forme (4) représe
un nombre p-adique β si et seulement si la forme

$$\alpha x^2 + \beta y^2 - z^2$$

représente zéro (théorème 6, § 1 de l'appendice). De plus, la condition p
que la forme (5) représente zéro ne change pas si on multiplie α et β par
carrés; nous pouvons donc supposer que α et β sont des éléments fixés d
chaque classe résiduelle du quotient du groupe $\mathbf{Q}_p^*$ par le groupe $\mathbf{Q}_p^{*2}$.

Considérons d'abord le cas $p \neq 2$ et montrons que $H_\alpha \neq \mathbf{Q}_p^{*2}$. C'
évident si $-\alpha$ n'est pas un carré (puisque $-\alpha \in H_\alpha$). Si maintenant $-$
est un carré, la forme $x^2 - \alpha y^2$ est équivalente à la forme $x^2 + y^2$ qui rep
sente toutes les unités p-adiques (corollaire 2 du théorème 3); cela signi
que, dans ce cas, H_α ne coïncide pas avec $\mathbf{Q}_p^{*2}$. De plus, H_α ne coïncide p
avec $\mathbf{Q}_p^*$ (si, bien sûr, $\alpha \notin \mathbf{Q}_p^{*2}$). En effet, choisissant une unité p-adique
qui n'est pas un carré, nous pouvons nous borner à donner à α les valeurs ε,
et $p\varepsilon$. Mais d'après le théorème 3 (et le théorème 10 du § 1 de l'appendice)
la forme (5) ne représente pas zéro pour $\alpha = \varepsilon$, $\beta = p$ ni pour $\alpha = p$, p

$\beta = \varepsilon$. Ainsi, on a bien $H_\alpha \neq \mathbf{Q}_p^*$. Appliquons maintenant le corollaire 2 du théorème 1. Puisque $\mathbf{Q}_p^* \supset H_\alpha \supset \mathbf{Q}_p^{*2}$, alors l'indice $(\mathbf{Q}_p^* : H_\alpha)$ est un diviseur de l'indice $(\mathbf{Q}_p^* : \mathbf{Q}_p^{*2}) = 4$. Mais, d'après ce qui précède, il ne peut être égal ni à 4 ni à 1; par suite, $(\mathbf{Q}_p^* : H_\alpha) = 2$, ce qui démontre le théorème 6 dans le cas $p \neq 2$.

Soit maintenant $p = 2$. Il existe alors 8 classes résiduelles de $\mathbf{Q}_2^*$ selon $\mathbf{Q}_2^{*2}$ dont on peut prendre comme représentants les nombres 1, 3, 5, 7, 2.1, 2.3, 2.5, 2.7. Nous considérerons donc que α et β dans la forme (5) coïncident avec l'un de ces nombres et nous expliciterons dans quels cas cette forme représente zéro dans $\mathbf{Q}_2$. La réponse à cette question est donnée par le tableau ci-dessous, dans lequel le signe + indique que pour les valeurs correspondantes de α et β la forme représente zéro; les cases vides correspondent à des formes ne représentant pas zéro.

α \ β	1	3	5	7	2.1	2.3	2.5	2.7
1	+	+	+	+	+	+	+	+
3	+		+			+		+
5	+	+	+	+				
7	+		+		+		+	
2.1	+			+	+			+
2.3	+	+					+	+
2.5	+			+		+	+	
2.7	+	+			+	+		

(D'après la symétrie des rôles de α et β dans la forme (5), les signes + du tableau sont répartis symétriquement par rapport à la diagonale principale). Dans chaque ligne à l'exception de la première, le signe + figure dans quatre cases. Cela signifie que pour tout $\alpha \in \mathbf{Q}_2^*$ qui n'est pas un carré, il y a quatre classes résiduelles selon le sous-groupe $\mathbf{Q}_2^{*2}$ qui sont représentables par la

forme (4). Ainsi $(H_\alpha : \mathbf{Q}_2^{*2}) = 4$ et puisque $(\mathbf{Q}_2^* : \mathbf{Q}_2^{*2}) = 8$ (corollaire d théorème 2), alors $(\mathbf{Q}_2^* : H_\alpha) = 2$.

Le tableau est établi à partir des résultats de 2). Soient $\alpha = 2\varepsilon$, $\beta = 2$ où ε et η sont des unités 2-adiques et supposons

$$2\varepsilon x^2 + 2\eta y^2 - z^2 = 0.$$

Nous pouvons supposer que x, y, z sont des entiers qui ne sont pas to divisibles simultanément par 2. Il est clair que $z \equiv 0 \pmod 2$ et que x et ne sont pas simultanément divisibles par 2 (car sinon la partie gauche de ne serait pas divisible par (4)). Posant $z = 2t$, l'égalité (6) devient

$$\varepsilon x^2 + \eta y^2 - 2t^2 = 0;$$

en accord avec le corollaire du théorème 4, cette égalité équivaut à u congruence modulo 8 (avec x et y impairs). Puisque $x^2 \equiv y^2 \equiv 1 \pmod$ et $2t^2 \equiv 2 \pmod 8$ ou $2t^2 \equiv 0 \pmod 8$, alors nous obtenons que la réso bilité de l'équation (6) est équivalente à la réalisation d'une au moins congruences.

$$\varepsilon + \eta \equiv 2 \pmod 8, \qquad \varepsilon + \eta \equiv 0 \pmod 8.$$

Soit maintenant $\alpha = 2\varepsilon$, $\beta = \eta$. Dans l'égalité $2\varepsilon x^2 + \eta y^2 - z^2 = 0$ (a x, y, z entiers 2-adiques non divisibles par 2 simultanément), nous avo pour ces mêmes raisons, $y \not\equiv 0 \pmod 2$ et $z \not\equiv 0 \pmod 2$. Par suite, la r lisation de cette égalité (d'après le même corollaire du théorème 4) est éq valente à la réalisation d'une au moins des congruences

$$2\varepsilon + \eta \equiv 1 \pmod 8, \qquad \varepsilon \equiv 1 \pmod 8,$$

qui correspondent aux cas $2 \nmid x$ et $2|x$.

Il reste encore à examiner le cas $\alpha = \varepsilon$, $\beta = \eta$. Si dans l'égalité

$$\varepsilon x^2 + \eta y^2 - z^2 = 0,$$

les entiers 2-adiques x, y, z ne sont pas tous divisibles par 2 alors l'un d'en eux est divisible par 2 mais les autres pas. Si $z \equiv 0 \pmod 2$, alors

$$\varepsilon x^2 + \eta y^2 \equiv \varepsilon + \eta \equiv 0 \pmod 4,$$

d'où il résulte que soit $\varepsilon \equiv 1 \pmod 4$, soit $\eta \equiv 1 \pmod 4$. Si mainten $z \not\equiv 0 \pmod 2$, alors $\varepsilon x^2 + \eta y^2 \equiv 1 \pmod 4$ et puisque l'un des nombre ou y est divisible par 2, alors l'autre ne l'est pas. Nous obtenons alors nouveau que l'une des congruences

$$\varepsilon \equiv 1 \pmod 4, \qquad \eta \equiv 1 \pmod 4$$

est réalisée. Réciproquement, supposons par exemple que $\varepsilon \equiv 1 \pmod 4$. Alors la congruence $\varepsilon x^2 + \eta y^2 - z^2 \equiv 0 \pmod 8$ est réalisée pour $x = 1$, $y = 0$, $z = 1$ si $\varepsilon \equiv 1 \pmod 8$ et pour $x = 1$, $y = 2$, $z = 1$ si $\varepsilon \equiv 5 \pmod 8$; cela signifie que la forme $\varepsilon x^2 + \eta y^2 - z^2$ représente zéro.

Après avoir terminé la vérification du tableau, on a, en même temps, démontré le théorème 6.

Du théorème 6 résulte que pour un nombre p-adique $\alpha \neq 0$ qui n'est pas un carré, le groupe quotient $\mathbf{Q}_p^*/H_\alpha$ est un groupe cyclique d'ordre 2. On peut donc établir un isomorphisme de ce groupe avec le groupe $\{1, -1\}$ des racines d'ordre 2 de 1. Cet isomorphisme entre $\mathbf{Q}_p^*/H_\alpha$ et $\{1, -1\}$ associe au sous-groupe H_α le nombre $+1$ et à la classe résiduelle βH_α distincte de H_α le nombre -1. Il convient d'examiner cet homomorphisme du groupe $\mathbf{Q}_p^*$ dans le groupe $\{+1, -1\}$, de noyaux H_α.

DÉFINITION. — *Pour des nombres p-adiques $\alpha \neq 0$ et $\beta \neq 0$, définissons le symbole (α, β) comme égal à $+1$ ou -1 suivant que la forme $\alpha x^2 + \beta y^2 - z^2$ représente ou non zéro dans le corps $\mathbf{Q}_p$. Le symbole (α, β) s'appelle symbole de Hilbert.*

De cette définition résulte immédiatement que si α est un carré, alors $(\alpha, \beta) = 1$ pour tout β. Si maintenant $\alpha \notin \mathbf{Q}_p^{*2}$, alors $(\alpha, \beta) = 1$ si et seulement si $\beta \in H_\alpha$. On en déduit facilement que pour tout $\alpha \neq 0$, l'application $\beta \to (\alpha, \beta)$ est un homomorphisme du groupe $\mathbf{Q}_p^*$ dans le groupe $\{1, -1\}$ de noyau H_α. En d'autres termes, on a la formule

$$(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)(\alpha, \beta_2). \tag{9}$$

De plus, la valeur du symbole (α, β) dépend de la résolubilité de l'équation (5) qui dépend symétriquement de α et β; par suite

$$(\alpha, \beta) = (\beta, \alpha), \tag{10}$$

d'où, d'après (9),

$$(\alpha_1\alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta). \tag{11}$$

Remarquons encore que

$$(\alpha, -\alpha) = 1 \tag{12}$$

pour tout $\alpha \in \mathbf{Q}_p^*$ (puisque l'équation $\alpha x^2 - \alpha y^2 - z^2 = 0$ admet la solution $x = y = 1$, $z = 0$), d'où, d'après (9),

$$(\alpha, \alpha) = (\alpha, -1). \tag{13}$$

D'après les formules (9) à (13), le calcul du symbole (α, β) dans le général se ramène au calcul des valeurs (p, ε) et (ε, η), ε et η étant des un p-adiques. En effet, si $\alpha = p^k\varepsilon$, $\beta = p^l\eta$, alors

$$(p^k\varepsilon, p^l\eta) = (p, p)^{kl}(\varepsilon, p)^l(p, \eta)^k(\varepsilon, \eta) = (p, \varepsilon^l\eta^k(-1)^{kl})(\varepsilon, \eta).$$

Effectuons le calcul des valeurs (p, ε) et (ε, η). Si $p \neq 2$, alors, d'apr théorème 3, la forme $px^2 + \varepsilon y^2 - z^2$ représente zéro si et seulemen $\varepsilon y^2 - z^2$ représente zéro, i. e. si l'unité ε est un carré. Ainsi $(p, \varepsilon) =$ pour $p \neq 2$ (voir 1)). De plus, d'après le corollaire 2 du théorème 3 forme $\varepsilon x^2 + \eta y^2 - z^2$ représente toujours zéro et cela signifie que $(\varepsilon, \eta) =$ pour tout couple ε, η d'unités p-adiques ($p \neq 2$).

Dans le cas $p = 2$, les valeurs des symboles $(2, \eta)$ et (ε, η) pour des un 2-adiques ε et η ont déjà été virtuellement déterminées dans la démonstra du théorème 6. En effet, d'après (7) (pour $\varepsilon = 1$), la forme $2x^2 + \eta y^2$ représente zéro si et seulement si $\eta \equiv +1 \pmod 8$. Par suite,

$$(2, \eta) = (-1)^{\frac{\eta^2-1}{8}}.$$

De plus, nous avons vu que la forme $\varepsilon x^2 - \eta y^2 - z^2$ représente zéro seulement si une des congruences (8) est réalisée. Par suite,

$$(\varepsilon, \eta) = (-1)^{\frac{\varepsilon-1}{2}\cdot\frac{\eta-1}{2}}.$$

Formulons le résultat obtenu.

THÉORÈME 7. — *Les valeurs des symboles de Hilbert (p, ε) et (ε, η) p des unités p-adiques ε et η sont définies par les formules*

$$(p, \varepsilon) = \left(\frac{\varepsilon}{p}\right), \qquad (\varepsilon, \eta) = 1 \quad \text{pour} \quad p \neq 2;$$

$$(2, \varepsilon) = (-1)^{\frac{\varepsilon^2-1}{8}}, \qquad (\varepsilon, \eta) = (-1)^{\frac{\varepsilon-1}{2}\cdot\frac{\eta-1}{2}} \quad \text{pour} \quad p = 2.$$

4) Équivalence des formes binaires

Le symbole de Hilbert permet d'écrire sous forme évidente la conditio d'équivalence de deux formes quadratiques binaires dans le corps $\mathbf{Q}_p$. Soient $f(x, y)$ et $g(x, y)$ deux formes quadratiques binaires non singulière

à coefficients dans $\mathbf{Q}_p$ et soient $\delta(f)$ et $\delta(g)$ leurs déterminants. Pour que les deux formes f et g soient équivalentes, il est nécessaire que $\delta(f)$ et $\delta(g)$ diffèrent par un facteur multiplicatif appartenant à $\mathbf{Q}_p^{*2}$ (théorème 1, § 1 de l'appendice). Pour formuler une condition nécessaire et suffisante d'équivalence, établissons le théorème suivant.

THÉORÈME 8. — *Pour tout nombre p-adique $\alpha \neq 0$ représentable par une forme binaire f de déterminant $\delta \neq 0$, la valeur du symbole de Hilbert $(\alpha, -\delta)$ est la même.*

DÉMONSTRATION. — Soient α et α' deux nombres p-adiques non nuls représentables par la forme f. D'après le théorème 2, § 1 de l'appendice la forme f est équivalente à une forme f_1 du type $\alpha x^2 + \beta y^2$. Puisque α' est également représentable par la forme f_1, alors

$$\alpha' = \alpha x_0^2 + \beta y_0^2, \qquad \text{d'où} \qquad \alpha\alpha' - \alpha\beta y_0^2 - (\alpha x_0)^2 = 0.$$

Cette dernière équation exprime que la forme $\alpha\alpha' x^2 - \alpha\beta y^2 - z^2$ représente zéro et par suite $(\alpha\alpha', -\alpha\beta) = 1$. Mais $\alpha\beta$ diffère de δ par un carré ; c'est pourquoi nous avons aussi $(\alpha\alpha', -\delta) = -1$ et cela entraîne, d'après la propriété (11), $(\alpha, -\delta) = (\alpha', -\delta)$; ainsi, notre théorème est démontré.

D'après le théorème 8, nous pouvons introduire pour toute forme binaire f un nouvel invariant

$$e(f) = (\alpha, -\delta(f))$$

où α est un nombre p-adique différent de zéro représentable par la forme f.

THÉORÈME 9. — *Pour que deux formes quadratiques binaires non singulières f et g sur $\mathbf{Q}_p$ soient équivalentes, il faut et il suffit que les conditions ci-dessous soient réalisées* :

1) $\delta(f) = \delta(g)\gamma^2, \qquad \gamma \in \mathbf{Q}_p^*$;

2) $e(f) = e(g)$.

DÉMONSTRATION. — La nécessité de ces deux conditions est évidente. Pour démontrer la suffisance montrons que, si les conditions du théorème sont remplies, les formes f et g représentent les mêmes nombres p-adiques. Soit $\gamma \in \mathbf{Q}_p^*$ un nombre représentable par la forme g. Supposant la forme f du type $\alpha x^2 + \beta y^2$, nous aurons

$$(\alpha, -\alpha\beta) = e(f) = e(g) = (\gamma, -\delta(g)) = (\gamma, -\alpha\beta),$$

d'où

$$(\gamma\alpha^{-1}, -\alpha\beta) = 1.$$

D'après la définition du symbole de Hilbert, cela signifie que l'équation

$$\gamma\alpha^{-1}x^2 - \alpha\beta y^2 - z^2 = 0$$

est résoluble avec x, y, z différents de zéro. Mais alors

$$\gamma = \alpha\left(\frac{z}{x}\right)^2 + \beta\left(\frac{\alpha y}{x}\right)^2$$

i. e. la forme f représente γ. L'équivalence de f et g résulte alors du théorème 11, § 1 de l'appendice.

5) Remarques sur les formes de degré plus grand

Le théorème 5 traduit un phénomène que l'on rencontre souvent en théorie des nombres : « tout se passe bien » si le nombre de variables est assez grand. Dans notre cas, « bien » signifie que la forme quadratique représente zéro dans le corps $\mathbf{Q}_p$ et « suffisamment grand » que le nombre de variables est $\geqslant 5$. Il serait très intéressant de continuer cette étude pour des formes de degré plus grand sur le corps des nombres p-adiques.

Le résultat exact est le suivant. Pour tout nombre naturel r, il existe un nombre $N(r)$ tel que toute forme de degré r sur le corps des nombres p-adiques dont le nombre de variables est $> N(r)$ représente zéro. L'existence d'un nombre $N(r)$ est loin d'être évidente *a priori*. Nous avons examiné ci-dessus le cas $r = 2$; les exemples de formes de degré supérieur que l'on peut examiner rendent très probable que $N(r) = r^2$, i. e. on a la conjecture suivante :

Toute forme de degré r à coefficients p-adiques et dont le nombre de variables est plus grand que r^2 représente zéro (*).

On connaît très peu de résultats généraux en direction de cette conjecture. Brauer a démontré la finitude du nombre $N(r)$ mais l'estimation obtenue à partir de sa démonstration est bien supérieure à r^2 (R. Brauer, A note on systems of homogeneous algebraic equations. *Bull. Amer. Math. Soc.*, 1945, **51**, 749-755). Pour $r = 2$, la vérification de la conjecture repose sur le théorème 5. Pour $r = 3$, la conjecture a été démontrée par V. B. Demianov et D. J. Lewis : ils ont démontré que toute forme cubique sur le corps des nombres p-adiques dont le nombre de variable est $\geqslant 10$ représente zéro (V. B. Demianov, Sur les formes cubiques dans les corps métriques. *Dokl. Akad. Nauk URSS*, 1950, **74**, n° 5, 889-891 ; D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields. *Ann. Math.*, 1952, **56**, n° 3, 473-478).

(*) On sait maintenant, grâce à un exemple construit par G. Terjanian, que cette conjecture est *fausse* ; cf. *C. R. Acad. Sci.*, Paris, 1966. Toutefois, J. Ax et S. Kochen ont prouvé que, pour un degré r donné, elle est vraie pour toutes les valeurs de p sauf un nombre fini (dépendant de r) ; cf. *Amer. J. of Math.*, 1965 (note communiquée par M. J. P. Serre).

En outre, Lang a démontré que si la conjecture est vraie pour tout r, on a également le résultat plus fort suivant :

Le système d'équations

$$\left.\begin{aligned} F_1(x_1, \ldots, x_m) &= 0 \\ &\vdots \\ F_k(x_1, \ldots, x_m) &= 0 \end{aligned}\right\} \tag{14}$$

dans lequel $F_1, \ldots, F_k$ sont des formes de degrés $r_1, \ldots, r_k$ à coefficients p-adiques a une solution non nulle si le nombre m de variables est plus grand que $r_1^2 + \ldots + r_k^2$ (S. Lang, On quasi algebraic closure. *Ann. Math.*, 1952, **55**, n° 2, 373-390).

Dans le cas de deux formes quadratiques, pour $m \geqslant 9$, la résolubilité du système (14) a été démontrée par V. B. Demianof (une démonstration simple du résultat de Demianov est contenue dans : B. J. Birch, D. J. Lewis et T. G. Murphy, Simultaneous quadratic forms. *Amer. J. Math.*, 1962, **84**, n° 1, 110-115).

Il est enfin facile de montrer que la valeur hypothétique $N(r) = r^2$ est une borne inférieure, i. e. pour tout r il existe des formes de degré r à r^2 variables ne représentant pas zéro dans le corps des nombres p-adiques. Construisons un exemple d'une telle forme.

Rappelons dans ce but que, au point 2 § 1 de ce chapitre, on a construit une forme $F(x_1, \ldots, x_n)$ de degré n et à n variables telle que la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

n'ait que la seule solution :

$$x_1 \equiv 0 \pmod{p}, \ldots, x_n \equiv 0 \pmod{p}. \tag{15}$$

Posons

$$\Phi(x_1, \ldots, x_{n^2}) = F(x_1, \ldots, x_n) + pF(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-1}F(x_{n^2-n+1}, \ldots, x_{n^2})$$

et démontrons que la forme Φ ne représente pas zéro dans le corps des nombres p-adiques. Raisonnons par l'absurde, i. e. supposons que l'équation

$$\Phi(x_1, \ldots, x_n) = 0 \tag{16}$$

ait une solution non nulle. D'après l'homogénéité de Φ, nous pouvons supposer que toutes les inconnues sont des entiers et que l'un au moins n'est pas divisible par p. Considérant (16) modulo p, on a $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ d'où, d'après (15), $x_1 = px_1', \ldots, x_n = px_n'$. L'égalité (16) prend maintenant la forme

$$p^n F(x_1', \ldots, x_n') + pF(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-1}F(x_{n^2-n+1}, \ldots, x_{n^2}) = 0$$

ou encore, après simplification par p,

$$F(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-2}F(x_{n^2-n+1}, \ldots, x_{n^2}) + \ldots + p^{n-1}F(x'_1, \ldots, x'_n) = 0$$

Par suite, $x_{n+1}, \ldots, x_{2n}$ sont divisibles par p. Répétant ce raisonnement n fois, nous démontrerions que $x_1, \ldots, x_{n^2}$ sont tous divisibles par p ce qui contredit notre hypothèse initiale.

EXERCICES

1. Démontrer les propriétés suivantes du symbole de Hilbert :

1) $(\alpha, 1-\alpha) = +1, \quad \alpha \neq 1;$

2) $(\alpha, \beta) = (\gamma, -\alpha\beta), \quad \gamma = \alpha\xi^2 + \beta\eta^2 \neq 0;$

3) $(\alpha\gamma, \beta\gamma) = (\alpha, \beta)(\gamma, -\alpha\beta).$

2. Soit $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ $(\alpha_i \in \mathbf{Q}_p^*)$ une forme quadratique ; l'expression

$$c_p(f) = (-1, -1) \prod_{1 \leqslant i \leqslant j \leqslant n} (\alpha_i, \alpha_j)$$

s'appelle le symbole de Hasse de la forme f. Démontrer que

$$c_p(\alpha x^2 + f) = c_p(f)(\alpha, -\delta),$$

$$c_p(\alpha x^2 + \beta y^2 + f) = c_p(f)(\alpha\beta, -\delta)(\alpha, \beta)$$

(δ est le déterminant de la forme f).

3. Soit $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ une forme à coefficients p-adiques représentant un nombre $\gamma \neq 0$ de $\mathbf{Q}_p$. Montrer que γ peut s'écrire sous la forme

$$\gamma = \alpha_1 \xi_1^2 + \ldots + \alpha_n \xi_n^2 \qquad (\xi_i \in \mathbf{Q}_p),$$

toutes les sommes « partielles »

$$\gamma_k = \alpha_1 \xi_1^2 + \ldots + \alpha_k \xi_k^2 \qquad (1 \leqslant k \leqslant n)$$

étant différentes de zéro (utiliser les théorèmes 5 et 8 du § 1 de l'appendice).

4. Sous les hypothèses de l'exercice précédent, montrer que la forme f est équivalente à une forme diagonale du type

$$g = \gamma y_1^2 + \beta_2 y_2^2 + \ldots + \beta_n y_n^2 \quad \text{telle que} \quad c_p(g) = c_p(f)$$

(on démontrera tout d'abord que par le changement de variable $x = \mu X - \nu\beta Y$, $y = \nu X + \mu\alpha Y$ $(\alpha\mu^2 + \beta\nu^2 = \gamma \neq 0)$ la forme $\alpha x^2 + \beta y^2$ s'écrit $\gamma X^2 + \alpha\beta\gamma Y^2$, d'où $(\alpha, \beta) = (\gamma, \alpha\beta\gamma)$).

