

Bulletin de l'Association des Professeurs de Mathématiques de l'Enseignement Public

I. ÉTUDES

ANNEAUX, CONGRUENCES, IDÉAUX *

1. Rappel de définitions et de quelques propriétés simples

Nous donnerons le nom d'*anneau* à tout ensemble A d'éléments $a, b, \dots$ sur lesquels sont définies deux opérations ou lois de composition internes, nommées *addition* et *multiplication*, représentées par les notations habituelles et soumises aux axiomes suivants :

I. A est un *groupe abélien par rapport à l'addition*, c'est-à-dire l'addition est *associative* : $a + (b + c) = (a + b) + c$, *commutative* : $a + b = b + a$ (propriété exprimée par le mot « abélien ») ; il existe un *élément neutre* appelé *zéro* et désigné par 0 : $a + 0 = a$, et, pour tout élément a un *élément opposé* $-a$: $a + (-a) = 0$ (ce qui s'écrit plus brièvement : $a - a = 0$).

II. La *multiplication* est *associative* : $a(bc) = (ab)c$.

III. La *multiplication* est *distributive* par rapport à l'addition :

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca.$$

Ces différentes propriétés sont, bien entendu, supposées vraies, quels que soient a, b, c dans A .

Si la multiplication est commutative, l'anneau est dit *commutatif*. C'est essentiellement aux anneaux commutatifs que nous nous intéresserons aujourd'hui.

Dans les axiomes définissant un anneau, nous n'avons pas fait figurer l'existence d'un *élément-unité* e ou 1 (élément-neutre pour la multiplication : $ea = ae = a$, quel que soit $a \in A$) (1). Si un tel élément existe, A est dit *anneau avec élément-unité*. Dans un anneau qui se composerait

(*) Conférence prononcée le 15 mars 1956 à l'Institut Henri-Poincaré, seconde conférence du cycle sur l'Algèbre organisé par la Société Mathématique de France, en accord avec l'A.P.M., à l'intention spéciale des professeurs de Mathématiques.

(1) Cette définition diffère donc, sur ce point, de celle qui a été donnée par Henri Cartan dans sa conférence sur les structures algébriques, et est un peu plus générale. C'est d'ailleurs la définition classique, voir par exemple [3], p. 35 et 38, [1], p. 115, [2], p. 138 ; les numéros entre crochets renvoient à la bibliographie placée à la fin de l'article.

du seul élément zéro, zéro serait élément-unité (pour la multiplication), mais on exclut généralement ce cas quand on parle d'un anneau avec élément-unité.

On voit immédiatement que, dans tout anneau A , la multiplication est distributive par rapport à la soustraction et que 0 est élément permis : $0 \cdot a = a \cdot 0 = 0$ (quel que soit $a \in A$). *Un produit est nul dès qu'au moins un des facteurs l'est.* Cette condition suffisante n'est nécessaire que dans des anneaux particuliers : nous rencontrerons des anneaux très simples où des éléments différents de zéro peuvent avoir un produit nul.

Un anneau K ayant plus d'un élément, $K \neq \{0\}$, ne peut jamais être un groupe par rapport à la multiplication ; cette propriété est en effet incompatible avec :

$$a \neq 0, \quad a \cdot 0 = 0 \cdot 0 (= 0).$$

Mais il peut arriver que $K - \{0\}$ soit un groupe par rapport à la multiplication (c'est-à-dire que le produit, dans K , de deux éléments non nuls soit différent de zéro, qu'il existe un élément-unité e et que tout $a \neq 0$ admette un inverse a^{-1} : $aa^{-1} = a^{-1}a = e$). On dit alors que K est un *corps*.

2. Exemples

L'ensemble $C = \{\dots, -m, \dots, -1, 0, 1, 2, \dots, n, \dots\}$ des entiers relatifs (c'est-à-dire ≥ 0) est un anneau ; il en est de même de l'ensemble des entiers relatifs pairs, puisque nous ne nous bornons pas à considérer des anneaux avec élément-unité.

L'ensemble des nombres rationnels Γ , celui des nombres réels P , celui des nombres complexes Ω sont des corps (contenant C). L'ensemble Σ des *nombres algébriques*, c'est-à-dire des nombres (réels ou complexes), solutions d'équations algébriques à coefficients rationnels ou, ce qui revient au même, à coefficients entiers, est également un corps (2).

Étant donné un anneau A , par exemple l'un des précédents, on sait définir (3) l'anneau $A[X]$ des *polynômes* en X à coefficients dans A , puis l'anneau $A[X][Y]$ des polynômes en Y ayant leurs coefficients dans

$A[X]$; ces polynômes s'écrivent $\sum_{ij} a_{ij} X^i Y^j$, $a_{ij} \in A$ (avec, dans cha-

que somme, seulement un nombre fini de coefficients a_{ij} non nuls), la symétrie en X et Y est évidente, et nous avons là ce qu'on appelle l'anneau des polynômes en X et Y à coefficients dans A , désigné par la notation $A[X, Y]$. De proche en proche, on définit l'anneau $A[X_1, \dots, X_n]$ des polynômes en n indéterminées $X_1, \dots, X_n$ à coefficients dans A .

Un autre exemple important d'anneau est celui des *entiers modulo m* , m étant un entier donné (cf. *Structures algébriques*, § 8). Il est

(2) Cette proposition peut se rattacher facilement à la théorie des fonctions symétriques. Voir par exemple [2], chapitre VII, p. 396.

(3) Voir la conférence sur les Structures algébriques, par Henri Cartan. La lettre X , « pur symbole », reçoit aussi le nom d'*indéterminée* et joue le rôle de générateur d'un demi-groupe cyclique, [3], p. 50, [2], p. 326. Dans un anneau avec élément-unité, c'est un polynôme particulier ($a_1 = e$, $a_i = 0$ pour $i \neq 1$).

défini à partir de la congruence arithmétique R par rapport au module m , avec laquelle l'addition et la multiplication sont compatibles (nous dirons aussi, dans le même sens, que cette congruence est une relation d'équivalence *régulière* par rapport à l'addition et à la multiplication de l'anneau C des entiers) : c'est l'ensemble-quotient C/R ou $C/(m)$ de C par cette équivalence, et on peut le représenter par l'ensemble $\{0, 1, \dots, m-1\}$ des m restes possibles dans la division par m . