6. Formes quadratiques

Cette théorie étudie l'arithmétique et l'algèbre des entiers définis à l'addition près d'un multiple d'un entier fixe p; les relations obtenues sont appelées *congruences* suivant le module p. Les entiers, ainsi définis, ne déterminent qu'un nombre fini d'êtres, encore appelées classes de congruence.

Si l'entier p (caractéristique) est premier, l'ensemble des classes forme un corps, c'est-à-dire que les 4 opérations élémentaires sont possibles. Mais le polynome $x^{p-1}-1$ est nul pour toute valeur x du corps, sans être identiquement nul; plus généralement un polynome $F(x^p)$ peut être irréductible et n'avoir que des racines multiples.

Dans une note assez brève, E. Galois complète ces résultats par l'introduction d'imaginaires. Il considère des êtres $f(i)$, définis suivant 2 modules p et $\varphi(i)$, où φ est un polynome irréductible de degré f. Il obtient ainsi p^f êtres, ou imaginaires de Galois; toute équation de degré f à cœfficients rationnels est décomposable.

Dickson a montré que les ensembles d'imaginaires de Galois forment tous les *corps* qui ne contiennent qu'un *nombre fini d'éléments* (corps finis). L'étude de ces corps est indispensable pour la résolution des équations diophantiennes.

Hensel a introduit des corps (infinis) — les corps locaux ou p-adiques — qui permettent d'utiliser les propriétés des congruences suivant les modules puissances de nombres premiers. Un tel corps est constitué par les séries formelles $(a_0+a_1p+\ldots)$, où les a_i sont des entiers définis au module p près.

Bibliographie: 2, 3, 9, 12, 13, 14, 15, 18, 27, 30, 37.

6. Formes quadratiques

L'équation congruentielle:

$$x^2-q \equiv 0 \ (mod.\ p)$$

a été particulièrement étudiée à 2 points de vue différents: p étant donné, trouver les q (appelés restes quadratiques mod. p); q étant donné, trouvé les p.

La loi de réciprocité quadratique de GAUSS lie ces 2 points de vue.

Mais les diviseurs p de x^2-q sont les mêmes que ceux de x^2-qy^2 (si ces diviseurs p sont sans facteurs carrés et premiers à q); cette dernière expression est un cas particulier d'une *forme quadratique binaire*

$$ax^2+bxy+cy^2.$$

L'étude des formes quadratiques binaires a été débutée par GAUSS et continuée par HERMITE. On appelle formes *équivalentes* celles qui représentent les mêmes nombres; elles peuvent être déduites les unes des autres par des substitutions unimodulaires. Dans chaque classe de formes équivalentes, on cherche des formes *réduites*. Ces problèmes sont liés, en analyse, à l'étude des fonctions fuchsiennes.

L'étude des formes quadratiques à 3, 4, ... variables a donné lieu à de nombreux travaux, mais pose encore des problèmes importants. L'étude des formes de degré supérieur est seulement ébauchée.

L'étude des formes quadratiques binaires a été partiellement abandonnée et remplacée par celle des corps quadratiques, grâce à la relation:

$$ax^2+bxy+cy^2 = (\alpha x+\beta y)(\alpha' x+\beta' y)$$

avec α, β nombres quadratiques.

Bibliographie: 15, 18, 21, 30, 34, 43.

7. APPROXIMATIONS DIOPHANTIENNES

Etant donné un nombre rationnel ou irrationnel, on peut chercher les fractions rationnelles à termes simples qui en diffèrent peu; c'est le problème des approximations diophantiennes.

La seule solution entièrement satisfaisante est celle des *fractions continues*. Il est remarquable qu'elle soit liée à la théorie des formes quadratiques binaires, du développement pé:iodique des irrationnelles du second degré et aux substitutions unimodulaires.