5. Montrer, par récurrence sur le nombre des variables, que les symboles de Hasse de deux formes quadratiques diagonales non singulières équivalentes sur le corps $\mathbf{Q}_p$ sont égaux (Utiliser le théorème 4 du § 1 de l'appendice). On peut

donc maintenant définir le symbole de Hasse pour des formes quadratiques non singulières quelconques (non nécessairement diagonales) : si la forme f est équivalente à une forme quadratique f_0, nous poserons $c_p(f) = c_p(f_0)$.

6. Soient f_1 et f_2 deux formes quadratiques sur le corps $\mathbf{Q}_p$, de déterminants δ_1 et δ_2. Démontrer que :

$$c_p(f_1 + f_2) = c_p(f_1)\, c_p(f_2)(-1, -1)(\delta_1, \delta_2).$$

7. Soit f une forme quadratique non singulière sur le corps $\mathbf{Q}_p$, de déterminant δ et soit $\alpha \neq 0$ un nombre du corps $\mathbf{Q}_p$. Montrer que

$$c_p(\alpha f) = \begin{cases} c_p(f)\left(\alpha, (-1)^{\frac{n+1}{2}}\right), & \text{si } n \text{ impair,} \\ c_p(f)\left(\alpha, (-1)^{\frac{n}{2}}\delta\right), & \text{si } n \text{ pair} \end{cases}$$

8. Démontrer qu'une forme quadratique non singulière f de trois variables sur le corps $\mathbf{Q}_p$ représente zéro si et seulement si $c_p(f) = +1$.

9. Soit f une forme quadratique non singulière de quatre variables sur le corps $\mathbf{Q}_p$, de déterminant δ. Montrer que f ne représente pas zéro dans $\mathbf{Q}_p$ si et seulement si δ est un carré dans $\mathbf{Q}_p$ et $c_p(f) = -1$.

10. Soit f une forme quadratique non singulière de n variables sur le corps $\mathbf{Q}_p$, de déterminant δ. Montrer que f représente un nombre p-adique $\alpha \neq 0$ si et seulement si l'une des conditions suivantes est remplie :

1) $n = 1$ et $\alpha\delta$ est un carré dans $\mathbf{Q}_p$;
2) $n = 2$ et $c_p(f) = (-\alpha, -\delta)$;
3) $n = 3$, $\alpha\delta$ est un carré dans $\mathbf{Q}_p$ et $c_p(f) = 1$;
4) $n = 3$ et $\alpha\delta$ n'est pas un carré dans $\mathbf{Q}_p$;
5) $n \geqslant 4$.

11. Donner des conditions pour qu'une forme quadratique non singulière sur le corps $\mathbf{Q}_p$ ne représente pas zéro (sauf de manière triviale) mais représente tous les autres nombres p-adiques.

12. Dans quels corps de nombres p-adiques la forme $2x^2 - 5y^2 + 14z^2$ ne représente-t-elle pas zéro ?

13. Quels sont les nombres 5-adiques qui sont représentés par la forme $2x^2 + 5y^2$?

14. Soient f et f' deux formes quadratiques non singulières à n variables sur le corps $\mathbf{Q}_p$ et δ et δ' leurs déterminants. Démontrer que f et f' sont équivalentes si et seulement si $c_p(f) = c_p(f')$ et $\delta = \delta'\alpha^2$ $(\alpha \in \mathbf{Q}_p)$.

§ 7. — FORMES QUADRATIQUES RATIONNELLES

1) Le théorème de Minkowski-Hasse

Nous exposerons ici la démonstration d'un des plus beaux résultats de la théorie des nombres, le théorème de Minkowski-Hasse.

THÉORÈME 1 (Minkowski-Hasse). — *Une forme quadratique à coefficients rationnels représente zéro dans le corps des nombres rationnels si et seulement si elle représente zéro dans le corps des nombres rationnels et dans tous les corps de nombres p-adiques (pour tout nombre premier p).*

La démonstration de ce théorème dépend de manière essentielle du nombre n de variables de la forme quadratique. Pour $n = 1$, c'est trivial. Pour $n = 2$, la démonstration est encore très simple. Si une forme quadratique binaire rationnelle f de discriminant $d \neq 0$ représente zéro dans le corps des réels, alors $-d > 0$ (cf. appendice § 1, théorème 10); par suite

$$-d = p_1^{k_1} \dots p_s^{k_s},$$

où les p_i sont des nombres premiers deux à deux distincts. Si f représente zéro dans le corps $\mathbf{Q}_{p_i}$, alors, puisque $-d$ est un carré dans $\mathbf{Q}_{p_i}$, l'exposant k_i est pair ($i = 1, \dots, s$). Mais alors $-d$ est un carré aussi dans le corps $\mathbf{Q}$ des nombres rationnels et par suite f représente zéro dans $\mathbf{Q}$.

Pour $n \geqslant 3$, la démonstration du théorème est beaucoup plus compliquée. Faisons quelques remarques pour commencer.

Nous supposerons que les coefficients de la forme quadratique considérée sont des entiers rationnels (car s'il n'en est pas ainsi, nous multiplierons la forme par le dénominateur commun de ses coefficients). Il est clair que la résolubilité de l'équation (1) dans $\mathbf{Q}$ ou dans le corps $\mathbf{Q}_p$ des nombres p-adiques est équivalente, d'après l'homogénéité, à sa résolubilité dans l'anneau $\mathbf{Z}$ des entiers rationnels ou dans l'anneau $\mathbf{Z}_p$ des nombres entiers p-adiques. La résolubilité de (1) dans le corps des nombres réels est équivalente au fait que f est une forme non définie. Par suite et d'après le théorème 2 du § 5, on peut donner au théorème de Minkowski-Hasse la forme suivante :

Pour que l'équation (1) *soit résoluble dans les nombres entiers rationnels, il faut et il suffit que la forme f soit non définie et que pour tout entier de la forme p^m, la congruence*

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p^m}$$

ait une solution telle que la valeur de l'une au moins des inconnues ne soit pas divisible par p.

D'après le théorème 5, § 6, toute forme de cinq variables ou plus représente toujours zéro dans le corps des nombres p-adiques. Par suite pour de telles formes le théorème de Minkowski-Hasse devient :

Pour qu'une forme quadratique rationnelle non singulière de $n \geqslant 5$ variables représente zéro dans le corps des nombres rationnels, il faut et il suffit qu'elle soit non définie.

Ainsi, il suffit de vérifier les conditions de résolubilité dans les corps de nombres p-adiques pour $n = 3,4$. Pour ces valeurs particulières, le théorème de Minkowski-Hasse nous donne également un critère effectif de résolubilité de l'équation (1). En effet, si la forme f est réduite à une somme de carrés, $f = \Sigma a_i x_i^2$, p premier impair ne divisant aucun des coefficients a_i, la forme f, pour $n \geqslant 3$, représente toujours zéro dans $\mathbf{Q}_p$, d'après le corollaire 2 du théorème 3, § 6. Par suite, les vérifications à effectuer sont relatives seulement à un nombre fini d'entiers premiers. Pour chacun de ces p, la question de la représentation de zéro par f dans $\mathbf{Q}_p$ est résoluble par les théorèmes du paragraphe précédent.

D'après le théorème 6, § 1 de l'appendice, le théorème 1 entraîne le résultat suivant.

COROLLAIRE. — *Pour qu'une forme quadratique non singulière à coefficients rationnels représente un nombre rationnel a, il faut et il suffit qu'elle représente a dans le corps des nombres réels et dans tous les corps $\mathbf{Q}_p$ de nombres p-adiques.*

2) Formes de trois variables

Démontrons le théorème de Minkowski-Hasse dans le cas $n = 3$. Pour les formes de 3 variables, le théorème 1 a été démontré (sous une autre forme) par Legendre. La formulation de Legendre est exposée dans l'exercice 1.

Supposons la forme réduite à une somme de carrés $a_1x^2 + a_2y^2 + a_3z^2$. Dire que la forme est non définie signifie que les trois coefficients a_1, a_2, a_3 ne sont pas de même signe. Multipliant la forme par -1 si cela est nécessaire, nous sommes ramenés au cas où deux coefficients sont positifs et le troisième négatif. Nous pouvons d'autre part supposer que les nombres a_1, a_2, a_3 sont entiers, non divisibles par des carrés et premiers dans leur ensemble. De plus, si par exemple a_1 et a_2 ont un facteur premier commun p, multipliant la formule par p et prenant px et py comme nouvelles variables, on obtient une forme à coefficients $\frac{a_1}{p}, \frac{a_2}{p}, pa_3$. Répétant plusieurs fois cette opération, notre forme devient une forme du type

$$ax^2 + by^2 - cz^2 \tag{2}$$

dans laquelle a, b, c sont premiers deux à deux (et sans carrés).

Soit p un diviseur premier impair du nombre c. Puisque, par hypothèse, la forme 2 représente zéro dans $\mathbf{Q}_p$, alors, d'après le théorème 3 du § 6 et le corollaire 1 de ce théorème, la congruence

$$ax^2 + by^2 \equiv 0 \pmod{p}$$

a une solution non triviale (disons (x_0, y_0)). Mais alors, la forme $ax^2 + by^2$ est décomposable en facteurs modulo p :

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Ceci est aussi vrai pour la forme (2), i. e. on a une congruence du type

$$ax^2 + by^2 - cz^2 \equiv \mathrm{L}^{(p)}(x, y, z)\ \mathrm{M}^{(p)}(x, y, z) \pmod{p}$$

dans laquelle $\mathrm{L}^{(p)}$ et $\mathrm{M}^{(p)}$ sont des formes linéaires à coefficients entie
On a des congruences analogues pour les diviseurs premiers impairs p d
coefficients a et b et aussi pour $p = 2$, puisque

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod{2}.$$

Prenons maintenant des formes linéaires $\mathrm{L}(x, y, z)$ et $\mathrm{M}(x, y, z)$ telles q

$$\mathrm{L}(x, y, z) \equiv \mathrm{L}^{(p)}(x, y, z) \pmod{p}$$
$$\mathrm{M}(x, y, z) \equiv \mathrm{M}^{(p)}(x, y, z) \pmod{p}$$

pour tous les diviseurs premiers p de l'un des coefficients a, b, c. L
congruences (3) montrent alors que

$$ax^2 + by^2 - cz^2 \equiv \mathrm{L}(x, y, z)\,\mathrm{M}(x, y, z) \pmod{abc}.$$

Imposons aux variables x, y, z de prendre des valeurs entières satisfais
aux conditions

$$0 \leqslant x < \sqrt{bc}, \qquad 0 \leqslant y < \sqrt{ac}, \qquad 0 \leqslant z < \sqrt{ab}.$$

Si nous excluons de cette étude le cas $a = b = c = 1$ (pour la forme

$$x^2 + y^2 - z^2,$$

le théorème est évident : elle représente zéro dans tout corps), alors, puis
a, b, c sont premiers deux à deux, les nombres $\sqrt{bc}$, $\sqrt{ac}$ et $\sqrt{ab}$ ne s
pas tous entiers. Il en résulte facilement que le nombre des triplets $(x, y$
satisfaisant aux conditions (5) est strictement supérieur à

$$\sqrt{ab}.\sqrt{bc}.\sqrt{ac} = abc.$$

Considérons les valeurs prises par la forme linéaire $\mathrm{L}(x, y, z)$ pour
valeurs des variables. Puisque le nombre des triplets (x, y, z) vérifiant
est supérieur au nombre des résidus modulo abc, alors il existe deux tripl
distincts (x_1, y_1, z_1) et (x_2, y_2, z_2) tels que l'on ait la congruence

$$\mathrm{L}(x_1, y_1, z_1) \equiv \mathrm{L}(x_2, y_2, z_2) \pmod{abc}.$$

Il résulte alors de la linéarité de la forme L que

$$\mathrm{L}(x_0, y_0, z_0) \equiv 0 \pmod{abc}$$

pour $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$, $z_0 = z_1 - z_2$.

De la congruence (4) résulte alors

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc}. \tag{6}$$

Puisque les conditions (5) sont réalisées pour les triplets (x_1, y_1, z_1) et (x_2, y_2, z_2) alors

$$|x_0| < \sqrt{bc}, \qquad |y_0| < \sqrt{ac}, \qquad |z_0| < \sqrt{ab},$$

et par suite

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc. \tag{7}$$

L'inégalité (7) est compatible avec la congruence (6) seulement si

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \tag{8}$$

ou bien

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \tag{9}$$

Dans le premier cas nous obtenons une représentation non triviale de zéro par la forme (2); c'est ce qu'il fallait établir. Dans le deuxième cas, nous arriverons au même résultat grâce au lemme suivant.

LEMME 1. — *Si la forme* (2) *représente abc, alors elle représente aussi zéro.*

Soient x_0, y_0, z_0 satisfaisant à l'égalité (9). Il est alors facile de voir que

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0. \tag{10}$$

Si $z_0^2 = ab \neq 0$, alors cette égalité démontre le lemme. Si maintenant $-ab = z_0^2$, alors la forme $ax^2 + by^2$ représente zéro (cf. appendice, § 1, théorème 10). Mais alors la forme (2) représente aussi zéro et par suite le lemme est encore vérifié dans ce cas.

La démonstration du lemme 1 est très courte, mais elle repose sur un calcul qui utilise l'identité (10). Donnons une autre démonstration plus générale. Si bc est un carré, alors la forme $by^2 - cz^2$ et avec elle la forme (2) représente zéro. Supposons que bc n'est pas un carré. Dans ce cas, la représentabilité de zéro par la forme (2) est équivalente au fait que ac est la norme d'un élément du corps $\mathbf{Q}(\sqrt{bc})$. En effet, l'égalité (8) (dans laquelle on peut supposer $x_0 \neq 0$) entraîne

$$ac = \left(\frac{cz_0}{x_0}\right)^2 - bc\left(\frac{y_0}{x_0}\right)^2 = \mathrm{N}\left(\frac{cz_0}{x_0} + \frac{y_0}{x_0}\sqrt{bc}\right).$$

Réciproquement, si $ac = \mathrm{N}(u + v\sqrt{bc})$, alors

$$ac^2 + b(cv)^2 - cu^2 = 0.$$

Supposons maintenant que l'égalité (9) soit satisfaite. En la multipli
par c, elle prend la forme

$$ac(x_0^2 - bc) = (cz_0)^2 - bcy_0^2$$

ou bien

$$ac\mathrm{N}(\alpha) = \mathrm{N}(\beta),$$

avec

$$\alpha = x_0 + \sqrt{bc}, \qquad \beta = cz_0 + y_0\sqrt{bc}.$$

Mais

$$ac = \mathrm{N}(\gamma), \qquad \gamma = \frac{\beta}{\alpha} \in \mathrm{R}(\sqrt{bc}),$$

et cela, comme nous l'avons vu, signifie aussi que la forme (2) repré
zéro dans $\mathbf{Q}$.

Attirons l'attention sur le fait suivant. Dans la démonstration ci-de
du théorème 1 pour trois variables, nous n'avons utilisé nulle part la ré
bilité de l'équation (2) dans le corps des nombres 2-adiques. Par s
la résolubilité de l'équation (2) dans le corps des nombres réels et dan
corps $\mathbf{Q}_p$ pour tout p impair entraîne sa résolubilité aussi dans le corps
On a une propriété analogue pour tout corps $\mathbf{Q}_q$: si une forme quadrat
rationnelle de trois variables représente zéro dans le corps des réels et d
tous les corps $\mathbf{Q}_p$ sauf peut-être dans le corps $\mathbf{Q}_q$, alors elle représente
aussi dans le corps $\mathbf{Q}_q$ (et par suite, d'après le théorème, dans le corp
des nombres rationnels). Essayons d'expliquer ce fait. Considérons p
cela les conditions de représentation de zéro par la forme

$$ax^2 + by^2 - z^2$$

dans les corps $\mathbf{Q}_p$ et dans le corps des nombres rationnels (ici a et b sont
nombres rationnels non nuls) ; il est clair que toute forme quadratique ra
nelle non singulière de trois variables peut être écrite sous la forme (11)
changement linéaire de variables et multiplication par un nombre ration
D'après le point 3) du § 6, la condition de représentabilité de zéro pa
forme (11) dans le corps des nombres p-adiques peut s'écrire

$$\left(\frac{a, b}{p}\right) = 1,$$

où $\left(\frac{a, b}{p}\right)$ est le symbole de Hilbert dans le corps $\mathbf{Q}_p$. Nous adoptons
cette notation pour le symbole de Hilbert (a, b) dans le corps $\mathbf{Q}_p$ po
préciser le corps dans lequel nous le considérons, car nous serons amen
à considérer simultanément des symboles de Hilbert pour plusieurs valeu
de p.

Dans le corps des nombres réels, la forme (11) représente zéro si et seul
ment si au moins un des nombres a, b est positif. Pour écrire cette cond

tion sous la même forme que (12), étendons les résultats du § 6.3 au corps des nombres réels. Utilisons le fait que les corps p-adiques $\mathbf{Q}_p$ et le corps des nombres réels sont tous les complétés du corps $\mathbf{Q}$ des nombres rationnels. Ainsi les corps $\mathbf{Q}_p$ correspondent biunivoquement aux nombres premiers p. Désirant englober dans cette correspondance le corps des nombres réels, on utilise souvent le symbole ∞ appelé nombre premier éloigné à l'infini et on dit que le corps des nombres réels est le complété du corps $\mathbf{Q}$ qui correspond au nombre premier ∞ éloigné à l'infini. Les nombres premiers usuels distincts du symbole ∞ introduit s'appellent alors nombres premiers finis. Par analogie avec la notation $\mathbf{Q}_p$, le corps des nombres réels sera désigné ici par $\mathbf{Q}_\infty$.

Pour tout α du groupe multiplicatif de $\mathbf{Q}_\infty$, considérons la forme

$$x^2 - \alpha y^2 \tag{13}$$

et désignons par H_α l'ensemble des nombres $\beta \in \mathbf{Q}_\infty^*$ représentés par cette forme. Si $\alpha > 0$, i. e. $\alpha \in \mathbf{Q}_\infty^{*2}$, alors la forme (13) représente tous les nombres réels et par suite $\mathrm{H}_\alpha = \mathbf{Q}_\infty^*$. Si maintenant $\alpha < 0$, i. e. α n'est pas un carré, la forme (13) représente seulement les nombres positifs et par suite, comme dans le théorème 6, § 6, nous avons :

$$(\mathbf{Q}_\infty^* : \mathrm{H}_\alpha) = 2. \tag{14}$$

Il en résulte que si pour α, $\beta \in \mathbf{Q}_\infty^*$ on pose $(\alpha, \beta) = \pm 1$ suivant que la forme (13) représente ou non le nombre β, alors le symbole (α, β) possède les propriétés (9) à (13) du § 6.

Le théorème 7, § 6 qui permet le calcul du symbole de Hilbert dans le corps $\mathbf{Q}_p$ se réduit ici à

$$\left.\begin{array}{llllll} (\alpha, \beta) = +1 & \text{si} & \alpha > 0 & \text{ou} & \beta > 0 \\ (\alpha, \beta) = -1 & \text{si} & \alpha < 0 & \text{et} & \beta < 0 \end{array}\right\} \tag{15}$$

Pour des nombres rationnels a, b nous désignerons par $\left(\frac{a, b}{\infty}\right)$ la valeur du symbole (a, b) dans le corps $\mathbf{Q}_\infty$.

En utilisant le symbole $\left(\frac{a, b}{p}\right)$, nous pouvons maintenant énoncer le théorème 1 pour les formes de 3 variables sous la forme suivante :

La forme $ax^2 + by^2 - z^2$, a, b étant des rationnels différents de zéro, représente zéro dans le corps des nombres rationnels si et seulement si, pour tout p (y compris $p = \infty$) l'égalité

$$\left(\frac{a, b}{p}\right) = 1 \tag{16}$$

est satisfaite

Pour tous les rationnels a et b différents de zéro, le symbole $\left(\frac{a, b}{p}\right)$ est di
rent de $+1$ seulement pour un nombre fini de valeurs de p. En effet,
$p \neq 2, \infty$ et si p ne figure pas dans la décomposition de a et b (cela sign
que a et b sont des unités p-adiques), alors, d'après le corollaire 2 du th
rème 3, § 6, la forme (11) représente zéro dans $\mathbf{Q}_p$ et, par suite, pour tou
ces valeurs de p, $\left(\frac{a, b}{p}\right) = 1$. Par ailleurs, les valeurs du symbole $\left(\frac{a,}{p}\right.$
pour a, b fixés satisfont à d'autres conditions. Ainsi, le nombre des valeur
(y compris $p = \infty$) pour lesquels $\left(\frac{a, b}{p}\right) = -1$ est toujours pair. On pe
aussi exprimer ce résultat sous la forme suivante :

$$\prod_p \left(\frac{a, b}{p}\right) = 1 \qquad (1$$

où p parcourt tous les nombres premiers et le symbole ∞. En effet, le pr
duit formel infini ci-dessus contient seulement un nombre fini de facte
différents de $+1$ et le fait que ce produit est égal à 1 est équivalent à la par
du nombre des p tels que $\left(\frac{a, b}{p}\right) = -1$.

Démontrons (17). Représentant a et b comme produit de puissances
nombres premiers et utilisant les formules (9) à (13) du § 6 (également vé
fiées pour $p = \infty$), il est facile de démontrer la formule (17) dans les c
particuliers suivants :

1) $a = -1, \quad b = -1$
2) $a = q \quad b = -1 \quad (q$ premier);
3) $a = q, \quad b = q' \quad (q$ et q' premiers, $q \neq q')$.

D'après le théorème 7, § 6 et les formules (15), nous obtenons

$$\prod_p \left(\frac{-1, -1}{p}\right) = \left(\frac{-1, -1}{2}\right)\left(\frac{-1, -1}{\infty}\right) = (-1)\cdot(-1) = 1 ;$$

$$\prod_p \left(\frac{2, -1}{p}\right) = \left(\frac{2, -1}{2}\right)\left(\frac{2, -1}{\infty}\right) = 1\cdot 1 = 1 ;$$

$$\prod_p \left(\frac{q, -1}{p}\right) = \left(\frac{q, -1}{q}\right)\left(\frac{q, -1}{2}\right) = \left(\frac{-1}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{-1-1}{2}} = 1 ;$$

$$\prod_p \left(\frac{2, q}{p}\right) = \left(\frac{2, q}{q}\right)\left(\frac{2, q}{2}\right) = \left(\frac{2}{q}\right)(-1)^{\frac{q^2-1}{8}} = 1 ;$$

$$\prod_p \left(\frac{q, q'}{p}\right) = \left(\frac{q, q'}{q}\right)\left(\frac{q, q'}{q'}\right)\left(\frac{q, q'}{2}\right) = \left(\frac{q'}{q}\right)\left(\frac{q}{q'}\right)(-1)^{\frac{q'-1}{2}\cdot\frac{q-1}{2}} = 1.$$

Les nombres premiers q et q' dans ces formules sont impairs et distincts et cela démontre la formule (17).

Remarquons que, dans cette démonstration, nous avons utilisé la loi de réciprocité quadratique de Gauss. Il est facile de voir, d'autre part, à l'aide de l'expression explicite du symbole de Hilbert donnée dans le théorème 7, § 6, que l'on peut déduire de la formule (17) la loi de réciprocité. Ainsi la formule (17) est équivalente à la loi de réciprocité de Gauss.

Supposons maintenant que la forme (11) représente zéro dans tous les corps $\mathbf{Q}_p$ sauf peut-être dans le corps $\mathbf{Q}_q$. L'égalité (17) et les conditions $\left(\frac{a, b}{p}\right) = +1$ pour tout $p \neq q$ nous donnent alors que $\left(\frac{a, b}{p}\right) = 1$. En d'autres termes, on a démontré l'affirmation suivante.

LEMME 2. — *Si une forme quadratique rationnelle de 3 variables représente zéro dans tous les corps $\mathbf{Q}_p$ (p parcourt tous les nombres premiers et le symbole ∞) sauf peut-être dans le corps $\mathbf{Q}_q$, elle représente aussi zéro dans le corps $\mathbf{Q}_q$.*

3) Formes de 4 variables

Nous considérerons les formes

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \qquad (18)$$

où les a_i sont des entiers ne contenant pas de facteurs au carré. La forme étant non définie, il est clair que nous pouvons supposer $a_1 > 0$ et $a_4 < 0$. Nous considérerons en même temps que la forme (18) les formes

$$g = a_1x_1^2 + a_2x_2^2 \quad \text{et} \quad h = -a_3x_3^2 - a_4x_4^2.$$

L'idée de la démonstration du théorème de Minkowski-Hasse pour les formes de 4 variables est la suivante.

Utilisant le fait que la forme (18) représente zéro dans les corps $\mathbf{Q}_p$, nous montrerons qu'il existe un entier rationnel $a \neq 0$ représentable simultanément par les formes g et h dans les rationnels. Cela nous donne immédiatement une représentation rationnelle de zéro par la forme (18).

Soient $p_1, \ldots, p_s$ les diviseurs premiers impairs distincts des coefficients a_1, a_2, a_3, a_4. Pour tout p égal à un des $p_1, \ldots, p_s$ et pour $p = 2$ choisissons dans le corps $\mathbf{Q}_p$ une représentation de zéro

$$a_1\xi_1^2 + a_2\xi_2^2 + a_3\xi_3^2 + a_4\xi_4^2 = 0,$$

telle que tous les ξ_i soient différents de zéro (cf. appendice § 1, théorème 8) et posons

$$b_p = a_1\xi_1^2 + a_2\xi_2^2 = -a_3\xi_3^2 - a_4\xi_4^2.$$

Il est facile de voir qu'on peut choisir les ξ_i tels que $b_p \neq 0$, soit un nombre entier p-adique non divisible par p^2 (si $b_p = 0$, les formes g et h représentent zéro dans $\mathbf{Q}_p$ et d'après le théorème 5, § 1 de l'appendice, représentent tous les nombres de $\mathbf{Q}_p$). Considérons le système des congruences

$$\left.\begin{aligned} a &\equiv b_2 \pmod{16} \\ a &\equiv b_{p_1} \pmod{p_1^2} \\ &\vdots \\ a &\equiv b_{p_s} \pmod{p_s^2} \end{aligned}\right\} \qquad (19)$$

L'entier rationnel a satisfaisant à ces congruences est défini de manière unique modulo $m = 16p_1^2, \ldots, p_s^2$. Puisque b_{p_i} n'est pas divisible par p_i, alors $b_{p_i}a^{-1}$ est une unité p_i-adique et par suite $b_{p_i}a^{-1} \equiv 1 \pmod{p_i}$. D'après le corollaire 1 du théorème 1, § 6, le nombre $b_{p_i}a^{-1}$ est un carré dans le corps $\mathbf{Q}_{p_i}$. De la même manière, puisque b_2 n'est pas divisible par 2, alors $b_2a^{-1} \equiv 1 \pmod 8$ et par suite (théorème 2, § 6) b_2a^{-1} est un carré dans $\mathbf{Q}_2$.

Du fait que b_p et a ne diffèrent que par un carré, pour tout $p = 2, p_1, \ldots, p_s$ les formes

$$-ax_0^2 + g \quad \text{et} \quad -ax_0^2 + h \qquad (20)$$

représentent zéro dans $\mathbf{Q}_p$. Si a a été choisi > 0, alors, d'après les conditions $a_1 > 0$ et $-a_4 > 0$, les formes (20) représentent aussi zéro dans le corps des nombres réels. Si maintenant $p \neq 2, p_1, \ldots, p_s$ et ne figure pas dans a, i. e. si p impair ne divise pas les coefficients des formes (20), alors ces formes représentent zéro dans $\mathbf{Q}_p$ d'après le corollaire 2 du théorème 1, § 6. Supposons que le nombre a contient un seul facteur premier q différent des nombres $p_1, \ldots, p_s$ (on montrera ci-dessous que l'on peut toujours choisir a ainsi); nous pouvons alors appliquer le lemme 2 aux formes (20) et conclure (d'après le théorème de Minkowski-Hasse pour les formes à 3 variables) que les formes (20) représentent zéro dans le corps des nombres rationnels. Mais alors, nous obtiendrons pour le nombre a les représentations

$$a = a_1c_1^2 + a_2c_2^2, \qquad a = -a_3c_3^2 - a_4c_4^2,$$

les c_i étant rationnels, d'où

$$a_1c_1^2 + a_2c_2^2 + a_3c_3^2 + a_4c_4^2 = 0$$

et le théorème est démontré.

Montrons que l'on peut toujours trouver $a > 0$ satisfaisant aux congruences (19) et possédant la propriété remarquable utilisée ci-dessus. Nous appliquerons le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique (ce théorème sera démontré dans le chapitre V, § 3-2)). Ce théorème affirme que si la raison et le premier terme d'une progression arithmétique infinie sont premiers entre eux, alors cette progression contient une infinité de nombres premiers. Soit $a^* > 0$ une des valeurs de a satisfaisant aux congruences (19). Désignons par d le plus grand diviseur commun de a^* et m. Puisque $\frac{a^*}{d}$ et $\frac{m}{d}$ sont premiers entre eux, il existe, d'après le théorème de Dirichlet, un nombre $k \geqslant 0$ tel que $\frac{a^*}{d} + k\frac{m}{d} = q$ soit premier. Nous prendrons alors pour a le nombre

$$a = a^* + km = dq.$$

Puisque d contient certains des nombres premiers 2, $p_1, \ldots, p_s$, alors ce choix de a permet de terminer la démonstration du théorème 1 pour les formes de 4 variables.

4) Les formes de 5 variables et plus

Soit une forme quadratique rationnelle non définie de 5 variables réduite à une somme de carrés

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 \qquad (21)$$

où tous les a_i sont entiers et sans carrés. Nous pouvons supposer $a_1 > 0$ et $a_5 < 0$. Posons

$$g = a_1x_1^2 + a_2x_2^2, \qquad h = a_3x_3^2 - a_4x_4^2 - a_5x_5^2.$$

En raisonnant comme dans le cas $n = 4$, nous déterminerons au moyen du théorème de Dirichlet un nombre entier rationnel $a > 0$ représentable par g et h dans le corps des nombres réels et dans tous les corps $\mathbf{Q}_p$ sauf peut-être dans le corps $\mathbf{Q}_q$, q étant un nombre premier impair ne figurant pas dans les coefficients a_i. Mais alors g et h représentent a aussi dans le corps $\mathbf{Q}_q$. Pour la forme g, cela s'établit de même que plus haut à l'aide du lemme 2. Pour la forme h, elle représente zéro dans $\mathbf{Q}_q$ (corollaire 2 du théorème 3, § 6) et par suite représente tous les nombres q-adiques (cf. appendice, § 1, théorème 5). D'après le corollaire du théorème de Minkowski-Hasse (cf. fin de 1), qui a été déjà été démontré pour 3 et 4 variables, nous obtenons que les formes g et h représentent a également dans le corps des nombres rationnels, d'où, comme ci-dessus, résulte facilement que la forme (21) représente rationnellement zéro.

Pour démontrer le théorème 1 dans le cas $n > 5$, il suffit de remarqu
que toute forme quadratique rationnelle non définie f réduite à une som
de carrés peut se représenter sous la forme $f = f_0 + f_1$, où f_0 est une for
non définie de 5 variables. D'après ce qui précède la forme f_0 et par su
la forme f représentent zéro dans le corps des nombres rationnels. Le th
rème de Minkowski-Hasse est complètement démontré.

5) Équivalence rationnelle

Le théorème de Minkowski-Hasse permet de résoudre l'importante qu
tion de l'équivalence des formes quadratiques rationnelles.

THÉORÈME 2. — *Pour que deux formes quadratiques non singulières à coe
cients rationnels soient équivalentes sur le corps des nombres rationnels,
faut et il suffit qu'elles soient équivalentes sur le corps des nombres réels
sur tous les corps $\mathbf{Q}_p$ de nombres p-adiques.*

DÉMONSTRATION. — La nécessité est triviale. La suffisance se démon
par récurrence sur le nombre n de variables. Soit $n = 1$. L'équivalen
des formes ax^2 et bx^2 sur un corps signifie que $\frac{a}{b}$ est un carré dans ce cor
Mais si $\frac{a}{b}$ est un carré dans le corps des nombres réels et dans tous
corps $\mathbf{Q}_p$, alors, comme nous l'avons vu dans 1), $\frac{a}{b}$ est également un ca
dans le corps $\mathbf{Q}$ des nombres rationnels. Ainsi le théorème 2 est démon
pour $n = 1$.

Soit maintenant $n > 1$. Choisissons un nombre rationnel $a \neq 0$ repré
table par la forme f (sur le corps $\mathbf{Q}$). Puisque des formes équivalentes rep
sentent les mêmes nombres, alors la forme g représente a dans le corps d
nombres réels et dans tous les corps $\mathbf{Q}_p$. Mais alors, d'après le corolla
du théorème de Minkowski-Hasse, la forme g représente également a da
le corps $\mathbf{Q}$. En utilisant le théorème 2, § 1 de l'appendice, nous conclu
alors que $f \sim ax^2 + f_1$, $g \sim ax^2 + g_1$, où f_1 et g_1 sont des formes quadr
tiques de $(n-1)$ variables sur le corps $\mathbf{Q}$ (le signe $\sim$ signifie ici équiv
lence sur $\mathbf{Q}$). De l'équivalence des formes $ax^2 + f_1$ et $ax^2 + g_1$ dans le corp
des nombres réels et dans les corps $\mathbf{Q}_p$, il résulte que les formes f_1 et g
sont également équivalentes dans tous ces corps (cf. appendice § 1, théo
rème 4). Par hypothèse de récurrence, f_1 et g_1 sont équivalentes sur le corps $\mathbf{Q}$
des nombres rationnels. Mais alors f et g sont aussi équivalentes sur $\mathbf{Q}$ et
le théorème 2 est démontré.

Comme exemple, étudions la question de l'équivalence des formes quadratiques binaires. Le discriminant $d(f)$ d'une forme rationnelle non singulière s'écrit de manière unique

$$d(f) = d_0(f)c^2$$

où $d_0(f)$ est un nombre entier sans carrés. D'après le théorème 1, § 1 de l'appendice, par le passage à une forme équivalente, la valeur $d_0(f)$ ne change pas et cela signifie que c'est un invariant de la classe des formes rationnellement équivalentes.

Soit a un nombre rationnel quelconque non nul représentable par une forme binaire non singulière f. Pour tout nombre premier p (y compris $p = \infty$), posons

$$e_p(f) = \left(\frac{a, -d(f)}{p}\right).$$

D'après le théorème 8, § 6 (qui est aussi vrai, c'est évident, pour le corps des nombres réels $\mathbf{Q}_\infty$), la valeur $e_p(f)$ ne dépend pas du choix de a. Par suite, c'est également un invariant de la forme f pour l'équivalence rationnelle des formes. Réunissant le théorème 2 au théorème 9 du § 6 (vrai aussi pour le corps $\mathbf{Q}_\infty$), nous obtenons le critère suivant d'équivalence rationnelle des formes quadratiques binaires.

THÉORÈME 3. — *Deux formes quadratiques binaires f et g sont rationnellement équivalentes si et seulement si*

$$d_0(f) = d_0(g), \qquad e_p(f) = e_p(g) \qquad \textit{pour tout } p.$$

Remarquons que si l'équivalence des formes est définie par le système infini des invariants $e_p(f)$, le nombre de ces invariants est en fait fini puisque $e_p(f) \neq +1$ seulement pour un nombre fini d'entiers p.

6) Remarques sur les formes de degré supérieur

On se propose ici d'étudier une extension éventuelle du théorème de Minkowski-Hasse à des formes d'autres degrés : est-il vrai qu'une forme rationnelle représente zéro dans le corps des nombres rationnels dès qu'elle représente zéro dans le corps réel et dans les corps $\mathbf{Q}_p$? Il est facile de construire des contre-exemples. Par exemple, si q, l, q', l' sont des nombres premiers distincts tels que $\left(\frac{l}{q}\right) = -1$, $\left(\frac{l'}{q'}\right) = -1$ et si la forme $x^2 + qy^2 - lz^2$ représente zéro dans le corps des nombres 2-adiques, alors la forme de degré 4

$$(x^2 + qy^2 - lz^2)(x^2 + q'y^2 - l'z^2) \tag{22}$$

représentera zéro dans tous les corps $\mathbf{Q}_p$ et dans le corps des nombres r
mais ne représentera pas zéro dans le corps des nombres rationnels. En
dans le corps $\mathbf{Q}_2$, le premier facteur représente zéro par hypothèse.
impair est différent de q et l, alors le premier facteur représente zéro da
corps $\mathbf{Q}_p$ d'après le corollaire 2 du théorème 3, § 6. Dans ces corp
et $\mathbf{Q}_l$, le deuxième facteur représente zéro pour la même raison. Pou
aucun de ces facteurs ne représente zéro dans R puisque le premier f
ne représente pas zéro dans R_q et la deuxième dans $R_{q'}$ $\left(\text{puisque } \left(\frac{l}{q}\right)=\right.$
et $\left.\left(\frac{l'}{q'}\right) = -1\right)$. Comme exemple numérique on a la forme

$$(x^2 + 3y^2 - 17z^2)(x^2 + 5y^2 - 7z^2).$$

Cet exemple peut sembler peu convaincant car la forme (22) est d
posée et on pourrait croire que c'est ce qui explique ce phénomène. S
a donné un exemple encore plus simple sans ce handicap (E. S. S
The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 1951
n° 3-4, 203-362). Il a montré en particulier que la forme $3x^3 + 4y^3$
représente zéro dans tout corps $\mathbf{Q}_p$ de nombres p-adiques et dans le
des réels mais ne représente pas zéro dans le corps des nombres ratio
Le fait que cette forme représente zéro dans tous les corps $\mathbf{Q}_p$ est fa
démontrer (exercice 8, § 5). La non-représentabilité de zéro dans le
des nombres rationnels est de démonstration plus délicate (cf. exerci
§ 7, chap. 3).

L'analogue du théorème de Minkowski-Hasse pour des formes de d
supérieur n'est pas vrai même dans le cas où le nombre de variable
grand. Par exemple, la forme

$$(x_1^2 + \ldots + x_n^2)^2 - 2(y_1^2 + \ldots + y_n^2)^2$$

pour $n \geqslant 5$ représente zéro à la fois dans le corps des nombres réels et
les corps p-adiques mais ne représente zéro dans le corps des nombres rat
nels pour aucune valeur de n. On a le même résultat pour la forme

$$3(x_1^2 + \ldots + x_n^2)^3 + 4(y_1^2 + \ldots + y_n^2)^3 - 5(z_1^2 + \ldots + z_n^2)^3,$$

qui, elle, est absolument irréductible.

Dans les exemples ci-dessus, les formes introduites sont de degré p
On ne connaît pas encore actuellement d'exemples de formes de de
impair possédant ces propriétés. On a donc émis la conjecture que l'analo
du théorème de Minkowski-Hasse est vrai pour les formes de degré imp
d'un nombre assez grand de variables. Rappelons le théorème de Brauer
les formes d'un nombre suffisamment grand de variables représentent zé

dans tous les corps de nombres p-adiques (nous avons déjà énoncé ce théorème au § 6-5)); nous arrivons donc à la conjecture suivante :

Une forme rationnelle de degré impair et d'un nombre suffisamment grand de variables représente rationnellement zéro.

C'est à Artin que l'on doit la forme la plus précise de cette conjecture : une forme rationnelle de degré r impair à n variables représente zéro dans le corps des nombres rationnels si $n > r^2$.

Les exemples connus jusqu'à présent, de formes de degré pair, infirmant la conjecture d'Artin sont toutes obtenues par le même procédé, la substitution d'une forme dans un autre. Il est possible que la conjecture d'Artin soit vraie également pour les formes de degré pair en excluant les formes de ce type et les produits de ces formes.

L'unique résultat général vers la conjecture d'Artin est dû à Birch (B. J. Birch, Homogeneous forms of odd degree in a large number of variables. *Mathematika*, 1957, **4**, n° 8, 102-105), qui a démontré qu'une forme de degré impair représente zéro dans le corps des nombres rationnels si le nombre de ses variables est suffisamment grand par rapport à son degré. La conjecture d'Artin n'est encore démontrée pour aucune valeur de r (sauf $r = 2$). Le cas le plus simple est relatif à $r = 3$ et affirme qu'une forme cubique de 10 variables représente zéro dans le corps des nombres rationnels.

EXERCICES

1. Démontrer le théorème suivant, dû à Legendre : si a, b, c sont des entiers rationnels premiers deux à deux, sans carrés et non tous de même signe, alors l'équation

$$ax^2 + by^2 + cz^2 = 0$$

admet une solution non nulle dans les nombres rationnels si et seulement si les trois congruences ci-dessous sont résolubles :

$$x^2 \equiv -bc \pmod{a};$$
$$x^2 \equiv -ca \pmod{b};$$
$$x^2 \equiv -ab \pmod{c}.$$

2. Les formes $3x^2 + 5y^2 - 7z^2$ et $3x^2 - 5y^2 - 7z^2$ représentent-elles zéro dans le corps des nombres rationnels ?

3. Quels sont les nombres premiers rationnels représentés par les formes $x^2 + y^2$, $x^2 + 5y^2$, $x^2 - 5y^2$?

4. Donner une description de tous les nombres rationnels qui sont représentables par la forme $2x^2 - 5y^2$.

5. Quels sont les nombres rationnels qui sont représentés par la forme

$$2x^2 - 6y^2 + 15z^2 ?$$

6. Soit f une forme quadratique non singulière sur le corps des nombres rat nels, dont le nombre de variables n'est pas égal à 4. Montrer que f représente les nombres rationnels si et seulement si elle représente zéro.

7. Pour quels entiers rationnels à la forme $x^2 + 2y^2 - az^2$ représente-t-elle dans le corps des nombres rationnels ?

8. Trouver toutes les solutions rationnelles de l'équation $x^2 + y^2 - 2z^2 =$

9. On considère les formes

$$x^2 - 2y^2 + 5z^2, \qquad x^2 - y^2 + 10z^2, \qquad 3x^2 - y^2 + 30z^2;$$

quelles sont celles qui sont équivalentes entre elles sur le corps des nor rationnels ?

10. Supposons que la forme $ax^2 + by^2 - z^2$, où a et b sont des entiers ratio sans carré et $|a| > |b|$, représente zéro dans tous les corps de nombres p-adi Montrer qu'il existe alors des entiers rationnels a_1 et c tels que

$$aa_1 = c^2 - b, \qquad |a_1| < |a|$$

(l'égalité $aa_1 + b - c^2 = 0$ montre que la forme $aa_1x^2 + by^2 - z^2$ représente rationnellement).

11. Considérant les formes du type $ax^2 + by^2 - z^2$, où a et b sont des e sans carrés, démontrer le théorème de Minkowski-Hasse pour trois variable récurrence sur le nombre $m = \max(|a|, |b|)$ (utiliser l'exercice 10 et l'exer du § 1 de l'appendice).

CHAPITRE II

REPRÉSENTATION DES NOMBRES RATIONNELS PAR DES FORMES DÉCOMPOSABLES

Nous avons étudié dans le chapitre précédent l'existence et la recherche des solutions rationnelles des équations. Ce chapitre est consacré à l'étude des solutions en nombres entiers. Nous commencerons par l'étude d'un exemple simple.

Considérons le problème de la recherche de toutes les solutions en nombres entiers de l'équation

$$x^2 - 2y^2 = 7. \tag{1}$$

Nous nous limiterons aux solutions $x > 0$, $y > 0$ (les autres s'obtiennent par changement de signe). L'équation admet les solutions (3,1) et (5,3). On peut obtenir à partir de ces deux solutions une infinité d'autres solutions, en effectuant la remarque suivante : si (x, y) est une solution de l'équation (1), alors, comme on le vérifie facilement $(3x + 4y, 2x + 3y)$ est encore une solution. Partant de la solution $(x_0, y_0) = (3, 1)$, nous obtenons ainsi une suite infinie (x_n, y_n) de solutions définies par les formules de récurrence

$$\begin{cases} x_{n+1} = 3x_n + 4y_n \\ y_{n+1} = 2x_n + 3y_n. \end{cases} \tag{2}$$

Partant de la solution $(x'_0, y'_0) = (5,3)$ nous obtenons par les mêmes formules une autre suite infinie (x'_n, y'_n) de solutions. On peut démontrer que ces deux suites épuisent toutes les solutions (x, y) de l'équation (1) telles que

$$x > 0, \qquad y > 0.$$

Cette résolution élémentaire de l'équation (1) repose sur des formules et des calculs. Nous pouvons la relier à des notions plus générales et préparer ainsi le terrain pour des généralisations ultérieures.

Remarquons que la forme $x^2 - 2y^2$ est irréductible sur le corps $\mathbf{Q}$ des nombres rationnels mais se décompose en facteurs linéaires $(x + y\sqrt{2})$

Mais si $\omega \equiv a \pmod{\mathfrak{L}}$, alors $\omega^l \equiv a^l \pmod{l\mathfrak{L}}$, ce qui entraîne que l'unité ε_0 est congrue modulo $\mathfrak{L}^l$ à un nombre entier rationnel. D'après le lemme de Kummer (théorème 3 du § 6; nous utilisons à nouveau la régularité du nombre l), l'unité ε_0 est une puissance $l^{\text{ième}}$ dans $\mathbf{Q}(\zeta)$, i. e. $\varepsilon_0 = \eta^l$ où η est aussi une unité du corps $\mathbf{Q}(\zeta)$. L'égalité (10) s'écrit alors

$$\alpha^l + (\eta\beta)^l = \varepsilon'(1-\zeta)^{l(m-1)}\gamma^l.$$

Nous avons obtenu une égalité du type (2), à cette différence près que l'exposant m est remplacé par $m-1$. Mais c'est impossible, puisque m a été choisi le plus petit possible. La contradiction obtenue montre que l'équation (1) n'a pas de solution en nombres entiers non nuls x, y et z dont l'un est divisible par l, i. e. le deuxième cas du théorème de Fermat est démontré pour un exposant l régulier.

2) Infinité de l'ensemble des nombres premiers irréguliers

Dans les limites des tables, la quantité des nombres premiers réguliers est supérieure à la quantité des nombres irréguliers. Pourtant, on ne sait pas si c'est toujours vrai pour l'intervalle (1, N). En fait, jusqu'à présent, on ignore même s'il existe une infinité de nombres réguliers. Le théorème suivant est lié à ces questions.

THÉORÈME 2. — *Il existe une infinité de nombres premiers irréguliers.*

La démonstration du théorème 2 s'appuie sur certaines propriétés des nombres de Bernoulli. Ces propriétés seront formulées et démontrées dans le paragraphe suivant.

Soit $p_1, \ldots, p_s$ un système fini quelconque de nombres premiers irréguliers. Le théorème 2 sera démontré si nous pouvons trouver un nombre premier irrégulier p différent de $p_1, \ldots, p_s$. Posons

$$n = r(p_1 - 1) \ldots (p_s - 1).$$

Puisque pour le nombre de Bernoulli B_{2k} on a

$$\left|\frac{B_{2k}}{2k}\right| \to \infty \qquad \text{pour} \qquad k \to \infty,$$

(cf. fin du § 8), si l'entier rationnel r est assez grand, le nombre rationnel $\frac{B_n}{n}$ sera supérieur à 1 en valeur absolue. Soit p un nombre premier figurant dans le numérateur (pour une écriture irréductible). Si $(p-1)|n$, alors, d'après le théorème 4 du § 8, le nombre p figure dans le dénominateur de B_n, ce qui n'est pas, d'après le choix de p. Ainsi $(p-1) \nmid n$ et p est donc différent de $p_1, \ldots, p_s$ (et différent de 2). Désignons par m le reste de la division de n par $p-1$, i. e. $n = m + a(p-1)$. Il est clair que m est pair et

$$2 \leqslant m \leqslant p-3.$$

De plus, simultanément avec n, le nombre m n'est pas divisible par $p-1$. Utilisant maintenant la congruence dite de Kummer (théorème 5 du § 8), nous obtenons dans l'anneau des nombres rationnels p-entiers la congruence

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

Mais $\frac{B_n}{n} \equiv 0 \pmod{p}$, d'où $\frac{B_m}{m} \equiv 0 \pmod{p}$ et $B_m \equiv 0 \pmod{p}$. Puisque m est égal ici à l'un des nombres 2, 4, ..., $p-3$, alors, d'après le corollaire du théorème 2 du § 6, le nombre p est irrégulier. Le théorème 2 est démontré.

EXERCICES

1. Démontrer que l'équation $x^3 + y^3 = 5z^3$ a pour unique solution $x=y=z=0$ dans les nombres entiers rationnels.

2. Démontrer qu'il existe une infinité de nombres premiers irréguliers de la forme $4n+3$ (utiliser les exercices 9 et 10 du § 8).

§ 8. — LES NOMBRES DE BERNOULLI

Nous démontrerons ici les propriétés des nombres de Bernoulli qui ont été utilisées dans les paragraphes précédents.

Toutes les séries entières considérées ci-dessous convergent dans un certain voisinage de l'origine des coordonnées et il est facile de déterminer leur rayon de convergence. Nous ne nous intéresserons pourtant pas à ces questions de convergence puisqu'il suffit pour notre propos de considérer ces séries formellement (à l'exclusion de la démonstration du théorème 6).

DÉFINITION. — *Les nombres rationnels* B_m $(m \geqslant 1)$ *définis par le développement en série*

$$\frac{t}{e^t - 1} = 1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t_m, \tag{1}$$

sont appelés nombres de Bernoulli.

Nous utiliserons les notations abrégées suivantes. Si

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

est un polynôme, nous désignerons par $f(\mathrm{B})$ le nombre

$$a_0 + a_1\mathrm{B}_1 + \ldots + a_n\mathrm{B}_n.$$

De manière analogue, si $f(x, t)$ est une série entière de la forme $\sum_{n=0}^{\infty} f_n(x)t^n$, où $f_n(x)$ est un polynôme, nous désignerons par $f(\mathrm{B}, t)$ la série

$$\sum_{n=0}^{\infty} f_n(\mathrm{B})t^n.$$

Ainsi par exemple, on peut écrire la série (1) définissant les nombres de Bernoulli sous la forme

$$\frac{t}{e^t - 1} = e^{\mathrm{B}t}.$$

Il est facile de voir que pour tout nombre a on a

$$e^{at}e^{\mathrm{B}t} = e^{(a+\mathrm{B})t}$$

(la démonstration s'effectue en multipliant terme à terme les séries de gauche).

THÉORÈME 1. — *Les nombres de Bernoulli vérifient la relation de récurrence*

$$(1 + \mathrm{B})^m - \mathrm{B}^m = 0 \quad \text{pour} \quad m \geqslant 2, \tag{2}$$

qui sous forme développée s'écrit

$$1 + \sum_{k=1}^{m-1} \mathrm{C}_m^k \mathrm{B}_k = 0 \qquad (m \geqslant 2).$$

Pour la démonstration, écrivons l'égalité (1) sous la forme

$$t = e^{(1+\mathrm{B})t} - e^{\mathrm{B}t}.$$

Égalant les coefficients des termes $\frac{t^m}{m!}$ $(m \geqslant 2)$, nous obtenons la relation (2). Pour $m = 2$, la formule (2) donne $1 + 2\mathrm{B}_1 = 0$, d'où

$$\mathrm{B}_1 = -\frac{1}{2}.$$

THÉORÈME 2. — *A l'exception de* B_1, *tous les nombres de Bernoulli d'indices impairs sont nuls* :

$$\mathrm{B}_{2m+1} = 0 \quad \text{pour} \quad m \geqslant 1. \tag{3}$$

Les égalités (3) équivalent au fait que la fonction

$$\frac{t}{e^t - 1} + \frac{t}{2} = 1 + \sum_{m=2}^{\infty} \frac{\mathrm{B}_m}{m!} t^m$$

est paire, ce qui est facile à vérifier.

Donnons les valeurs des douze premiers nombres de Bernoulli d'indices pairs :

$$\mathrm{B}_2 = \frac{1}{6}, \quad \mathrm{B}_4 = -\frac{1}{30}, \quad \mathrm{B}_6 = \frac{1}{42}, \quad \mathrm{B}_8 = -\frac{1}{30}, \quad \mathrm{B}_{10} = \frac{5}{66},$$

$$\mathrm{B}_{12} = -\frac{691}{2730}, \quad \mathrm{B}_{14} = \frac{7}{6}, \quad \mathrm{B}_{16} = -\frac{3\ 617}{510}, \quad \mathrm{B}_{18} = \frac{43\ 867}{798},$$

$$\mathrm{B}_{20} = -\frac{174\ 611}{330}, \quad \mathrm{B}_{22} = \frac{854\ 513}{138}, \quad \mathrm{B}_{24} = -\frac{236\ 364\ 091}{2730}.$$

Les nombres de Bernoulli sont liés aux sommes des puissances des nombres entiers naturels. Posons

$$\mathrm{S}_k(n) = 1^k + 2^k + \ldots + (n-1)^k.$$

THÉORÈME 3. — *Les sommes* $\mathrm{S}_k(n)$ *vérifient la formule*

$$(m+1)\mathrm{S}_m(n) = (n + \mathrm{B})^{m+1} - \mathrm{B}^{m+1}, \qquad m \geqslant 1 \tag{4}$$

ou, sous forme développée,

$$(m+1)\mathrm{S}_m(n) = \sum_{k=0}^{m} \mathrm{C}_{m+1}^k \mathrm{B}_k n^{m+1-k}, \qquad m \geqslant 1 \ (\mathrm{B}_0 = 1). \tag{5}$$

En effet, l'expression de droite dans l'égalité (4) est égale au coefficient de $\frac{t^{m+1}}{(m+1)!}$ dans la série $e^{(n+\mathrm{B})t} - e^{\mathrm{B}t}$. Par ailleurs

$$e^{(n+\mathrm{B})t} - e^{\mathrm{B}t} = e^{\mathrm{B}t}(e^{nt} - 1) = t\frac{e^{nt} - 1}{e^t - 1} = t\sum_{r=}^{n-1} e^{rt}$$

$$= nt + \sum_{m=1}^{\infty}\left(\sum_{r=1}^{n-1} r^m\right)\frac{t^{m+1}}{m!} = nt + \sum_{m=1}^{\infty}\frac{(m+1)\mathrm{S}_m(n)t^{m+1}}{(m+1)!},$$

ce qui démontre la formule (4).

Remarquons que, pour $n = 1$, la formule (4) coïncide avec (2).

THÉORÈME 4 (théorème de von Staudt). — *Soient p un nombre premier et m un nombre pair. Si* $(p-1) \nmid m$, *alors* B_m *est p-entier* (i. e. B_m *ne contient*

pas p en dénominateur). Si maintenant $(p-1)\,|\,m$, *alors* pB_m *est un nombre p-entier et*

$$pB_m \equiv -1 \pmod{p}.$$

Nous démontrerons le théorème 4 par récurrence sur m en utilisant la relation

$$(m+1)S_m(p) = (m+1)B_m p + \sum_{k=0}^{m-1} C_{m+1}^k B_k p^{m+1-k},$$

obtenue à partir de (5) en remplaçant n par p. Écrivons-la sous la forme

$$pB_m = S_m(p) - \sum_{k=0}^{m-1} \frac{1}{m+1} C_{m+1}^k p^{m-k} pB_k \tag{6}$$

et démontrons que tous les nombres qui figurent dans la somme sont des nombres p-entiers et sont divisibles par p (dans l'anneau des nombres p-entiers).

Le facteur pB_k pour $k < m$ est p-entier par hypothèse de récurrence. Étudions le nombre

$$\frac{1}{m+1} C_{m+1}^k p^{m-k}. \tag{7}$$

Si $p = 2$, alors, puisque $m+1$ est impair, ce nombre est 2-entier et divisible par 2 (puisque $k < m$). Pour $p \neq 2$, écrivons le nombre (7) sous la forme

$$\frac{1}{m+1} C_{m+1}^{m+1-k} p^{m-k} = \frac{m(m-1)\dots(k+1)}{(m-k+1)!} p^{m-k}.$$

Le nombre p figure dans $(m-k+1)! = r!$ avec l'exposant

$$\left[\frac{r}{p}\right] + \left[\frac{r}{p^2}\right] + \dots < \frac{r}{p} + \frac{r}{p^2} + \dots = \frac{r}{p-1} \leqslant \frac{r}{2} \leqslant r-1 = m-k,$$

et par suite $\dfrac{1}{(m-k+1)!} p^{m-k}$ est un nombre p-entier divisible par p.

On a ainsi démontré que pB_m est p-entier et que

$$pB_m \equiv S_m(p) \pmod{p} \tag{8}$$

dans l'anneau des nombres p-entiers

D'autre part, on a les congruences

$$S_m(p) \equiv -1 \pmod{p} \quad \text{si} \quad (p-1)\,|\,m; \tag{9}$$

$$S_m(p) \equiv 0 \pmod{p} \quad \text{si} \quad (p-1) \nmid m. \tag{10}$$

En effet, si $(p-1)\,|\,m$, alors $x^m \equiv 1 \pmod{p}$ pour $1 \leqslant x \leqslant p-1$, d'où

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{x=1}^{p-1} 1 = p-1 \equiv -1 \pmod{p}.$$

Si maintenant $(p-1) \nmid m$, soit g une racine primitive modulo p; nous aurons

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{r=0}^{p-2} g^{mr} = \frac{g^{(p-1)m}-1}{g^m-1} \equiv 0 \pmod{p},$$

puisque $g^{p-1} \equiv 1 \pmod{p}$ et $g^m \not\equiv 1 \pmod{p}$.

Réunissant (8) et (10), nous obtenons que, si $(p-1) \nmid m$, alors $pB_m \equiv 0 \pmod{p}$, i. e. B_m est p-entier. Le deuxième argument du théorème 4 résulte des congruences (8) et (9).

Dans le cas $m \leqslant p-1$, le nombre $p-1$ ne divise aucun des nombres $k < m$ et par suite tous les B_k pour $k < m$ sont p-entiers et par suite tous les termes qui figurent dans la somme de droite de l'égalité (6) sont divisible par p^2. On a donc le résultat suivant.

COROLLAIRE. — Si $p \neq 2$ et $m \leqslant p-1$ (m pair), *alors*

$$pB_m \equiv S_m(p) \pmod{p^2}. \tag{11}$$

THÉORÈME 5 (congruence de Kummer). — *Si p est premier et* $(p-1) \nmid m$ *(m est pair positif), alors le nombre* $\dfrac{B_m}{m}$ *est un nombre p-entier et on a la congruence*

$$\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \pmod{p}. \tag{12}$$

Autrement dit, les quotients $\dfrac{B_m}{m}$ (pour $(p-1) \nmid m$) sont périodiques modulo p, de période $p-1$.

DÉMONSTRATION. — Considérons la fonction

$$F(t) = \frac{gt}{e^{gt}-1} - \frac{t}{e^t-1} = \sum_{m=1}^{\infty} \frac{B_m(g^m-1)}{m!} t^m, \tag{13}$$

où g est une racine primitive modulo p, $1 < g < p$. Posons $e^t - 1 = u$. Alors

$$F(t) = \frac{gt}{(1+u)^g - 1} - \frac{t}{u} = tG(u),$$

où

$$G(u) = \frac{g}{(1+u)^g - 1} - \frac{1}{u} = \frac{g}{gu + \ldots + u^g} - \frac{1}{u} = \sum_{k=0}^{\infty} c_k u^k.$$

Il est clair que ces nombres c_k sont p-entiers.

Démontrons que, dans le développement de la fonction $G(u)$ suivant les puissances de t :

$$G(u) = G(e^t - 1) = \sum_{k=0}^{\infty} c_k (e^t - 1)^k = \sum_{m=0}^{\infty} \frac{A_m}{m!} t^m, \tag{14}$$

tous les coefficients A_m sont p-entiers et de période $p - 1$ modulo p (pour $m > 0$). Il est clair que si cette dernière propriété est satisfaite pour certaines séries elle l'est aussi pour toute combinaison linéaire à coefficients p-entiers. Il nous suffit donc de le vérifier pour les fonctions $(e^t - 1)^k$. Mais ces fonctions, à leur tour, sont des combinaisons linéaires des fonctions e^{rt} pour des entiers $r \geqslant 0$. Mais

$$e^{rt} = \sum_{n=0}^{\infty} \frac{r^n}{n!} t^n$$

et, d'après le petit théorème de Fermat,

$$r^{n+p-1} \equiv r^n \pmod{p} \qquad \text{pour} \qquad n > 0 ;$$

par suite, les fonctions e^{rt} possèdent la propriété demandée et notre argument sur les coefficients A_m est démontré.

Égalant maintenant les coefficients correspondants dans (13) et (14), nous obtenons

$$\frac{B_m(g^m - 1)}{m!} = \frac{A_{m-1}}{(m-1)!},$$

d'où

$$\frac{B_m}{m}(g^m - 1) = A_{m-1}.$$

Puisque $g^m - 1 \not\equiv 0 \pmod{p}$ pour $(p-1) \nmid m$ et que la suite des nombres $g^m - 1$ possède, d'après le petit théorème de Fermat, la période $p - 1$ modulo p, alors, d'après la propriété démontrée des nombres A_m, les nombres $\frac{B_m}{m}$ pour $(p - 1) \nmid m$ sont p-entiers et de période $p - 1$ modulo p. Le théorème 5 est démontré.

THÉORÈME 6. — *Les nombres de Bernoulli* B_{2m} *vérifient la formule*

$$B_{2m} = (-1)^{m-1} \frac{2(2m)!}{(2\pi)^{2m}} \zeta(2m), \tag{15}$$

où $\zeta(2m)$ *est la valeur de la fonction zêta de Riemann* $\zeta(s)$ *pour* $s = 2m$.

Pour la démonstration, nous utiliserons la décomposition de $\frac{1}{e^t - 1}$ en série de fractions rationnelles :

$$\frac{t}{e^t - 1} = -\frac{1}{2} + \sum_{n=-\infty}^{+\infty} \frac{1}{t - 2\pi i n} = -\frac{1}{2} + \frac{1}{t} + \sum_{n=1}^{\infty} \frac{2t}{t^2 + (2\pi n)^2}. \tag{16}$$

On peut déduire ce développement par exemple du développement classique suivant de la cotangente :

$$\operatorname{cotg} z = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - (\pi n)^2},$$

en utilisant le fait que

$$\operatorname{cotg} z = i \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = i + \frac{2i}{e^{2iz} - 1}.$$

Il résulte de (16) que

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2 \sum_{n=1}^{\infty} \frac{t^2}{t^2 + (2\pi n)^2},$$

et puisque

$$\frac{t^2}{t^2 + (2\pi n)^2} = \sum_{m=1}^{\infty} (-1)^{m-1} \left(\frac{t}{2\pi n}\right)^{2m},$$

alors

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2 \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} (-1)^{m-1} \frac{t^{2m}}{(2\pi n)^{2m}}$$

$$= 1 - \frac{t}{2} + \sum_{m=1}^{\infty} (-1)^{m-1} \frac{2\zeta(2m)}{(2\pi)^{2m}} t^{2m}.$$

Comparant cette égalité avec (1) et égalant les coefficients correspondants, nous obtenons l'égalité (15).

La formule (15) permet d'étudier la croissance de $|B_{2m}|$ quand l'indice croît. Puisque $\zeta(2m) > 1$ et $(2m)! > \left(\frac{2m}{e}\right)^{2m}$ (cela résulte de la formule bien connue de Stirling), alors

$$|B_{2m}| > 2\left(\frac{m}{\pi e}\right)^{2m}.$$

Nous obtenons en particulier que

$$\frac{|B_{2m}|}{2m} \to \infty \qquad \text{pour} \qquad m \to \infty.$$

EXERCICES

1. Démontrer que

$$(x + \mathrm{B})^m = (x - 1 - \mathrm{B})^m, \qquad m \geqslant 1.$$

2. Démontrer que

$$\left(\frac{1}{2} + \mathrm{B}\right)^m = \left(\frac{1}{2^{m-1}} - 1\right)\mathrm{B}_m.$$

3. Soit p un nombre premier, $p \neq 2$. Démontrer que

$$\sum_{x=1}^{\frac{p-1}{2}} x^{\frac{p-1}{2}} \equiv 2\left(\left(\frac{2}{p}\right) - 2\right)\mathrm{B}_{\frac{p+1}{2}} \pmod{p}.$$

4. Soit $p > 3$ un nombre premier de la forme $4k + 3$. Démontrer que le nombre h des classes de diviseurs du corps quadratique imaginaire $\mathbf{Q}(\sqrt{-p})$ satisfait à la congruence

$$h \equiv -2\mathrm{B}_{\frac{p+1}{2}} \pmod{p}.$$

5. Démontrer que, pour $p > 3$ premier,

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$$

6. Démontrer la formule

$$(kx + \mathrm{B})^m = k^{m-1} \sum_{s=0}^{k-1} \left(x + \frac{s}{k} + \mathrm{B}\right)^m$$

(k et m sont des entiers naturels).

7. La fonction tg x admet la décomposition

$$\operatorname{tg} x = \sum_{n=1}^{\infty} \mathrm{T}_n \frac{x^{2n-1}}{(2n-1)!}$$

où

$$\mathrm{T}_n = 2^{2n}(2^{2n} - 1)\frac{|\mathrm{B}_{2n}|}{2n}.$$

Démontrer que tous les coefficients T_n sont des entiers naturels.

8. Pour $m > 1$, démontrer

$$2\mathrm{B}_{2m} \equiv 1 \pmod{4}.$$

9. Soit q un nombre premier tel que $2q + 1$ ne soit pas premier (par exemple $q \equiv 1 \pmod 3$). Démontrer que le numérateur du nombre de Bernoulli B_{2q} contient (en écriture irréductible) un nombre premier de la forme $4n + 3$.

10. Soient $p_1, \ldots, p_s$ des nombres premiers supérieurs à 3,

$$\mathrm{M} = (p_1 - 1) \ldots (p_s - 1)$$

et q un entier naturel satisfaisant à la congruence $q \equiv 1 \pmod{\mathrm{M}}$. Démontrer qu'aucun des nombres premiers $p_1, \ldots, p_s$ ne figure dans le dénominateur de la fraction $\frac{\mathrm{B}_{2q}}{2q}$.

APPENDICE ALGÉBRIQUE

§ 1. — FORMES QUADRATIQUES SUR UN CORPS QUELCONQUE DE CARACTÉRISTIQUE DIFFÉRENTE DE 2

Nous exposerons dans ce paragraphe une série de résultats généraux sur les formes quadratiques sur un corps quelconque. Dans le cas de résultats bien connus, nous nous contenterons de les énoncer. K désignera, sauf précisions supplémentaires, un corps arbitraire dont la caractéristique est différente de 2. Pour toute matrice rectangulaire A on désignera par A′ la matrice transposée.

1) Équivalence des formes quadratiques

On appelle forme quadratique sur un corps K un polynôme homogène de degré 2 à coefficients dans K. Toute forme quadratique f peut s'écrire sous la forme

$$f = \sum_{i,j} a_{ij} x_i x_j$$

avec $a_{ij} = a_{ji}$. La matrice symétrique $\mathrm{A} = (a_{ij})$ s'appelle la matrice de la forme quadratique f. La forme quadratique est complètement déterminée par la donnée de sa matrice à la désignation des variables près. Le déterminant $d = \det \mathrm{A}$ s'appelle le *déterminant* de la forme quadratique ; si $d = 0$, la forme f est dite *singulière* et *non singulière* dans le cas contraire. Désignant par X la matrice colonne des variables $x_1, x_2, \ldots, x_n$, nous pouvons écrire ainsi la forme quadratique f :

$$f = \mathrm{X'AX}.$$

Supposons qu'à la place des variables $x_1, \ldots, x_n$ on introduise de nouvelles variables $y_1, \ldots, y_n$ par les formules

$$x_i = \sum_{j=1}^{n} c_{ij} y_i \qquad (1 \leqslant i \leqslant n,\ c_{ij} \in \mathrm{K}).$$

sous forme matricielle, cette transformation linéaire peut s'écrire sous la forme

$$X = CY,$$

où Y est la matrice colonne des variables $y_1, \ldots, y_n$ et C la matrice (c_{ij}). Remplaçant dans la forme quadratique f les variables $x_1, \ldots, x_n$ par leur expression en fonction de $y_1, \ldots, y_n$ nous obtenons (après avoir effectué toutes les opérations convenables) une nouvelle forme quadratique g (encore sur le corps K) des variables $y_1, \ldots, y_n$. La matrice A_1 de la forme quadratique g est

$$A_1 = C'AC. \qquad (1)$$

Deux formes quadratiques f et g sont dites *équivalentes* et on note $f \sim g$, s'il existe une transformation linéaire non singulière des variables par laquelle une des formes est transformée en l'autre (à la désignation des variables près). De la formule (1) résulte :

THÉORÈME. — *Si deux formes quadratiques sont équivalentes, alors leurs déterminants diffèrent l'un de l'autre par un facteur non nul qui est un carré dans* K.

Soit γ un élément quelconque de K. S'il existe dans K des éléments $\alpha_1, \ldots, \alpha_n$ tels que

$$f(\alpha_1, \ldots, \alpha_n) = \gamma,$$

on dit que la *forme quadratique f représente* γ. En d'autres termes, l'élément γ est représenté par la forme f s'il est la valeur de cette forme pour certaines valeurs des variables. On voit facilement que des formes quadratiques équivalentes représentent les mêmes éléments du corps K.

Nous dirons de plus que la *forme quadratique représente zéro dans le corps* K s'il existe des nombres de K non tous nuls $\alpha_i \in K$ $(1 \leqslant i \leqslant n)$ tels que $f(\alpha_1, \ldots, \alpha_n) = 0$. Il est clair que, pour une forme, la propriété de représenter zéro est conservée par passage à une forme équivalente.

THÉORÈME 2. — *Si une forme quadratique à n variables représente un élément* $\alpha \neq 0$, *elle est équivalente à une forme du type*

$$\alpha x_1^2 + g(x_2, \ldots, x_n)$$

où g est une forme quadratique à n — 1 variables.

Pour la démonstration de ce théorème, remarquons ce qui suit. Si

$$f(\alpha_1, \ldots, \alpha_n) = \alpha,$$

alors tous les α_i ne sont pas nuls; nous pouvons donc construire une matrice C non singulière dont la première ligne est constituée par les nombres $\alpha_1, \ldots, \alpha_n$.

Si maintenant nous effectuons sur les variables de la forme f la transformation linéaire de matrice C, nous obtenons une forme dont le coefficient du carré de la première variable est égal à α. On continue alors la démonstration comme d'habitude.

Si la matrice d'une forme quadratique est diagonale (tous les coefficients des produits de variables différents sont égaux à 0), nous dirons que cette forme est *diagonale*. Du théorème 2 résulte facilement.

THÉORÈME 3. — *Toute forme quadratique sur un corps* K *peut être mise sous forme diagonale par une transformation linéaire non singulière des variables.*

Autrement dit, toute forme quadratique est équivalente à une forme diagonale.

En termes matriciels, le théorème 3 signifie que pour toute matrice symétrique A il existe une matrice non singulière C telle que la matrice C'AC soit diagonale.

2) Somme directe de formes quadratiques

Puisque la désignation des variables est sans importance, nous pouvons considérer que deux formes quadratiques f et g n'ont pas de variable commune. La forme $f + g$ s'appelle alors *somme directe des formes f et g* et se désigne par $f \dotplus g$ (à ne pas confondre avec l'addition usuelle des formes quadratiques des mêmes variables). Il est évident que si $g \sim h$, alors $f \dotplus g \sim f \dotplus h$. Ce dernier fait admet une réciproque.

THÉORÈME 4 (théorème de Witt). — *Soient f, g, h des formes quadratiques non singulières sur un corps* K. *Si les formes* $f \dotplus g$ *et* $f \dotplus h$ *sont équivalentes, alors les formes g et h sont aussi équivalentes.*

DÉMONSTRATION. — Soit f_0 une forme diagonale équivalente à la forme f. Alors, comme on l'a remarqué ci-dessus, $f \dotplus g \sim f_0 \dotplus g$ et $f \dotplus h \sim f_0 \dotplus h$, d'où $f_0 \dotplus g \sim f_0 \dotplus h$. Ainsi, nous pouvons supposer que f est une forme diagonale. Il est clair maintenant qu'il suffit de considérer le cas $f = ax_0^2$, $a \neq 0$. Désignons par A et B les matrices respectives des formes g et h. Puisque les formes $ax_0^2 \dotplus g$ et $ax_0^2 \dotplus h$ sont équivalentes, il existe une matrice

$$C = \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix}$$

telle que

$$\begin{pmatrix} \gamma & T' \\ S' & Q' \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}$$

(ici S est une matrice ligne et T une matrice colonne). De cette égalité résulte

$$\gamma^2 a + T'AT = a \tag{2}$$

$$\gamma a S + T'AQ = 0 \tag{3}$$

$$S'aS + Q'AQ = B. \tag{4}$$

Il faut montrer qu'il existe une matrice C_0, non singulière, telle que

$$C_0'AC_0 = B.$$

Nous chercherons cette matrice sous la forme

$$C_0 = Q + \xi TS,$$

où ξ sera choisi de manière convenable. D'après (2) et (3), nous avons

$$\begin{aligned} C_0'AC_0 &= (Q' + \xi S'T')\,A(Q + \xi TS) \\ &= Q'AQ + \xi S'T'AQ + \xi Q'ATS + \xi^2 S'T'ATS \\ &= Q'AQ + a[(1 - \gamma^2)\xi^2 - 2\gamma\xi]S'S. \end{aligned}$$

D'après l'égalité (4), cette dernière expression sera égale à la matrice B si $(1 - \gamma^2)\xi^2 - 2\gamma\xi = 1$. L'équation en ξ obtenue peut s'écrire sous la forme $\xi^2 - (\gamma\xi + 1)^2 = 0$ et a donc une solution ξ_0 dans le corps K pour tout $\gamma \in K$ (la caractéristique de K n'est pas égale à 2). Ainsi, nous avons trouvé une matrice $C_0 = Q + \xi_0 TS$ telle que $C_0'AC_0 = B$. Puisque par hypothèse la matrice B est non singulière, il en est de même de C_0. Le théorème 4 est démontré.

3) Représentation des éléments du corps

THÉORÈME 5. — *Si une forme quadratique non singulière représente zéro dans le corps* K, *elle représente aussi tous les éléments de* K.

DÉMONSTRATION. — Puisque des formes équivalentes représentent les mêmes éléments du corps, il suffit de démontrer le théorème pour une forme diagonale $f = a_1\alpha_1^2 + \ldots + a_n x_n^2$. Soit $a_1x_1^2 + a_2\alpha_2^2 + \ldots + a_n\alpha_n^2 = 0$, une représentation non nulle de zéro et soit γ un élément quelconque du corps K. Nous pouvons supposer que $\alpha_1 \neq 0$. Donnons aux variables $x_1, \ldots, x_n$ les valeurs

$$x_1 = \alpha_1(1 + t), \qquad x_k = \alpha_k(1 - t) \qquad k = 1, 2, \ldots, n,$$

où t est une nouvelle variable et substituons ces valeurs dans la forme f; nous obtenons

$$f^* = f^*(t) = 2a_1\alpha_1^2 t - 2a_2\alpha_2^2 t - \ldots - 2a_n\alpha_n^2 t = 4a_1\alpha_1^2 t$$

Si nous posons maintenant $t = \dfrac{\gamma}{4a_1\alpha_1^2}$, nous obtenons $f^*(t) = \gamma$.

THÉORÈME 6. — *Une forme quadratique non singulière f représente un élément $\gamma \neq 0$ de* K *si et seulement si la forme $-\gamma x_0^2 + f$ représente zéro.*

DÉMONSTRATION. — La nécessité de la condition est évidente. Supposons

$$-\gamma\alpha_0^2 + f(\alpha_1, \ldots, \alpha_n) = 0,$$

tous les α_i n'étant pas nuls. Si $\alpha_0 \neq 0$, alors $\gamma = f\left(\dfrac{\alpha_1}{\alpha_0}, \ldots, \dfrac{\alpha_n}{\alpha_0}\right)$. Si maintenant $\alpha_0 = 0$, la forme f représente zéro et par suite, d'après le théorème 5, elle représente aussi tous les éléments du corps K.

Remarque. — Il résulte de la démonstration du théorème 6 que nous obtenons toutes les représentations de l'élément γ par la forme f à partir des représentations de zéro par la forme $-\gamma_2 x_0^2 + f$ (il suffit de connaître toutes les représentations telles que $x_0 \neq 0$). Ainsi l'étude des représentations par des formes quadratiques non singulières des éléments non nuls d'un corps K se ramène à l'étude des représentations de zéro par des formes non singulières à une variable de plus.

THÉORÈME 7. — *Si pour une forme f représentant zéro, on connaît une représentation de zéro, on peut trouver explicitement une transformation linéaire non singulière des variables telle que la transformée de f soit du type*

$$y_1y_2 + g(y_3, \ldots, y_n).$$

DÉMONSTRATION. — D'après la démonstration du théorème 5, on peut trouver $\alpha_1, \ldots, \alpha_n$ tels que $f(\alpha_1, \ldots, \alpha_n) = 1$. D'après le théorème 2, on peut maintenant transformer f en la forme $x_1^2 + f_1(x_2, \ldots, x_n)$. Puisqu'on connaît une représentation de zéro de la forme $x_1^2 + f_1$ on peut trouver $\beta_2, \ldots, \beta_n$ tel que $f_1(\beta_2, \ldots, \beta_n) = -1$. Appliquant de nouveau le théorème 2, f_1 prend la forme $-x_2^2 + g(y_3, \ldots, y_n)$. Posant $x_1 - x_2 = y_1$, $x_1 + x_2 = y_2$, nous obtenons le résultat demandé.

Remarque. — Supposons que pour toute forme quadratique sur K qui représente zéro dans ce corps, on sache trouver au moins une représentation de zéro. Alors on peut transformer toute forme non singulière en

$$y_1y_2 + \ldots + y_{2s-1}y_{2s} + h(y_{2s+1}, \ldots, y_n), \tag{5}$$

où la forme h ne représente pas zéro. Pour toute représentation de zéro par la forme (5) la valeur d'une au moins des variables $y_1, y_2, \ldots, y_{2s-1}$, y_{2s} est non nulle. Pour trouver toutes les représentations telles que, par exemple, $y_1 = \alpha_1 \neq 0$, nous pouvons donner aux variables $y_3, \ldots, y_n$ des valeurs arbitraires $\alpha_3, \ldots, \alpha_n$ et définir la valeur de y_2 par l'équation

$$\alpha_1y_2 + \alpha_3\alpha_4 + \ldots + g(\alpha_{2s+1}, \ldots, \alpha_n) = 0.$$

Ainsi, le problème de la recherche effective de toutes les représentations de zéro dans le corps K par une forme quadratique non singulière est résolu si on connaît des critères permettant de savoir si une forme donnée représente zéro ou non et si on connaît un algorithme permettant de trouver une représentation de zéro pour toute forme représentant zéro.

THÉORÈME 8. — *Soit un corps* K *contenant plus de 5 éléments. Si la forme diagonale*

$$a_1x_1^2 + \ldots + a_nx_n^2 \qquad (a_i \in \mathrm{K})$$

représente zéro dans le corps K, *il existe une représentation de zéro telle que les valeurs de toutes les variables soient différentes de zéro.*

DÉMONSTRATION. — Montrons tout d'abord que si $a\xi^2 = \lambda \neq 0$, alors, pour tout $b \neq 0$ il existe des éléments α et β différents de zéro tels que

$$a\alpha^2 + b\beta^2 = \lambda.$$

Pour le démontrer, considérons l'identité

$$\frac{(t-1)^2}{(t+1)^2} + \frac{4t}{(t+1)^2} = 1.$$

Multipliant cette identité par $a\xi^2 = \lambda$, nous obtenons

$$a\left(\xi\frac{t-1}{t+1}\right)^2 + at\left(\frac{2\xi}{t+1}\right)^2 = \lambda. \tag{6}$$

Choisissons maintenant dans le corps K un élément $\gamma \neq 0$ tel que la valeur $t = t_0 = \dfrac{b\gamma^2}{a}$ soit différente de ± 1. Puisque chacune des équations

$$bx^2 - a = 0 \qquad \text{et} \qquad bx^2 + a = 0$$

n'a pas plus de deux solutions en x dans K, il y a au plus 5 éléments du corps K qu'on ne peut pas prendre comme γ. Puisque par hypothèse le corps K contient plus de 5 éléments, on peut trouver un tel γ. Posant $t = t_0$ dans l'identité (6), nous obtenons

$$a\left(\xi\frac{t_0-1}{t_0+1}\right)^2 + b\left(\frac{2\xi\gamma}{t_0+1}\right)^2 = \lambda,$$

ce qui démontre l'affirmation ci-dessus.

Il est maintenant facile de terminer la démonstration du théorème. Si la représentation $a_1\xi_1^2 + \ldots + a_n\xi_n^2 = 0$ est telle que $\xi_1 \neq 0, \ldots, \xi_r \neq 0$, $\xi_{r+1} = \ldots = \xi_n = 0$, avec $r \geqslant 2$, alors, d'après ce qui précède, on peut trouver $\alpha \neq 0$ et $\beta \neq 0$ tels que $a_r\xi_r^2 = a_r\alpha^2 + a_{r+1}\beta^2$ et nous obtenons une

représentation avec une variable de plus non nulle. Répétant ce raisonnement, on obtient une représentation dont toutes les valeurs des variables sont non nulles.

4) Formes quadratiques binaires

On appelle forme *binaire* toute forme quadratique de deux variables.

THÉORÈME 9. — *Toutes les formes binaires non singulières représentant zéro dans le corps* K *sont équivalentes entre elles.*

En effet, d'après le théorème 7, toutes ces formes sont équivalentes à la forme y_1y_2.

THÉORÈME 10. — *Pour qu'une forme quadratique binaire f de déterminant $d \neq 0$ représente zéro, il faut et il suffit que $-d$ soit un carré dans* K (i. e. $-d = \alpha^2$, $\alpha \in \mathrm{K}$).

DÉMONSTRATION. — La nécessité de la condition découle des théorèmes 1 et 7. Réciproquement, si $f = ax^2 + by^2$ et $-d = -ab = \alpha^2$, alors

$$f(\alpha, a) = a\alpha^2 + ba^2 = 0.$$

THÉORÈME 11. — *Pour que deux formes binaires non singulières f et g soient équivalentes sur le corps* K, *il faut et il suffit que tout d'abord leurs déterminants diffèrent par un carré dans* K *et ensuite qu'il existe dans* K *au moins un élément non nul représentable simultanément par les deux formes f et g.*

DÉMONSTRATION. — La nécessité de ces deux conditions est évidente. Pour démontrer la suffisance, choisissons dans K un élément $\alpha \neq 0$ représentable par les formes f et g. D'après le théorème 2, les formes f et g sont équivalentes respectivement à des formes du type $f_1 = \alpha x^2 + \beta y^2$ et

$$g_1 = \alpha x^2 + \beta' y^2.$$

Mais, d'après la première condition, $\alpha\beta$ diffère de $\alpha\beta'$ par un carré, d'où $\beta' = \beta\gamma^2$, $\gamma \in \mathrm{K}$, ce qui entraîne $f_1 \sim g_1$, d'où $f \sim g$.

EXERCICES

1. Démontrer que toute forme quadratique singulière représente zéro.

2. Démontrer que le théorème 5 n'est pas valable en général pour les formes singulières.

3. Démontrer que si la forme binaire $x^2 - ay^2$ représente deux éléments γ_1 et γ_2 de K elle représente aussi leur produit $\gamma_1\gamma_2$.

4. Montrer que le théorème 8 n'est pas toujours vrai pour les corps dont le nombre d'éléments ne dépasse pas cinq.

5. Considérons la répartition suivante de toutes les formes quadratiques non singulières à $n = 0, 1, 2, \ldots$ variables sur un corps donné K en classse appelées classes de Witt (nous interpréterons zéro comme une forme non singulière d'un ensemble vide de variables et considérerons que cette forme représente zéro). On dit que deux formes f_1 et f_2 appartiennent à la même classe de Witt, $[f_1] = [f_2]$, si après réduction de ces formes à des formes du type (5) les formes correspondantes h (qui ne représentent pas zéro) contiennent le même nombre de variables et sont équivalentes. L'addition des classes de Witt est alors définie par

$$[f_1] + [f_2] = [f_1 + f_2].$$

Démontrer que les classes de Witt forment un groupe pour cette opération.

6. Définir le groupe des classes de Witt pour les formes quadratiques sur le corps des nombres réels ou sur le corps des nombres complexes.

7. Démontrer qu'une forme quadratique sur un corps fini représente zéro si et seulement si le nombre de ses variables est supérieur ou égal à 3 (on suppose la caractéristique du corps différente de 2).

§ 2. — EXTENSIONS ALGÉBRIQUES

Nous énoncerons sans démonstration les théorèmes de ce paragraphe. Le lecteur pourra trouver les démonstrations dans le livre d'algèbre moderne de Van der Waerden, t. I, chap. 5.

1) Extensions finies

Si un corps Ω contient un corps k comme sous-corps, nous dirons que Ω est une *extension* du corps k. Si on veut préciser que Ω est considéré comme une extension du corps k, on écrit Ω/k. Un corps K qui est un sous-corps du corps Ω contenant k, i. e. $k \subset \mathrm{K} \subset \Omega$, est appelé un *corps intermédiaire de l'extension* Ω/k.

On peut considérer toute extension Ω/k comme un espace vectoriel sur le corps k (pour les opérations d'addition dans Ω et de multiplication par les éléments de k).

DÉFINITION. — *Une extension* K/k *est dite finie si le corps* K, *considéré comme espace vectoriel sur* k, *est de dimension finie. Cette dimension s'appelle le degré de l'extension* K/k *et est désignée par* $(\mathrm{K} : k)$. *Toute base de l'espace vectoriel* K *sur* k *est appelée une base de l'extension* K/k.

Si l'extension K/k est finie, alors, pour tout corps intermédiaire K_0, les extensions K_0/k et K/K_0 sont aussi finies. La réciproque est vraie :

THÉORÈME 1. — *Soit* K_0 *un corps intermédiaire d'une extension* K/k. *Si les extensions* K/K_0 *et* K_0/k *sont finies, alors* K/k *est également une extension finie et son degré est égal au produit des degrés des extensions* K/K_0 *et* K_0/k :

$$(\mathrm{K} : k) = (\mathrm{K} : \mathrm{K}_0)\,(\mathrm{K}_0 : k).$$

DÉMONSTRATION. — Soient $\theta_1, \ldots, \theta_m$ une base de K/K_0 et $\omega_1, \ldots, \omega_n$ une base de K_0/k. Puisque tout élément de K se représente comme combinaison linéaire des produits $\omega_i\theta_j$, alors l'extension K/k est finie. De plus, il est facile de voir que ces produits sont linéairement indépendants sur K et par suite $(\mathrm{K} : k) = mn$.

Pour tout corps k, on désigne par $k[t]$ l'anneau des polynômes en t à coefficients dans k.

Soit Ω/k une extension du corps k. Un élément $\alpha \in \Omega$ est dit *algébrique sur* k si c'est une racine d'un polynôme non nul de l'anneau $k[t]$. Choisissons parmi ces polynômes $f(t)$ (dont α est une racine) le polynôme $\varphi(t)$ non nul de plus bas degré dont le coefficient du terme dominant est égal à 1. Puisque tout $f(t)$ est divisible par $\varphi(t)$ (sinon, le reste de la division par $\varphi(t)$ ne serait pas nul, aurait α comme racine et serait d'un degré inférieur à celui de φ), le polynôme $\varphi(t)$ est défini de manière unique par ces conditions; on l'appelle le *polynôme minimal* de l'élément du corps Ω algébrique sur k. Le polynôme minimal $\varphi \in k[t]$ est toujours irréductible puisque la décomposition $\varphi = gh$ entraîne que α est racine de $g(t)$ ou de $h(t)$. Tout élément $a \in k$ est algébrique sur k et son polynôme minimal est $t - a$. Un élément $\xi \in \Omega$ qui n'est pas algébrique sur k est dit *transcendant sur* k.

L'extension Ω/k est dite *algébrique* si tout élément $\alpha \in \Omega$ est algébrique sur k.

THÉORÈME 2. — *Toute extension finie* K/k *est algébrique.*

THÉORÈME 3. — *Soit* α *un élément d'une extension* Ω/k, *algébrique sur* k *et soit* $\varphi(t) \in k[t]$ *son polynôme minimal, de degré* m. *Alors les puissances* $1, \alpha, \ldots, \alpha^{m-1}$ *sont linéairement indépendantes sur* k *et leurs combinaisons linéaires*

$$a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}, \tag{1}$$

à coefficients $a_i \in k$ *forment un corps intermédiaire noté* $k(\alpha)$. *L'extension* $k(\alpha)/k$ *est finie et de degré* m.

Pour effectuer la somme de deux éléments du corps $k(\alpha)$ écrits sous la forme (1), il est clair qu'il faut additionner les coefficients correspondants. Pour mettre sous la forme (1) le produit des éléments $\xi = g(\alpha)$ et $\eta = h(\alpha)$, où $g(t)$ et $h(t)$ sont des éléments de $k[t]$ de degré $\leqslant m - 1$, on divise gh par φ,

$$g(t)\,h(t) = \varphi(t)\,q(t) + r(t),$$

le reste $r(t)$ étant de degré inférieur ou égal à $m - 1$; puisque $\varphi(\alpha) = 0$, alors $\xi\eta = r(\alpha)$. Ainsi l'opération de multiplication dans l'extension $k(\alpha)/k$ est complètement définie par la connaissance du polynôme minimal $\varphi(t)$ de l'élément α.

Soient $\alpha_1, \ldots, \alpha_s$ un nombre fini d'éléments du corps Ω, algébriques sur k et soient $m_1, \ldots, m_s$ les degrés respectifs de leurs polynômes minimaux sur k. L'ensemble de toutes les combinaisons linéaires des éléments

$$\alpha_1^{k_1} \ldots \alpha_s^{k_s} \qquad (0 \leqslant k_1 < m_1, \ldots, 0 \leqslant k_s < m_s),$$

à coefficients dans k, est un corps intermédiaire que nous désignerons par $k(\alpha_1, \ldots, \alpha_s)$; on l'appelle le corps engendré par les éléments $\alpha_1, \ldots, \alpha_s$. Son degré sur k est inférieur ou égal au produit $m_1 \ldots m_s$.

Toute extension finie K/k contenue dans Ω se représente sous la forme $K = k(\alpha_1, \ldots, \alpha_s)$ pour certains $\alpha_1, \ldots, \alpha_s$.

DÉFINITION. — *Une extension finie* K/k *est dite monogène s'il existe un élément* θ *dans* K *tel que* $K = k(\theta)$. *Tout élément* $\theta \in K$ *tel que* $K = k(\theta)$ *est appelé un élément primitif du corps* K *sur le corps* k.

Les éléments primitifs du corps K sur k sont caractérisés, c'est clair, par le fait que le degré de leur polynôme minimal est égal au degré de l'extension K/k.

THÉORÈME 4. — *Soient* Ω/k *et* Ω'/k *deux extensions du corps* k *et soient des éléments* $\theta \in \Omega$ *et* $\theta' \in \Omega'$ *algébriques sur* k, *possédant le même polynôme minimal* $\varphi(t)$; *alors il existe un isomorphisme (et un seul) du corps* $K(\theta)$ *sur le corps* $K(\theta')$ *tel que* $\theta \to \theta'$ *et* $a \to a$ *pour tout* $a \in k$.

Soit m le degré du polynôme $\varphi(t)$. L'isomorphisme $k(\theta) \to k(\theta')$ défini par le théorème 4 coïncide avec l'application

$$a_0 + a_1\theta + \ldots + a_{m-1}\theta^{m-1} \to a_0 + a_1\theta' + \ldots + a_{m-1}\theta'^{m-1} \qquad (2)$$

($a_0, a_1, \ldots, a_{m-1}$ sont des éléments quelconques du corps k).

Jusqu'à présent, nous n'avons considéré que des extensions finies K/k contenues dans une extension précédemment donnée Ω/k. Étudions maintenant la construction des extensions finies d'un corps fondamental fixé k.

THÉORÈME 5. — *Soit* k *un corps. Pour tout polynôme irréductible* $\varphi(t) \in k[t]$ *de degré* n, *il existe une extension finie* K/k *de degré* n *dans laquelle ce polynôme* φ *a une racine. L'extension* K/k *est unique, à un isomorphisme laissant invariant les éléments de* k *près. Si* $\varphi(\theta) = 0$, $\theta \in K$, *alors* $K = k(\theta)$.

Le corps K (pour $n > 1$) se construit ainsi. Choisissons un nouvel objet θ et considérons l'ensemble K de toutes les combinaisons linéaires formelles de θ,

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} \qquad (3)$$

à coefficients $a_i \in K$. Si on désigne par $g(t)$ le polynôme

$$a_0 + a_1 t + \ldots + a_{n-1}t^{n-1},$$

l'expression (3) peut aussi s'écrire sous la forme $g(\theta)$. Soit $\xi = g(\theta)$ et $\eta = h(\theta)$ deux combinaisons linéaires du type (3) (g et $h \in k[t]$ et sont de degrés $\leqslant n - 1$). Désignons par $s(t)$ la somme $g(t) + h(t)$ et par $r(t)$ le reste de la division du produit de $h(t)$ $g(t)$ par $\varphi(t)$. Posons

$$\xi + \eta = s(\theta)$$
$$\xi\eta = r(\theta).$$

Il est maintenant facile de vérifier que pour ces opérations, l'ensemble K est le corps cherché.

COROLLAIRE. — *Pour tout polynôme* $h(t) \in k[t]$, *il existe une extension finie* K/k *dans laquelle* $h(t)$ *se décompose en facteurs linéaires.*

2) Normes et traces

Soit K/k une extension finie de degré n. Pour tout élément $\alpha \in K$, l'application $\xi \to \alpha\xi$ ($\xi \in K$) est une transformation linéaire de K (comme espace vectoriel sur k). Le polynôme caractéristique $f_\alpha(t)$ de cette transformation linéaire est aussi appelé *polynôme caractéristique de l'élément* $\alpha \in K$ dans l'extension K/k. Soient $\omega_1, \ldots, \omega_n$ une base de l'extension K/k et

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \qquad a_{ij} \in k\ ; \qquad (4)$$

alors

$$f_\alpha(t) = \det(tE - (a_{ij})),$$

où E est la matrice unité d'ordre n.

THÉORÈME 6. — *Le polynôme caractéristique* $f_\alpha(t)$ *d'un élément* $\alpha \in K$ *dans l'extension* K/k *est égal à une puissance de son polynôme minimal* $\varphi_\alpha(t)$ *par rapport à* k.

DÉMONSTRATION. — Soit

$$\varphi_\alpha(t) = t^m + c_1 t^{m-1} + \ldots + c_m.$$

D'après le théorème 3, les nombres $1, \alpha, \ldots, \alpha^{m-1}$ forment une base de l'extension $k(\alpha)/k$. Si $\theta_1, \ldots, \theta_s$ est une base de $K/k(\alpha)$, on peut prendre comme base de K/k les produits

$$\theta_1, \alpha\theta_1, \ldots, \alpha^{m-1}\theta_1\ ; \ldots ;\ \theta_s, \alpha\theta_s, \ldots, \alpha^{m-1}\theta_s.$$

La matrice de la transformation linéaire $\xi \to \alpha\xi$ par rapport à cette base est

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & & 0 & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \dots & -c_2 & -c_1 \end{pmatrix}$$

Son polynôme caractéristique, comme on le vérifie facilement est égal à $t^m + c_1 t^{m-1} + \dots + c_m$, i. e. est égal à $\varphi_\alpha(t)$. Par suite $f_\alpha = \varphi_\alpha^s$ et le théorème 6 est démontré.

Puisque, par passage d'une base de l'espace à un autre, la matrice d'une application linéaire est remplacée par une matrice équivalente, le déterminant et la trace de la matrice (a_{ij}) définie par les égalités (4) ne dépend pas du choix de la base $\omega_1, \dots, \omega_n$.

DÉFINITION. — *Le déterminant* $\det(a_{ij})$ *de la matrice* (a_{ij}) *et sa trace*

$$\operatorname{Tr}(a_{ij}) = \sum_{i=1}^{n} a_{ii}$$

sont appelés respectivement norme et trace de l'élément $\alpha \in K$ *dans l'extension* K/*k*. La norme et la trace sont désignées respectivement par $N_{K/k}(\alpha)$. et $\operatorname{Tr}_{K/k}(\alpha)$ ou, plus simplement, par $N(\alpha)$ et $\operatorname{Tr}(\alpha)$.

Pour $a \in k$, la matrice de la transformation linéaire $\xi \to a\xi$ ($\xi \in K$) est la matrice diagonale aE. Par suite, pour $a \in k$, on a

$$N_{K/k}(a) = a^n$$
$$\operatorname{Tr}_{K/k}(a) = na.$$

D'après les propriétés des matrices des applications linéaires, on a, pour $\alpha, \beta \in K$,

$$N_{K/k}(\alpha\beta) = N_{K/k}(\alpha) N_{K/k}(\beta), \tag{5}$$
$$\operatorname{Tr}_{K/k}(\alpha + \beta) = \operatorname{Tr}_{K/k}(\alpha) + \operatorname{Tr}_{K/k}(\beta). \tag{6}$$

La matrice de la transformation linéaire $\xi \to a\alpha\xi$ ($a \in k$, $\alpha \in K$) est obtenue en multipliant par a tous les termes de la matrice de la transformation $\xi \to \alpha\xi$. Par suite, on a la formule

$$\operatorname{Tr}_{K/k}(a\alpha) = a \operatorname{Tr}_{K/k}(\alpha) \qquad (a \in k,\ \alpha \in K). \tag{7}$$

Si $\alpha \neq 0$, d'après la non-singularité de l'application $\xi \to \alpha\xi$, la norme $N_{K/k}(\alpha)$ est différente de zéro. La formule (5) montre que l'application

$\alpha \to N_{K/k}(\alpha)$ est un homomorphisme du groupe multiplicatif K* du corps K dans le groupe multiplicatif k^* du corps k. En ce qui concerne l'application $\alpha \to \operatorname{Tr}_{K/k} \alpha$ de K dans k, il résulte de (6) et (7) qu'elle est linéaire.

THÉORÈME 7. — *Soit* Ω/k *une extension telle que le polynôme caractéristique* $f_\alpha(t)$ *de l'élément* $\alpha \in K$ *dans une extension finie* K/*k soit décomposable en facteurs linéaires dans* Ω :

$$f_\alpha(t) = (t - \alpha_1) \dots (t - \alpha_n).$$

Alors

$$N_{K/k}(\alpha) = \alpha_1 \alpha_2 \dots \alpha_n$$
$$\operatorname{Tr}_{K/k}(\alpha) = \alpha_1 + \alpha_2 + \dots + \alpha_n.$$

DÉMONSTRATION. — Si

$$f_\alpha(t) = \det(tE - (a_{ij})) = t^n + a_1 t^{n-1} + \dots + a_n,$$

alors

$$a_1 = -\operatorname{Tr}(a_{ij}), \qquad a_n = (-1)^n \det(a_{ij}).$$

D'autre part, d'après les formules de Viète,

$$\alpha_1 + \alpha_2 + \dots + \alpha_n = -a_1, \qquad \alpha_1 \alpha_2 \dots \alpha_n = (-1)^n a_n,$$

d'où le théorème.

THÉORÈME 8. — *Avec les notations et hypothèses du théorème 7, le polynôme caractéristique* $f_\gamma(t)$ *d'un élément* $\gamma = g(\alpha) \in K$ ($g(t) \in k[t]$) *admet la décomposition*

$$(t - g(\alpha_1))(t - g(\alpha_2)) \dots (t - g(\alpha_n)) \tag{8}$$

dans le corps Ω.

DÉMONSTRATION. — Remarquons tout d'abord que les coefficients du polynôme (8), étant des expressions symétriques de $\alpha_1, \dots, \alpha_n$, appartiennent au corps k. Soit $\varphi_\gamma(t)$ le polynôme minimal de l'élément γ sur K. En soumettant l'égalité $\varphi_\gamma(\alpha) = 0$ à l'isomorphisme $k(\alpha) \to k(\alpha_i)$ (tel que $\alpha \to \alpha_i$ et $a \to a$ pour $a \in k$), on obtient $\varphi_\gamma(g(\alpha_i)) = 0$. Toutes les racines du polynôme (8) sont ainsi les racines du polynôme $\varphi_\gamma(t)$, irréductible sur k et cela n'est possible que si ce polynôme est une puissance de $\varphi_\gamma(t)$. Pour terminer la démonstration, il suffit d'appliquer le théorème 6.

Soit $k \subset K \subset L$ une chaîne d'extensions finies. Choisissons pour K/k et L/K respectivement des bases $\omega_1, \dots, \omega_n$ et $\theta_1, \dots, \theta_m$. Pour tout $\gamma \in L$, posons

$$\gamma\theta_j = \sum_{s=1}^{m} \alpha_{js}\theta_s, \qquad \alpha_{js} \in K$$

$$\alpha_{js}\omega_i = \sum_{r=1}^{n} a_{jsir}\omega_r, \qquad a_{jsir} \in k.$$

Puisque

$$\gamma\omega_i\theta_j = \sum_{s,r} a_{jsir}\omega_r\theta_s,$$

alors

$$\mathrm{Tr}_{L/K}(\gamma) = \sum_{i,j} a_{jjii}.$$

D'autre part, nous avons aussi

$$\mathrm{Tr}_{K/k}(\mathrm{Tr}_{L/K}(\gamma)) = \mathrm{Tr}_{K/k}\left(\sum_j a_{jj}\right) = \sum_{i,j} a_{jjii}.$$

Par suite, pour tout $\gamma \in K$, on a

$$\mathrm{Tr}_{L/k}(\gamma) = \mathrm{Tr}_{K/k}(\mathrm{Tr}_{L/K}(\gamma)). \tag{9}$$

On a une formule analogue pour la norme (exercice 2).

3) Extensions séparables

DÉFINITION. — *Une extension finie* K/k *est dite séparable si l'application linéaire* $\xi \to \mathrm{Tr}_{K/k}(\xi)$, $\xi \in K$, *n'est pas identiquement nulle.*

Si la caractéristique du corps k est nulle, alors $\mathrm{Tr}_{K/k}(1) = n = (K : k)$. Par suite, toutes les extensions finies d'un corps de caractéristique zéro sont séparables. C'est vrai aussi, bien entendu, pour toutes les extensions finies d'un corps de caractéristique p dont le degré n'est pas divisible par p.

Choisissons dans une extension finie séparable K/k une base $\omega_1, \ldots, \omega_n$ et considérons la matrice

$$(\mathrm{Tr}\ (\omega_i\omega_j))_{1 \leqslant i,j \leqslant n}. \tag{10}$$

Si le déterminant de cette matrice était nul, alors on pourrait trouver dans le corps k des éléments non tous nuls $c_1, \ldots, c_n$ tels que

$$\sum_{j=1}^{n} c_j\ \mathrm{Tr}\ (\omega_i\omega_j) = 0 \qquad (i = 1, \ldots, n).$$

Posant $\gamma = c_1\omega_1 + \ldots + c_n\omega_n$, nous pouvons transcrire ces égalités sous la forme

$$\mathrm{Tr}\ (\omega_i\gamma) = 0 \qquad (i = 1, \ldots, n). \tag{11}$$

Soit ξ un élément quelconque de K. Puisque $\gamma \neq 0$, on peut représenter ξ sous la forme

$$\xi = a_1\omega_1\gamma + \ldots + a_n\omega_n\gamma \qquad (a_i \in k),$$

d'où, d'après (6), (7) et (11), $\mathrm{Tr}\ (\xi) = 0$. Cela contredit la séparabilité de K/k. Ainsi la matrice (10) est toujours non singulière pour toute extension séparable.

DÉFINITION. — *Le déterminant* $\det\ (\mathrm{Tr}\ (\omega_i\omega_j))$ *est appelé le discriminant de la base* $\omega_1, \ldots, \omega_n$ *de l'extension finie séparable* K/k *et est désigné par* $D(\omega_1, \ldots, \omega_n)$.

D'après ce qui précède, le discriminant de toute base d'une extension finie séparable est un élément non nul du corps de base.

Soit $\omega_1', \ldots, \omega_n'$ une autre base de l'extension K/k et soit

$$\omega_i' = \sum_{j=1}^{n} c_{ij}\omega_j \qquad (i = 1, \ldots, n).$$

Puisque la matrice $(\mathrm{Tr}\ (\omega_i'\omega_j'))$ est égale au produit $(c_{ij})\ (\mathrm{Tr}\ (\omega_i\omega_j))\ (c_{ij})'$ (le prime indique la transposition de la matrice), alors

$$D(\omega_1', \ldots, \omega_n') = (\det\ (c_{ij}))^2\, D(\omega_1, \ldots, \omega_n). \tag{12}$$

Ainsi, les discriminants de deux bases différentes diffèrent l'un de l'autre par un facteur qui est le carré d'un élément du corps fondamental.

Fixons une base quelconque de l'extension K/k. Alors pour des éléments quelconques $c_1, \ldots, c_n$ du corps k il existe un élément $\alpha \in K$ (et un seul) tel que

$$\mathrm{Tr}\ (\omega_i\alpha) = c \qquad (i = 1, \ldots, n). \tag{13}$$

En effet, écrivant α sous la forme $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ ($x_j \in k$) et substituant cette expression de α dans l'égalité (13), nous obtenons un système de n-équations linéaires à n inconnues $x_1, \ldots, x_n$ dont le déterminant est différent de zéro. Ainsi, on peut trouver dans le corps K n éléments $\omega_1^*, \ldots, \omega_n^*$ tels que

$$\mathrm{Tr}\ (\omega_i\omega_i^*) = \begin{cases} 1 & \text{pour} \quad i = j \\ 0 & \text{pour} \quad i \neq j \end{cases} \tag{14}$$

Ces n éléments ω_j^* sont linéairement indépendants sur k puisque si

$$c_1\omega_1^* + \ldots + c_n\omega_n^* = 0 \qquad (c_i \in k),$$

alors multipliant cette égalité par ω_i et prenant la trace on obtient $c_i = 0$ pour tout $i = 1, \ldots, n$.

DÉFINITION. — *La base* $\omega_1^*, \ldots, \omega_n^*$ *de l'extension séparable* K/k *définie de manière unique par les égalités* (14) *est appelée base duale de la base* $\omega_1, \ldots, \omega_n$.

La base duale permet d'écrire sous forme simple les valeurs des coefficients $a_i \in k$ dans la décomposition

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n,$$

d'un élément quelconque α de K. En effet, prenant la trace du produit $\alpha\omega_i^*$, nous obtenons les formules

$$a_i = \mathrm{Tr}\,(\alpha\omega_i^*) \qquad (i = 1, \ldots, n).$$

Supposons que le polynôme minimal $\varphi(t)$ d'un élément α dans une extension séparable K/k se décompose en facteurs linéaires dans l'extension Ω/k :

$$\varphi(t) = (t - \alpha_1) \ldots (t - \alpha_m).$$

Il résulte de manière évidente de la formule (9) que, de même que K/k, l'extension $k(\alpha)/k$ est aussi séparable. Puisque le polynôme minimal φ est aussi le polynôme caractéristique de α dans l'extension $k(\alpha)/k$, alors, d'après les théorèmes 7 et 8

$$\mathrm{Tr}_{k(\alpha)/k}(\alpha^k) = \sum_{s=1}^{m} \alpha_s^k,$$

et par suite le discriminant $\mathrm{D} = \mathrm{D}(1, \alpha, \ldots, \alpha^{m-1})$ de la base $1, \alpha, \ldots, \alpha^{m-1}$ de l'extension $k(\alpha)/k$ s'écrit

$$\mathrm{D} = \det\left(\sum_{s=1}^{m} \alpha_s^{i+j}\right)_{0 \leqslant i,j \leqslant m-1} = \det\left(\alpha_s^i\right) \cdot \det\left(\alpha_s^j\right) = \prod_{0 \leqslant i,j \leqslant m-1} (\alpha_i - \alpha_j)^2.$$

Mais $\mathrm{D} \neq 0$, d'où $\alpha_i \neq \alpha_j$ et nous avons établi le résultat suivant.

THÉORÈME 9. — *Le polynôme minimal de tout élément d'une extension séparable n'a pas de racine multiple* (dans tout corps où il se décompose en facteurs linéaires).

THÉORÈME 10 (théorème de l'élément primitif). — *Toute extension finie séparable* K/k *est monogène*, i. e. *il existe un élément* θ *tel que* $\mathrm{K} = k(\theta)$.

THÉORÈME 11. — *Pour toute extension finie séparable de degré n, il existe n isomorphismes (et n seulement) de l'extension* Ω/k *laissant fixe tout élément de k. Si* $\sigma_1, \ldots, \sigma_n$ *sont ces isomorphismes, pour tout élément* $\alpha \in \mathrm{K}$, *le polynôme caractéristique* $f_\alpha(t)$ *admet dans* Ω *la décomposition*

$$f_\alpha(t) = (t - \sigma_1(\alpha))\,(t - \sigma_2(\alpha)) \ldots (t - \sigma_n(\alpha)).$$

Les éléments $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ (appartenant au corps Ω) sont appelés les *conjugués* de l'élément $\alpha \in \mathrm{K}$. Les images $\sigma_1(\mathrm{K}), \ldots, \sigma_n(\mathrm{K})$ du corps K par les isomorphismes σ_i sont appelés *corps conjugués* du corps K. Si θ est un élément primitif du corps K/k, il est évident que $\sigma_i(\mathrm{K}) = k(\sigma_i(\theta))$.

COROLLAIRE 1. — *Avec ces notations, nous avons*

$$\mathrm{N}_{\mathrm{K}/k}(\alpha) = \sigma_1(\alpha)\,\sigma_2(\alpha) \ldots \sigma_n(\alpha)$$
$$\mathrm{Tr}_{\mathrm{K}/k}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha).$$

COROLLAIRE 2. — *Pour toute extension finie de degré n du corps des nombres rationnels, il existe exactement n isomorphismes dans le corps des nombres complexes.*

Soit $\omega_1, \ldots, \omega_n$ une base de K/k. Puisque

$$\mathrm{Tr}\,(\omega_i\omega_j) = \sum_{s=1}^{n} \sigma_s(\omega_i)\sigma_s(\omega_j),$$

la matrice $(\mathrm{Tr}\,(\omega_i\omega_j))$ est égale au produit des matrices $(\sigma_i(\omega_j))$ $(\sigma_i(\omega_j))$ (le prime signifie la transposition) et par suite on a la formule suivante :

$$\mathrm{D}(\omega_1, \ldots, \omega_n) = (\det(\sigma_i(\omega_j)))^2. \tag{15}$$

EXERCICES

1. Soit $\Omega = k(x)$ le corps des fonctions rationnelles en x à coefficients dans le corps k. Démontrer que tout élément de Ω qui n'appartient pas à k est transcendant sur k.

2. Soit $k \subset \mathrm{K} \subset \mathrm{L}$ une chaîne d'extensions finies. Pour tout $\theta \in \mathrm{L}$, établir la formule

$$\mathrm{N}_{\mathrm{K}/k}(\mathrm{N}_{\mathrm{L}/\mathrm{K}}(\theta)) = \mathrm{N}_{\mathrm{L}/k}(\theta)$$

(Supposer tout d'abord que $\mathrm{L} = \mathrm{K}(\theta)$ et prendre comme base de l'extension L/k la base $\omega_i\theta^j$, où ω_i est une base de K/k).

3. Trouver un élément primitif pour l'extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ du corps $\mathbf{Q}$ des nombres rationnels et l'exprimer avec les nombres $\sqrt{2}$ et $\sqrt{3}$.

4. Démontrer qu'une extension finie K/k est monogène si et seulement si pour cette extension il n'existe qu'un nombre fini de corps conjugués.

5. Soit k un corps quelconque de caractéristique $p \neq 0$. Démontrer que le polynôme $f(t) = t^p - t - a$ $(a \in k)$ ou bien se décompose en un produit de facteurs linéaires dans le corps k ou bien est irréductible. Montrer de plus que, dans le deuxième cas, l'extension $k(\theta)/k$, où $f(\theta) = 0$, est séparable.

6. Soient k_0 un corps de caractéristique $p \neq 0$ et $k = k_0(x)$ le corps des fonctions rationnelles en x à coefficients dans k_0. Montrer que le polynôme $f(t) = t^p - x$ est irréductible dans l'anneau $k[t]$. Démontrer de plus que l'extension $k(\theta)/k$, où $f(\theta) = 0$, n'est pas séparable.

7. Démontrer que si, pour une extension finie K/k de degré n, il existe n isomorphismes distincts dans une extension Ω/k, laissant invariants les éléments de k, alors l'extension K/k est séparable.

8. Soit k un corps quelconque de caractéristique $\neq p$ contenant une racine primitive d'ordre p de 1. Démontrer que si un élément $\alpha \in k$ n'est pas égal à la puissance $p^{\text{ième}}$ d'un élément de k, alors :

$$(k(\sqrt[p]{\alpha}) : k) = p.$$

9. Soient K/k une extension finie séparable et φ une forme linéaire sur l'espace vectoriel K sur le corps k. Démontrer qu'il existe dans le corps K un élément α tel que

$$\varphi(\xi) = \mathrm{Tr}_{K/k}(\alpha\xi), \qquad \xi \in K,$$

§ 3. — CORPS FINIS

Un corps Σ est dit *fini* s'il ne contient qu'un nombre fini d'éléments. Un exemple de corps fini est le corps $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ des classes résiduelles modulo un nombre premier p dans l'anneau $\mathbf{Z}$ des entiers rationnels. Tous ces corps ont une caractéristique qui est un nombre premier et si la caractéristique d'un corps fini Σ est égale à p, alors ce corps contient un sous-corps premier (n'admettant pas de sous-corps propre), qui est isomorphe au corps $\mathbf{F}_p$. C'est pourquoi on peut considérer que $\mathbf{F}_p \subset \Sigma$. L'extension $\Sigma/\mathbf{F}_p$ est finie ; si son degré est égal à m et si $\omega_1, \ldots, \omega_m$ est une base de Σ sur $\mathbf{F}_p$, tout élément $\xi \in \Sigma$ s'écrit de manière unique $\xi = c_1\omega_1 + \ldots + c_m\omega_m$, où les c_i parcourent, indépendamment l'un de l'autre les p éléments de $\mathbf{F}_p$. Puisque le nombre de ces combinaisons linéaires est égal à p^m, cela démontre que *le nombre d'éléments d'un corps fini est égal à une puissance de sa caractéristique.*

Le groupe multiplicatif Σ^* du corps fini Σ est un groupe abélien fini. Précisons sa structure.

LEMME. — *Tout sous-groupe* G *du groupe multiplicatif* K^* *d'un corps fini* K *est cyclique.*

DÉMONSTRATION. — Montrons tout d'abord que si, dans un groupe abélien G, il existe des éléments d'ordres m et n, alors il existe également dans G un élément dont l'ordre est égal au plus petit commun multiple k des nombres m et n. Supposons que les éléments x et y de G sont d'ordres respectifs m et n. Si $(m, n) = 1$, le produit xy est d'ordre $k = mn$. Dans le cas général, utilisons les décompositions canoniques des nombres m et n comme produit de puissances de nombres premiers; nous pouvons les écrire sous la forme

$$m = m_0m_1, \qquad n = n_0n_1$$

tels que $(m_0, n_0) = 1$ et $k = m_0n_0$. Les éléments x^{m_1} et y^{n_1} sont d'ordres respectifs m_0 et n_0 et leur produit $x^{m_1}y^{n_1}$ est d'ordre $k = n_0m_0$.

Soit maintenant un sous-groupe fini d'ordre g du groupe multiplicatif du corps K. Si m est le plus grand des ordres des éléments du groupe G, il est clair que $m \leqslant g$. D'autre part, d'après ce qui précède, l'ordre de tout élément de G divise m, i. e. tous les éléments du groupe G sont des racines du polynôme $t^m - 1$. Mais, dans un corps, un polynôme de degré m ne peut avoir plus de m racines, d'où $g \leqslant m$. Ainsi $g = m$ et cela signifie que le groupe G est cyclique.

Appliquant le lemme ci-dessus au cas d'un corps fini, nous obtenons :

THÉORÈME 1. — *Le groupe multiplicatif d'un corps fini à p^m éléments est un groupe cyclique d'ordre $p^m - 1$.*

COROLLAIRE. — *Toute extension finie d'un corps fini est monogène.*

En effet, si θ est un élément du groupe Σ^*, alors il est évident que $\mathbf{F}_p(\theta) = \Sigma$. Pour tout corps intermédiaire Σ_0, on a donc $\Sigma_0(\theta) = \Sigma$.

Du théorème 1 découle aussi que tous les éléments de Σ sont les racines du polynôme $t^{p^m} - t$ et puisque le degré de ce polynôme est égal au nombre d'éléments de Σ on a dans l'anneau $\Sigma[t]$ la décomposition

$$t^{p^m} - t = \prod_{\xi \in \Sigma}(t - \xi)$$

(ξ parcourt tous les éléments du corps Σ).

THÉORÈME 2. — *Pour tout entier premier p et pour tout entier naturel m, il existe un corps fini et un seul à isomorphisme près, contenant p^m éléments.*

DÉMONSTRATION. — D'après le corollaire du théorème 5, § 2, il existe une extension $\Omega/\mathbf{F}_p$ dans laquelle le polynôme $t^{p^m} - t$ se décompose en facteurs linéaires. Désignons par Σ l'ensemble de toutes ces racines (contenues dans Ω). Puisque dans tout corps de caractéristique p, on a la formule

$$(x \pm y)^{p^m} = x^{p^m} \pm y^{p^m},$$

la somme et la différence de deux éléments de Σ sont encore des éléments de Σ. L'ensemble Σ est fermé aussi par rapport aux opérations de multiplication et de division (par un diviseur non nul). Par suite Σ est un sous-corps du corps Ω. Le polynôme $t^{p^m} - t$ n'a pas de racines multiples (puisque sa dérivée $p^m t^{p^m-1} - 1 = -1$ n'est nulle pour aucune valeur de t); ainsi Σ contient p^m élément. Ceci démontre l'existence d'un corps fini à p^m éléments.

Soient maintenant Σ et Σ' deux extensions de degré m de $\mathbf{F}_p$. Choisissons dans Σ un élément primitif θ (corollaire du théorème 1) et désignons par $\varphi(t)$ son polynôme minimal. Puisque $\varphi(t)$ est un diviseur du polynôme $t^{p^m} - t$ et que ce dernier est décomposable dans Σ' en facteurs linéaires, alors $\varphi(t)$ a une racine $\theta' \in \Sigma'$. L'extension $\mathbf{F}_p(\theta')/\mathbf{F}_p$ est de degré égal au degré du

polynôme $\varphi(t)$, i. e. m; par suite, $\mathbf{F}_p(\theta') = \Sigma'$. L'existence de l'isomorphisme des corps Σ et Σ' résulte alors du théorème 4, § 2.

On désigne habituellement par $GF(p^m)$ ou $\mathbf{F}_{p^m}$ le corps fini à p^m éléments (appelé corps de Galois).

COROLLAIRE. — *Sur tout corps fini $\Sigma_0 = GF(p^r)$, il existe des polynômes irréductibles de degré n quelconque.*

En effet, $p^r - 1$ est un diviseur de $p^{rn} - 1$ et par suite toutes les racines du polynôme $t^{p^r} - t$ dans le corps $\Sigma = GF(p^{rn})$ constituent un sous-corps isomorphe au corps Σ_0. Nous pouvons donc considérer que $\Sigma_0 \subset \Sigma$. Le polynôme minimal d'un élément primitif quelconque $\theta \in \Sigma$ par rapport à Σ_0 est un polynôme irréductible de l'anneau $\Sigma_0[t]$, de degré n puisque

$$(\Sigma : \Sigma_0) = \frac{(\Sigma : \mathbf{F}_p)}{(\Sigma_0 : \mathbf{F}_p)} = \frac{rn}{r} = n.$$

Remarquons pour terminer que pour qu'un anneau commutatif fini soit un corps, il suffit qu'il n'ait pas de diviseur de zéro. En effet, soit $\mathfrak{D}$ un anneau commutatif fini sans diviseurs de zéro et soit a un élément différent de zéro de $\mathfrak{D}$. Si $ax_1 = ax_2$, alors $(x_1 - x_2) = 0$, d'où $x_1 = x_2$; ainsi, si $x_1 \neq x_2$, les produits ax_1 et ax_2 sont aussi distincts et cela signifie le produit ax parcourt avec x tous les éléments de l'anneau $\mathfrak{D}$. Mais alors pour tout $b \neq 0$ l'équation $ax = b$ est résoluble dans $\mathfrak{D}$, i. e. tous les éléments non nuls de l'anneau $\mathfrak{D}$ constituent un groupe multiplicatif.

EXERCICES

1. Montrer que le nombre $r(m)$ de polynômes irréductibles de degré m distincts de l'anneau $\mathbf{F}_p[t]$ de coefficients dominants égaux à 1 s'exprime par la formule

$$r(m) = \frac{1}{m}\sum_{d|m} \mu\left(\frac{m}{d}\right) p^d$$

(d parcourt tous les diviseurs du nombre m et $\mu(k)$ désigne la fonction de Moëbius).

2. Trouver tous les polynômes irréductibles de degré 2 sur le corps $\mathbf{F}_5 = GF(5)$.

3. Montrer que le corps $GF(p^m)$ est contenu dans le corps $GF(p^n)$ (au sens d'un plongement isomorphe) si et seulement si $m|n$.

4. Quel est le degré sur $\mathbf{F}_p$ du corps de décomposition du polynôme $t^n - 1$?

5. Soit $\Sigma = GF(p^m)$. Montrer que les applications

$$\sigma_i : \xi \to \xi^{p^i}, \qquad \xi \in \Sigma \qquad (i = 0, 1, \ldots, m-1)$$

sont des automorphismes deux à deux distincts du corps Σ et que tout automorphisme de Σ coïncide avec un des σ_i.

6. Soient $\Sigma_0 = GF(p^r)$ et Σ une extension finie de degré n de Σ_0. Démontrer que les applications $\xi \to \xi^{p^{ri}}$, $\xi \in \Sigma$ ($i = 0, 1, \ldots, n-1$), constituent un système complet de n automorphismes deux à deux distincts de Σ laissant invariant les éléments de Σ_0. Montrer que le polynôme caractéristique $f_\xi(t)$ d'un élément $\xi \in \Sigma$ pour l'extension Σ/Σ_0 admet dans le corps Σ la décomposition

$$f_\xi(t) = (t - \xi)(t - \xi^q) \ldots \left(t - \xi^{q^{n-1}}\right)$$

où $q = p^r$ (utiliser le théorème 8 du § 2). En déduire que

$$\mathrm{Tr}_{\Sigma/\Sigma_0}(\xi) = \xi + \xi^q + \ldots + \xi^{q^{n-1}}, \quad \mathrm{N}_{\Sigma/\Sigma_0}(\xi) = \xi^{1+q+\ldots+q^{n-1}}.$$

7. Démontrer que toute extension finie d'un corps fini est séparable.

8. Avec les notations de l'exercice 6, démontrer que tout élément du corps Σ_0 est la norme d'un certain élément de Σ.

9. Soient $\Sigma = GF(p^{mr})$, $p^m = q$, $\alpha \in \Sigma$. Démontrer que l'équation $\xi^q - \xi = \alpha$ est résoluble dans le corps Σ si et seulement si $\alpha + \alpha^q + \ldots + \alpha^{q^{r-1}} = 0$.

10. Soit ε une racine primitive de 1 d'ordre premier p. Puisque les éléments du sous-corps premier $\Sigma_0 = GF(p)$ du corps $\Sigma = GF(p^m)$ sont des classes résiduelles de l'anneau des nombres entiers rationnels modulo p, la puissance $\varepsilon^{\mathrm{Tr}\,\gamma}$ a un sens pour tout $\gamma \in \Sigma$ (la trace est considérée dans l'extension Σ/Σ_0). Démontrer que

$$\sum_{\xi \in \Sigma} \varepsilon^{\mathrm{Tr}\,\xi\alpha} = \begin{cases} 0 & \text{si} \quad \alpha \neq 0, \\ p^m & \text{si} \quad \alpha = 0. \end{cases}$$

11. Soient χ un caractère du groupe multiplicatif du corps $\Sigma = GF(p^m)$, $p^m = q$ (pour la définition des caractères, cf. § 5). Prolongeons χ à tout le corps Σ en posant $\chi(0) = 0$. L'expression

$$\tau_\alpha(\chi) = \sum_{\xi \in \Sigma} \chi(\xi)\varepsilon^{\mathrm{Tr}\,\alpha\xi} \qquad (\alpha \in \Sigma),$$

qui est un nombre complexe, est appelé une somme de Gauss du corps fini Σ. Supposant que le caractère χ est différent du caractère unité χ_0, démontrer les formules

$$\tau_\alpha(\chi) = \chi(\alpha)^{-1}\tau_1(\chi), \qquad \alpha \neq 0 ;$$

$$|\tau_\alpha(\chi)| = \sqrt{q}, \qquad \alpha \neq 0 ;$$

$$\sum_{\alpha \neq 0} \tau_\alpha(\chi) = 0.$$

12. Soit $p \neq 2$. Puisque tous les carrés du groupe multiplicatif Σ^* du corps $\Sigma = GF(p^m)$ forment un sous-groupe d'indice 2, alors, posant $\psi(\alpha) = +1$ si $\alpha \neq 0$ est un carré et $\psi(\alpha) = -1$ dans le cas contraire nous obtenons un caractère ψ du groupe Σ^*. Démontrer, pour $\alpha\beta \neq 0$,

$$\tau_\alpha(\psi)\,\tau_\beta(\psi) = \psi(-\alpha\beta)p^m.$$

13. Démontrer, pour $\alpha \neq 0$, la relation

$$\sum_{\xi \in \Sigma} \psi(\xi^2 - \alpha) = -1.$$

14. Soit $f(x_1, \ldots, x_n)$ une forme quadratique non singulière, de déterminant δ, à coefficients dans $\Sigma = \mathrm{GF}(p^m)$, $p^m = q$, $p \neq 2$ et soit α un élément quelconque de Σ. Démontrer que le nombre N de solutions dans Σ de l'équation

$$f(x_1, \ldots, x_n) = \alpha$$

s'exprime par les formules

$$\mathrm{N} = q^{2r} + q^r \psi((-1)^r \alpha\delta), \qquad \text{si} \quad n = 2r+1,$$

$$\mathrm{N} = q^{2r-1} + \omega q^{r-1} \psi((-1)^r \delta), \qquad \text{si} \quad n = 2r,$$

avec $\omega = -1$ pour $\alpha \neq 0$ et $\omega = q - 1$ pour $\alpha = 0$.

15. Soient p et q des nombres rationnels premiers impairs distincts. Nous désignerons par la même lettre x les classes résiduelles d'un entier x dans les corps GF(p) et GF(q). Choisissons une extension Δ du corps GF(q) dans laquelle le polynôme $t^p - 1$ se décompose en facteurs linéaires et désignons par ε une racine primitive d'ordre p de 1 appartenant à Δ. Le symbole de Legendre $\left(\frac{x}{p}\right)$ coïncide, c'est clair, avec le caractère $\psi(x)$ du corps GF(p) introduit dans l'exercice 12. Puisque ses valeurs sont ± 1, on peut considérer que $\left(\frac{x}{p}\right) \in \Delta$. Démontrer que la « somme de Gauss »

$$\tau = \sum_{x \in \mathrm{GF}(p)} \left(\frac{x}{p}\right) \varepsilon^x \in \Delta$$

du corps GF(p) vérifie les égalités :

$$\tau^2 = (-1)^{\frac{p-1}{2}} p, \tag{1}$$

$$\tau^q = \left(\frac{q}{p}\right) \tau. \tag{2}$$

16. Utilisant la valeur $\left(\frac{q}{p}\right) = p^{\frac{q-1}{2}}$ du symbole de Legendre dans le corps GF(q), déduire des formules (1) et (2) la loi de réciprocité de Gauss :

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

§ 4. — NOTIONS SUR LES ANNEAUX COMMUTATIFS

Dans ce paragraphe, nous entendrons par anneau un anneau commutatif avec élément unité 1 et sans diviseurs de zéro.

1) Divisibilité dans les anneaux

Soit $\mathfrak{D}$ un anneau. Si pour des éléments α et $\beta \neq 0$ de $\mathfrak{D}$ il existe un élément $\xi \in \mathfrak{D}$ tel que $\beta\xi = \alpha$, on dit que α est divisible par β (ou que β divise α) et on écrit $\beta \mid \alpha$. Puisque $\mathfrak{D}$ n'a pas de diviseurs de zéro, l'égalité $\beta\xi = \alpha$ définit de manière unique l'élément ξ. La notion de divisibilité dans un anneau quelconque possède, c'est clair, les propriétés de la divisibilité pour les entiers rationnels. Par exemple, si γ/β et β/α, alors γ/α.

Un élément $\varepsilon \in \mathfrak{D}$ qui est un diviseur de l'élément 1 s'appelle une *unité* de l'anneau $\mathfrak{D}$ (ou élément inversible).

THÉORÈME 1. — *Les unités d'un anneau $\mathfrak{D}$ constituent un groupe multiplicatif.*

DÉMONSTRATION. — Soit E l'ensemble de toutes les unités de l'anneau $\mathfrak{D}$. Si $\varepsilon \in \mathrm{E}$ et $\eta \in \mathrm{E}$, alors $\varepsilon\varepsilon' = 1$ et $\eta\eta' = 1$ pour $\varepsilon', \eta' \in \mathfrak{D}$; mais alors

$$(\varepsilon\eta)(\varepsilon'\eta') = 1$$

et par suite $\varepsilon\eta \in \mathrm{E}$. Puisque $1 \in \mathrm{E}$ et que pour toute unité ε il existe un élément ε' défini par l'égalité $\varepsilon\varepsilon' = 1$, alors $\varepsilon' \in \mathrm{E}$ et E est donc un groupe.

Des éléments $\alpha \neq 0$ et $\beta \neq 0$ de l'anneau $\mathfrak{D}$ sont dits *associés* s'ils sont divisibles l'un par l'autre. Des égalités $\alpha = \beta\xi$ et $\beta = \alpha\eta$ ($\xi, \eta \in \mathfrak{D}$), il résulte que $\alpha = \alpha\xi\eta$, d'où $1 = \xi\eta$ (puisque $\alpha \neq 0$ et qu'il n'y a pas de diviseurs de zéro dans l'anneau). Ainsi, dire que deux éléments non nuls sont associés signifie qu'ils diffèrent l'un de l'autre par un facteur qui est une unité de $\mathfrak{D}$.

Soit $\mu \neq 0$ un élément de l'anneau $\mathfrak{D}$ qui n'est pas une unité. On dit que deux éléments α et β de $\mathfrak{D}$ sont congrus modulo μ et on écrit $\alpha \equiv \beta \pmod{\mu}$, si la différence $\alpha - \beta$ est divisible par μ. Cette notion de congruence vérifie les propriétés habituelles des congruences dans l'anneau des nombres entiers. Pour tout $\alpha \in \mathfrak{D}$, on désigne par $\bar{\alpha}$ l'ensemble de tous les éléments de $\mathfrak{D}$ congrus à α modulo μ. L'ensemble $\bar{\alpha}$ est appelé une classe résiduelle modulo μ. L'égalité $\bar{\alpha} = \bar{\beta}$ est satisfaite, c'est clair, si et seulement si $\alpha \equiv \beta \pmod{\mu}$. On peut définir la somme et le produit de deux classes dans l'ensemble des classes résiduelles modulo μ en posant

$$\bar{\alpha} + \bar{\beta} = \overline{\alpha + \beta}, \qquad \bar{\alpha}\bar{\beta} = \overline{\alpha\beta}.$$

Puisque la relation de congruence est compatible avec l'addition et la multiplication de l'anneau $\mathfrak{D}$, la somme et le produit des classes ainsi définis ne dépendent pas du choix des représentants α et β. Une simple vérification montre que l'ensemble de toutes les classes résiduelles modulo μ constitue un anneau commutatif pour les opérations ci-dessus, à élément unité $\bar{1}$ (c'est vrai même s'il y a des diviseurs de zéro). Cet anneau s'appelle l'anneau des classes résiduelles modulo μ.

Si dans chaque classe résiduelle modulo μ on choisit un représentant, l'ensemble S de ces éléments s'appelle un *système complet de résidus*

modulo μ. Un système complet de résidus S est donc caractérisé par le fait que tout élément de l'anneau $\mathfrak{D}$ est congru modulo μ à un élément de S et un seul.

2) Idéaux

Un sous-ensemble A d'un anneau $\mathfrak{D}$ s'appelle un idéal si c'est un sous-groupe du groupe additif de l'anneau $\mathfrak{D}$ et si pour tout $\alpha \in A$ et tout $\xi \in \mathfrak{D}$, le produit $\xi\alpha$ appartient à A. L'ensemble réduit à l'élément zéro et l'anneau $\mathfrak{D}$ tout entier constituent des exemples triviaux d'idéaux (appelés respectivement idéal nul et idéal unité).

Soient $\alpha_1, \ldots, \alpha_m$ des éléments quelconques de l'anneau $\mathfrak{D}$. Il est évident que l'ensemble A de toutes les combinaisons linéaires

$$\xi_1\alpha_1 + \xi_2\alpha_2 + \ldots + \xi_m\alpha_m$$

de ces éléments à coefficients $\xi_i \in \mathfrak{D}$ est un idéal de l'anneau $\mathfrak{D}$, appelé idéal engendré par les éléments $\alpha_1, \ldots, \alpha_m$ et désigné par $A = (\alpha_1, \ldots, \alpha_m)$. Les éléments $\alpha_1, \ldots, \alpha_m$ sont appelés des générateurs de l'idéal A. Dans le cas général, il n'existe pas pour tout idéal de système fini de générateurs. Un idéal A est dit *principal* s'il admet un système de générateurs formé d'un seul élément, i. e. s'il est de la forme $A = (\alpha)$. Il est clair que tout idéal principal non nul (α) est égal à l'ensemble des éléments de l'anneau $\mathfrak{D}$ qui sont divisibles par α. Les idéaux nul et unité sont principaux : l'idéal nul est engendré par 0 et l'idéal unité par une unité quelconque ε de l'anneau $\mathfrak{D}$. Deux idéaux principaux (α) et (β) coïncident si et seulement si α et β sont associés.

Soient A et B deux idéaux d'un anneau $\mathfrak{D}$. L'ensemble de tous les éléments $\xi \in \mathfrak{D}$ de la forme

$$\xi \equiv \alpha_1\beta_1 + \ldots + \alpha_s\beta_s$$

où $\alpha_i \in A$, $\beta_i \in B$ ($s \geqslant 1$) est encore un idéal dans $\mathfrak{D}$, que nous appellerons l'idéal produit des idéaux A et B; il sera désigné par AB. Puisque la multiplication des idéaux est commutative et associative, les idéaux de l'anneau $\mathfrak{D}$ (commutatif) constituent un monoïde pour cette opération.

Deux éléments α et β de $\mathfrak{D}$ sont dits congrus modulo un idéal A et on note $\alpha \equiv \beta \pmod{A}$, si la différence $\alpha - \beta$ appartient à A, i. e. si α et β appartiennent à la même classe résiduelle relative au sous-groupe additif A. Il est clair que la congruence $\alpha \equiv \beta \pmod{A}$ est satisfaite si et seulement si $\bar{\alpha} = \bar{\beta}$, en désignant par $\bar{\gamma}$ la classe résiduelle relative au sous-groupe A qui contient $\gamma \in \mathfrak{D}$. La relation de congruence modulo un idéal, dans le cas d'un idéal principal (μ) coïncide avec la congruence modulo l'élément μ (cf. 1)). Considérons le groupe $\mathfrak{D}/A$ quotient du groupe additif de l'anneau $\mathfrak{D}$ par le sous-groupe A. Dans le cas où A est un idéal, on peut définir une multiplication dans le groupe quotient $\mathfrak{D}/A$: pour $\bar{\alpha}$ et $\bar{\beta}$ dans $\mathfrak{D}/A$, posons

$$\bar{\alpha}\bar{\beta} = \overline{\alpha\beta}.$$

Si $\bar{\alpha} = \overline{\alpha_1}$ et $\bar{\beta} = \overline{\beta_1}$, alors, d'après l'égalité

$$\alpha_1\beta_1 - \alpha\beta = \alpha_1(\beta_1 - \beta) + \beta(\alpha_1 - \alpha)$$

et puisque $\alpha_1 - \alpha$ et $\beta_1 - \beta$ appartiennent à A, on a $\alpha_1\beta_1 \equiv \alpha\beta \pmod{A}$ (ici le fait que A soit un idéal est essentiel) et cela signifie que le produit $\bar{\alpha},\bar{\beta}$ ne dépend pas du choix des représentants α et β. Il est facile de vérifier que le groupe quotient $\mathfrak{D}/A$ est un anneau pour cette multiplication et pour l'addition $\bar{\alpha} + \bar{\beta} = \overline{\alpha + \beta}$. L'anneau $\mathfrak{D}/A$ est appelé anneau quotient de l'anneau $\mathfrak{D}$ par l'idéal A. Dans le cas d'un idéal principal (μ), l'anneau quotient $\mathfrak{D}/(\mu)$ n'est autre que l'anneau des classes résiduelles modulo μ.

3) Éléments entiers

Tout anneau $\mathfrak{U}$ (commutatif et sans diviseurs de zéro) peut être plongé dans un corps. Pour montrer ce résultat, considérons l'ensemble de toutes les fractions formelles $\frac{a}{b}$, où a et b sont des éléments de $\mathfrak{U}$ et $b \neq 0$. Deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ seront dites égales si et seulement si $ad = bc$. Définissons l'addition et la multiplication par les formules

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Il est facile de vérifier que ces opérations sont compatibles avec l'égalité et que l'ensemble de toutes les fractions considérées est ainsi muni d'une structure de corps; désignons ce corps par k_0. Si nous identifions les fractions $\frac{a}{1} = \frac{ac}{c}$, $c \neq 0$ à l'élément $a \in \mathfrak{U}$, alors $\mathfrak{U}$ est un sous-anneau du corps k_0. Tout élément de k_0 est alors le quotient de deux éléments de $\mathfrak{U}$.

Soit maintenant Ω un corps quelconque contenant $\mathfrak{U}$ comme sous-anneau. L'ensemble k de tous les quotients $\frac{a}{b}$, où $a, b \in \mathfrak{U}$ ($b \neq 0$) est un sous-corps du corps Ω. Ce sous-corps est appelé corps des fractions de

l'anneau $\mathfrak{U}$ (il est facile de voir que le corps k est isomorphe au corps k_0 construit ci-dessus et qu'il est défini par l'anneau $\mathfrak{U}$ de manière unique (à un isomorphisme près).

DÉFINITION. — *Soit un anneau $\mathfrak{U}$ contenu dans un corps Ω. Un élément $\alpha \in \Omega$ est dit entier sur $\mathfrak{U}$ si c'est une racine d'un polynôme à coefficients dans $\mathfrak{U}$ et dont le coefficient dominant est égal à* 1.

Puisque tout élément $a \in \mathfrak{U}$ est racine du polynôme $t - a$, alors tout élément de $\mathfrak{U}$ est entier sur $\mathfrak{U}$.

Soient $\omega_1, \ldots, \omega_m$ des éléments quelconques de Ω. L'ensemble M de toutes les combinaisons linéaires $a_1\omega_1 + \ldots + a_m\omega_m$ à coefficients $a_i \in \mathfrak{U}$ est appelé un $\mathfrak{U}$-module de type fini dans Ω et les éléments $\omega_1, \ldots, \omega_m$ sont appelés des générateurs du $\mathfrak{U}$-module M. Puisque $1 \in \mathfrak{U}$, tous les ω_i appartiennent à M.

LEMME 1. — *Si un $\mathfrak{U}$-module de type fini* M *est un anneau, alors tous ses éléments sont entiers sur $\mathfrak{U}$.*

DÉMONSTRATION. — Nous pouvons bien entendu supposer qu'aucun des ω_i n'est nul. Soit α un élément quelconque de M. Puisque pour tout i le produit $\alpha\omega_i$ appartient à M, alors

$$\alpha\omega_i = \sum_{j=1}^{m} a_{ij}\omega_j, \qquad a_{ij} \in \mathfrak{U}, \qquad (i = 1, \ldots, m).$$

Il en résulte que $\det(\alpha E - (a_{ij})) = 0$ (E est la matrice unité d'ordre n). Ainsi l'élément α est racine du polynôme $f(t) = \det(tE - (a_{ij}))$ à coefficients dans $\mathfrak{U}$ et dont le coefficient dominant est 1. Cela démontre le lemme.

THÉORÈME 2. — *L'ensemble $\mathfrak{D}$ de tous les éléments de Ω entiers sur $\mathfrak{U}$ est un anneau.*

DÉMONSTRATION. — Il faut montrer que la somme, la différence et le produit de deux éléments entiers α et β de Ω sont aussi des éléments entiers. Si α et β sont respectivement des racines des polynômes

$$t^m - a_m t^{m-1} - \ldots - a_1, \qquad t^n - b_n t^{n-1} - \ldots - b_1 ;$$

où a et $b_j \in \mathfrak{U}$, alors

$$\alpha^m = a_1 + a_2\alpha + \ldots + a_m\alpha^{m-1}, \qquad \beta^n = b_1 + b_1\beta + \ldots + b_n\beta^{n-1}.$$

Il en résulte facilement que le $\mathfrak{U}$-module constitué par toutes les combinaisons linéaires des produits

$$\alpha^i\beta \qquad (0 \leqslant i \leqslant m,\ 0 \leqslant j < m) \tag{1}$$

à coefficients dans $\mathfrak{U}$, est un anneau (puisque les produits $\alpha^k\beta^l$ pour $k \geqslant 0$ et $l \geqslant 0$ s'écrivent comme des combinaisons linéaires des éléments (1) à coefficients dans $\mathfrak{U}$). D'après le lemme 1, tous les éléments de cet anneau sont donc entiers sur $\mathfrak{U}$; en particulier, $\alpha \pm \beta$ et $\alpha\beta$ sont entiers. Le théorème 2 est démontré.

DÉFINITION. — *Soit $\mathfrak{U}$ un sous-anneau d'un corps Ω. L'ensemble $\mathfrak{D}$ de tous les éléments de Ω entiers sur $\mathfrak{U}$ s'appelle la fermeture intégrale de l'anneau $\mathfrak{U}$ dans le corps Ω.*

DÉFINITION. — *Un sous-anneau $\mathfrak{D}_0$ d'un corps* K *est dit intégralement fermé dans* K *si sa fermeture intégrale dans* K *coïncide avec $\mathfrak{D}_0$.*

On dit simplement que l'anneau $\mathfrak{U}$ est *intégralement clos* s'il est intégralement fermé dans son corps des fractions.

THÉORÈME 3. — *Soit $\mathfrak{U}$ un sous-anneau d'un corps Ω. La fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{U}$ dans le corps est intégralement fermée dans Ω.*

DÉMONSTRATION. — Soit θ un élément quelconque de Ω entier sur $\mathfrak{D}$ donc tel que

$$\theta^n = \alpha_1 + \alpha_2\theta + \ldots + \alpha_n\theta^{n-1}, \tag{2}$$

où tous les α_i appartiennent à $\mathfrak{D}$. Il faut démontrer que $\theta \in \mathfrak{D}$. Pour tout $i = 1, \ldots, n$, il existe un entier m tel que l'on ait l'égalité

$$\alpha^{m_i} = \sum_{j=1}^{m_i} a_{ij}\alpha_i^{j-1}, \qquad a_{ij} \in \mathfrak{U} \tag{3}$$

(puisque α_i est entier sur $\mathfrak{U}$). Considérons le $\mathfrak{U}$-module M engendré par les produits

$$\alpha_1^{k_1} \ldots \alpha_n^{k_n}\theta^k \qquad (0 \leqslant k_i < m_i,\quad 0 \leqslant k < n). \tag{4}$$

Il résulte facilement de (2) et (3) que tout produit $\alpha_1^{l_1} \ldots \alpha_n^{l_n}\theta^l$ avec des exposants positifs s'exprime comme combinaison linéaire des éléments (4) à coefficients dans $\mathfrak{U}$ et cela signifie que le module M est un anneau. D'après le lemme 1, tous les éléments de M sont donc entiers sur $\mathfrak{U}$. En particulier, θ est entier, C. Q. F. D.

LEMME 2. — *Soit $\mathfrak{U}$ un anneau intégralement clos (dans son corps des fractions k) et supposons que le coefficient dominant d'un polynôme $f(t) \in \mathfrak{U}[t]$ est égal à* 1. *Si le coefficient dominant d'un diviseur $\varphi(t) \in k[t]$ du polynôme $f(t)$ est égal à* 1, *alors $\varphi(t) \in \mathfrak{U}[t]$.*

DÉMONSTRATION. — Considérons une extension Ω/k du corps k dans laquelle $f(t)$ se décompose en facteurs linéaires (corollaire du théorème 5, § 2). Toutes les racines de $f(t)$ appartiennent à la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{U}$ dans le corps Ω. En particulier, toutes les racines de $\varphi(t)$ appartiennent à l'anneau $\mathfrak{D}$. Mais il résulte de la décomposition

$$\varphi(t) = (t - \gamma_1) \ldots (t - \gamma_s)$$

que tous les coefficients de $\varphi(t)$ appartiennent à $\mathfrak{D}$ et puisque $\mathfrak{D} \cap k = \mathfrak{U}$ (puisque $\mathfrak{U}$ est intégralement clos), ces coefficients appartiennent à $\mathfrak{U}$. C. Q. F. D.

Du lemme 2 découle de manière évidente le théorème suivant.

THÉORÈME 4. — *Soit $\mathfrak{U}$ un anneau intégralement clos (dans son corps des fractions) et soit Ω/k une extension algébrique du corps k. Pour qu'un élément $\alpha \in \Omega$ soit entier sur $\mathfrak{U}$, il faut et il suffit que tous les coefficients de son polynôme minimal appartiennent à $\mathfrak{U}$.*

EXERCICES

1. Un idéal A d'un anneau $\mathfrak{D}$ est dit maximal si $A \neq \mathfrak{D}$ et si tout idéal B contenant A (i. e. tel que $A \subset B \subset \mathfrak{D}$) coïncide soit avec A soit avec $\mathfrak{D}$. Démontrer qu'un idéal A est maximal si et seulement l'anneau quotient $\mathfrak{D}/A$ est un corps.

2. Démontrer que si un anneau $\mathfrak{O}$ est intégralement clos, alors l'anneau $\mathfrak{O}[t]$ des polynômes à coefficients dans $\mathfrak{O}$ est aussi intégralement clos.

§ 5. — CARACTÈRES

Dans ce paragraphe, nous exposerons quelques notions relatives aux caractères des groupes abéliens finis et aux caractères modulaires.

1) Structure des groupes abéliens finis

La structure des groupes abéliens finis quelconques est décrite par le théorème suivant (cf. par exemple M. Hall, *Theory of groups*, New York, The MacMillan Company, 1959).

THÉORÈME 1. — *Tout groupe abélien fini peut se représenter comme produit direct de sous-groupes cycliques.*

En accord avec les exercices 1 et 2, un groupe cyclique fini n'est pas décomposable en produit direct de sous-groupes propres si et seulement si son ordre est une puissance d'un nombre premier. Par suite, si dans la décomposition d'un groupe abélien fini quelconque G en produit direct,

$$G = A_1 \times \ldots \times A_s$$

les facteurs cycliques A_i ne sont pas décomposables, alors leurs ordres sont des puissances de nombres premiers. La décomposition du groupe G en produit direct n'est pas définie de manière unique par ses facteurs non décomposables. Cependant, l'ensemble des ordres des facteurs non décomposables A_i est défini de manière unique par le groupe G. Ces ordres, qui sont des puissances de nombres premiers, s'appellent les *invariants* du groupe abélien fini. Le produit de tous les invariants d'un groupe donné est égal à son ordre.

2) Caractères des groupes abéliens finis

DÉFINITION. — *On appelle caractère d'un groupe abélien fini* G *tout homomorphisme de* G *dans le groupe multiplicatif du corps des nombres complexes.*

Autrement dit, un caractère du groupe G est une fonction χ sur G, à valeurs complexes, ne s'annulant pas, et telle que

$$\chi(xy) = \chi(x)\chi(y) \tag{1}$$

pour $x, y \in G$.

Puisque pour tout homomorphisme de groupe, l'élément unité a pour image l'unité, alors $\chi(1) = 1$; si l'élément $x \in G$ est d'ordre k, alors

$$(\chi(x))^k = \chi(x^k) = 1, \tag{2}$$

i. e. $\chi(x)$ est une racine $k^{\text{ième}}$ de 1. Si m est le plus grand des ordres des éléments du groupe G, alors, d'après l'exercice 3, l'ordre de tout élément de G est un diviseur de m. Toute valeur $\chi(x)$ est donc une racine d'ordre m de 1 et par suite on peut définir les caractères comme les homomorphismes de G dans le groupe des racines $m^{\text{ièmes}}$ de 1.

Représentons le groupe G comme un produit direct de sous-groupes cycliques :

$$G = \{a_1\} \times \ldots \times \{a_s\}.$$

Puisque tout élément $x \in G$ peut s'écrire sous la forme

$$x = a_1^{k_1} \ldots a_s^{k_s}, \tag{3}$$

alors, d'après (1),

$$\chi(x) = \chi(a_1)^{k_1} \ldots \chi(a_s)^{k_s};$$

ainsi, le caractère χ est complètement déterminé par les valeurs $\chi(a_1), \ldots, \chi(a_s)$. Si a_i est d'ordre m_i, d'après (2), $\chi(a_i)$ est une racine d'ordre m_i de 1. Réciproquement, choisissons pour tout $i = 1, \ldots, s$ une racine quelconque ε_i d'ordre m_i de 1 et pour tout élément $x \in G$ représenté sous la forme (3), posons

$$\chi(x) = \varepsilon_1^{k_1} \ldots \varepsilon_s^{k_s}. \tag{4}$$

Il est facile de voir que la valeur (4) ne dépend pas du choix des exposants k_i dans la décomposition (3) (chaque exposant k est défini modulo m_i) et que la fonction χ ainsi définie sur G satisfait à la condition (1) et par suite est un caractère du groupe G. On peut choisir la racine ε_i de m_i manières et par suite nous avons $m_1 \ldots m_s$ fonctions χ distinctes du type (4). Ceci démontre le théorème suivant.

THÉORÈME 2. — *Le nombre des caractères d'un groupe abélien fini est égal à son ordre.*

Définissons la multiplication des caractères. Pour deux caractères χ et χ' du groupe G, posons

$$(\chi\chi')(x) = \chi(x)\chi'(x), \qquad x \in G.$$

Il est évident que la fonction $\chi\chi'$ est encore un caractère du groupe G. Le caractère χ_0 tel que $\chi_0(x) = 1$ pour tout $x \in G$ est appelé *caractère unité*. Il est clair que $\chi\chi_0 = \chi$ pour tout caractère χ. Si pour tout caractère χ du groupe G nous posons

$$\bar{\chi}(x) = \overline{\chi(x)}, \qquad x \in G$$

($\overline{\chi(x)}$ est le nombre complexe conjugué de $\chi(x)$), alors la fonction $\bar{\chi}$ ainsi définie est un caractère du groupe G tel que $\chi\bar{\chi} = \chi_0$. Puisque la multiplication des caractères est associative, l'ensemble de tous les caractères forme un groupe pour la multiplication ci-dessus.

Soit $G = \{a\}$ un groupe cyclique d'ordre m et soit ε une racine primitive d'ordre m de 1 fixée. Désignons par χ le caractère du groupe G tel que

$$\chi(a) = \varepsilon \qquad (\text{d'où } \chi(a^k) = \varepsilon^k).$$

Puisque $\chi^r(a) = \varepsilon^r$, les caractères $\chi_0 = \chi^m$, χ, χ^2, $\ldots$, χ^{m-1} sont deux à deux distincts et par suite épuisent tout le groupe des caractères du groupe G. Ainsi, nous voyons que le groupe des caractères d'un groupe cyclique fini est aussi cyclique. Dans le cas général, on peut facilement démontrer le théorème suivant : *tout groupe abélien fini est isomorphe au groupe de ses caractères.*

Dans un groupe abélien G d'ordre n, considérons un sous-groupe H d'ordre m. Si on considère la restriction à H d'un caractère du groupe G,

il est clair que cette fonction est un caractère du groupe H; désignons-le par $\widehat{\chi}$. Il est clair que l'application $\chi \to \widehat{\chi}$ est un homomorphisme du groupe X des caractères du groupe G dans le groupe Y des caractères du sous-groupe H; soit A son noyau. Les caractères $\chi \in A$ sont caractérisés par le fait que $\chi(z) = 1$ pour tout $z \in H$. Si $\chi \in A$ et x, x' appartiennent à la même classe résiduelle de G selon H, il est clair que $\chi(x) = \chi(x')$. Posant $\bar{\chi}(\bar{x}) = \chi(x)$, $\chi \in A$ et $\bar{x}$ classe résiduelle de x dans G selon H, nous avons une fonction $\bar{\chi}$ sur le groupe quotient G/H et cette fonction est un caractère du groupe G/H. Réciproquement, si ξ est un caractère quelconque du groupe quotient G/H, posant

$$\chi(x) = \psi(\bar{x}), \qquad x \in G,$$

nous obtenons un caractère $\chi \in A$ tel que $\bar{\chi} = \psi$. Puisque par l'application $\chi \to \bar{\chi}$ ($\chi \in A$), à des caractères distincts de A correspondent des caractères distincts du groupe G/H, nous avons établi que le nombre de caractères χ de A est égal au nombre de caractères du groupe G/H, i. e. égal à $\frac{n}{m}$ (théorème 2). Mais, dans ce cas, l'image du groupe X par l'homomorphisme $\chi \to \widehat{\chi}$ (du groupe X dans le groupe Y) est d'ordre n : $\frac{n}{m} = m$ et puisque, d'après le théorème 2, le groupe Y est aussi d'ordre m, alors cette image est égale à Y. Cela signifie que tout caractère du groupe H est de la forme $\widehat{\chi}$ pour un certain caractère χ du groupe G. Il est clair que le nombre des caractères $\chi \in X$ qui induisent le même caractère sur H est égal à $\frac{m}{n} = (G : H)$. Ceci démontre le théorème suivant :

THÉORÈME 3. — *Soit* G *un groupe abélien fini et* H *un sous-groupe. Tout caractère du groupe* H *est prolongeable en un caractère du groupe* G *et le nombre de ces prolongements est égal à l'indice* (G : H).

COROLLAIRE 1. — *Si x est un élément de* G *différent de l'unité, il existe un caractère χ du groupe* G *tel que* $\chi(x) \neq 1$.

En effet, considérons le groupe cyclique $\{x\} = H$. Puisque son ordre est > 1, alors il existe un caractère χ' sur H différent du caractère unité et donc tel que $\chi'(x) \neq 1$. Prolongeant χ' en un caractère de groupe G, nous obtenons ainsi le caractère χ demandé.

COROLLAIRE 2. — *Si un élément $x \in G$ n'appartient pas à un sous-groupe* H, *alors il existe un caractère χ du groupe* G *tel que* $\chi(x) \neq 1$ *et* $\chi(z) = 1$ *pour tout* $z \in H$.

En effet, on peut prolonger le caractère unité du groupe H en un carac-

tère différent du caractère unité du sous-groupe $\{x, H\}$, qui se prolonge à son tour en un caractère du groupe G.

Établissons maintenant quelques relations. Si χ_0 est le caractère unité, alors $\chi_0(x) = 1$ pour tout $x \in G$ et par suite $\sum_{x\in G} \chi_0(x) = n$, où n est l'ordre du groupe G. Supposons que le caractère χ est différent de χ_0, i. e. $\chi(z) \neq 1$ pour un certain $z \in G$. Si x parcourt tous les éléments du groupe G, zx parcourt aussi tous les éléments de G; posant $S = \sum_{x\in G} \chi(x)$, nous aurons donc

$$S = \sum_{x\in G} \chi(zx) = \chi(z)S.$$

Puisque $\chi(z) \neq 1$, cette égalité n'est possible que si $S = 0$. Ainsi nous avons établi la formule :

$$\sum_{x\in G} \chi(x) = \begin{cases} n & \text{si} \quad \chi = \chi_0 \\ 0 & \text{si} \quad \chi \neq \chi_0. \end{cases} \tag{5}$$

La valeur de chaque caractère sur l'élément unité du groupe est égale à 1 et par suite $\sum_{\chi} \chi(1) = n$ (χ parcourt ici tous les caractères du groupe G). Posons $T = \sum_{\chi} \chi(x)$. D'après le corollaire 1 du théorème 3, il existe un caractère χ' tel que $\chi'(x) \neq 1$ (si $x \neq 1$). Le produit $\chi'\chi$ parcourt en même temps que χ tous les caractères du groupe G, d'où

$$T = \sum_{\chi} (\chi'\chi)(x) = \sum_{\chi} \chi'(x)\,\chi(x) = \chi'(x)T,$$

et puisque $\chi'(x) \neq 1$, on a $T = 0$. On a donc établi la formule

$$\sum_{\chi} \chi(x) = \begin{cases} n & \text{si} \quad x = 1, \\ 0 & \text{si} \quad x \neq 1. \end{cases} \tag{6}$$

3) Caractères modulaires

Pour tout nombre entier naturel m, désignons par G_m le groupe multiplicatif des classes résiduelles modulo m des entiers rationnels relativement premiers avec m. Nous désignerons par $\bar{a}$ la classe résiduelle de a modulo m.

A tout caractère χ du groupe G_m, nous pouvons associer la fonction χ^* définie sur l'ensemble des nombres a premiers avec m par la formule

$$\chi^*(a) = \chi(\bar{a}).$$

Prolongeons cette fonction χ^* à l'ensemble de tous les entiers rationnels en posant $\chi^*(a) = 0$ si a et m ne sont pas premiers entre eux. La fonction χ^* ainsi définie (sur l'ensemble des entiers rationnels) est appelée un *caractère modulaire* modulo m. Dans la suite, nous désignerons χ^* par la même lettre χ que le caractère du groupe G_m qui l'engendre. Il est clair que des caractères distincts du groupe G_m engendrent des caractères modulaires distincts et par suite le nombre de caractères modulaires modulo m est égal à $\varphi(m)$.

De cette définition découlent facilement les propriétés suivantes des caractères modulaires :

1° pour tout entier rationnel a, la valeur $\chi(a)$ est un nombre complexe et $\chi(a) \neq 0$ si et seulement si a est relativement premier avec m;

2° si $a \equiv a'$ (mod m), alors $\chi(a) = \chi(a')$;

3° pour tout couple d'entiers rationnels a et b, on a $\chi(ab) = \chi(a)\,\chi(b)$.

Montrons que les caractères modulaires sont entièrement caractérisés par ces trois propriétés. En effet, soit η une fonction satisfaisant aux conditions 1°, 2° et 3°. Pour toute classe $\bar{a} \in G_m$, $(a, m) = 1$, posons $\chi(\bar{a}) = \eta(a)$; d'après 2°, la valeur $\chi(\bar{a})$ ne dépend pas du choix du représentant a et est différente de 0 d'après 1°. En outre, si $(a, m) = 1$ et $(b, m) = 1$, on a, d'après la condition 3°,

$$\chi(\bar{a}\bar{b}) = \chi(\overline{ab}) = \eta(ab) = \eta(a) \quad \eta(b) = \chi(\bar{a}) \quad \chi(\bar{b}).$$

Ainsi, χ est un caractère du groupe G_m et le caractère χ^* qu'il engendre coïncide avec la fonction η.

Soit m' un entier naturel divisible par m. Nous pouvons associer à tout caractère χ modulo m un certain caractère χ' modulo m' : si a est relativement premier à m' (et par suite aussi à m), posons $\chi'(a) = \chi(a)$; si $(a, m') > 1$, posons $\chi'(a) = 0$. La fonction numérique χ' satisfait aux trois conditions 1°, 2° et 3° et par suite est un caractère modulaire modulo m'. Nous dirons que le caractère χ' est induit par le caractère χ.

DÉFINITION. — *Soit χ un caractère modulaire modulo m. S'il existe un diviseur propre d du nombre m et un caractère χ_1 modulo d qui induit χ, on dit que le caractère χ est non primitif. Dans le cas contraire, il est dit primitif.*

THÉORÈME 4. — *Pour qu'un caractère χ modulo m soit primitif, il faut et il suffit que pour tout diviseur propre d du nombre m il existe un nombre x, $x \equiv 1$ (mod d), $(x, m) = 1$ tel que $\chi(x) \neq 1$.*

DÉMONSTRATION. — Si le caractère χ est non primitif, il est induit par un caractère χ_1 modulo d, où d est un diviseur propre de m. Ainsi, pour tout x relativement premier avec m, on a $\chi(x) = \chi_1(x)$; si de plus $x \equiv 1$ (mod d), alors $\chi(x) = \chi_1(x) = 1$. Réciproquement, supposons que pour un certain

diviseur propre d du nombre m on ait $\chi(x) = 1$ pour tout x tel que $x \equiv 1 \pmod{d}$ et $(x, m) = 1$. Pour tout a relativement premier à d, on peut trouver a' tel que $(a', m) = 1$ et $a' \equiv a \pmod{d}$. Posons

$$\chi_1(a) = \chi(a').$$

La valeur $\chi_1(a)$ est indépendante du choix de a'. En effet, si $a' \equiv a'' \pmod{d}$, $(a'', m) = 1$, alors $a'' \equiv xa' \pmod{m}$ pour un certain x relativement premier avec m. Puisque $x \equiv 1 \pmod{d}$, on a donc par hypothèse $\chi(x) = 1$, d'où $\chi(a'') = \chi(x)\ \chi(a') = \chi(a')$. Posant de plus $\chi_1(a) = 0$ si $(a, d) \neq 1$, nous obtenons une fonction numérique χ_1 qui est un caractère modulaire modulo d. Puisque $\chi_1(a) = \chi(a)$ pour $(a, m) = 1$, χ est induit par le caractère χ_1. Cela termine la démonstration du théorème 4.

EXERCICES

1. Montrer qu'un groupe cyclique fini dont l'ordre est une puissance d'un nombre premier n'est pas décomposable en produit direct de sous-groupes propres.

2. Supposons que l'ordre d'un groupe cyclique fini G est égal au produit de deux nombres premiers k et l. Montrons qu'on peut représenter G comme produit direct de deux sous-groupes cycliques d'ordre k et l.

3. Soit a un élément d'ordre maximum d'un groupe abélien fini G. Démontrer que le sous-groupe cyclique $\{ a \}$ est facteur direct dans G.

4. Soit k un entier naturel. Démontrer qu'un élément x d'un groupe abélien fini G est la puissance $k^{\text{ième}}$ d'un élément de G si et seulement si on a $\chi(x) = 0$ pour tout caractère χ du groupe G tel que $\chi^k = \chi_0$ (χ_0 est le caractère unité).

5. Soit G un groupe abélien fini d'ordre n. Numérotons ses éléments $x_1, \ldots, x_n$ et ses caractères $\chi_1, \ldots, \chi_n$. Démontrer que la matrice

$$\left(\frac{1}{n}\chi_i(x_j)\right)_{i,j}$$

est unitaire.

6. Soient $m_1, \ldots, m_k$ des entiers naturels premiers deux à deux et $m = m_1 \ldots m_k$. Démontrer que pour tout caractère χ modulo m il existe des caractères χ_i modulo m_i ($i = 1, \ldots, k$), définis de manière unique, tels que pour tout entier rationnel a on ait l'égalité

$$\chi(a) = \chi_1(a) \ldots \chi_k(a).$$

(Pour tout i le caractère χ_i est défini par l'égalité $\chi_i(a) = \chi(a')$, où a' est défini par les congruences

$$a' \equiv a \pmod{m_i}, \qquad a' \equiv 1 \left(\mod \frac{m}{m_i}\right).$$

7. Sous les hypothèses de l'exercice 6, montrer que si le caractère χ modulo m est primitif, alors, pour tout $i = 1, \ldots, k$, le caractère χ_i modulo m_i est aussi primitif.

8. Soient d_1 et d_2 des diviseurs d'un nombre entier naturel m et $d = d_1 d_2$. Démontrer que si un caractère χ modulo m est induit par un certain caractère modulo d_1 et est induit par un certain caractère modulo d_2, alors il est induit aussi par un caractère modulo d.

9. Montrer que tout caractère χ modulo m est induit par un caractère primitif modulo f, défini de manière unique (f est un diviseur de m). Le nombre f est appelé le *conducteur* du caractère χ.

10. Démontrer que le nombre des caractères primitifs modulo m est égal à

$$\sum_{d|m} \mu(d)\varphi\left(\frac{m}{d}\right)$$

(d parcourt tous les diviseurs du nombre m; μ est la fonction de Moëbius; φ est la fonction d'Euler).

11. Démontrer qu'il existe des caractères primitifs modulo m si et seulement si m est soit impair soit divisible par 4.

12. Soit $\mathcal{F}$ l'espace vectoriel sur le corps des nombres complexes formé des fonctions f définies sur un groupe abélien G, à valeurs complexes $f(\sigma)$, $\sigma \in G$. Pour tout élément $\omega \in G$, désignons par T_ω l'opérateur de translation défini par la formule $(T_\omega f)(\sigma) = f(\omega\sigma)$. Démontrer que tous les caractères χ du groupe G sont des vecteurs propres des opérateurs T_ω. Quelles sont les valeurs propres correspondantes ?

13. Conservant les notations de l'exercice précédent, considérons, pour une fonction fixée $f \in \mathcal{F}$, la matrice carrée

$$A = (f(\sigma\tau^{-1}))_{\sigma,\tau},$$

où σ et τ parcourent tous les éléments du groupe G disposés dans un certain ordre. Démontrer que le déterminant de cette matrice est égal à

$$\prod_{\chi}\left(\sum_{\sigma} f(\sigma)\chi(\sigma)\right)$$

(σ parcourt tous les éléments et χ tous les caractères du groupe G).

Indication. — La matrice A est la matrice de l'opérateur

$$T = \sum_{\omega} f(\omega)T_\omega$$

par rapport à la base formée par les fonctions L_σ telles que

$$L_\sigma(\tau) = \begin{cases} 1 & \text{pour} \quad \sigma = \tau \\ 0 & \text{pour} \quad \sigma \neq \tau. \end{cases}$$

Trouver les valeurs propres de l'opérateur T.

14. Démontrer la formule de l'exercice 13 en considérant le déterminant du produit de la matrice $(\chi(\sigma))_{\chi,\sigma}$ par la matrice A.

TABLE DES MATIÈRES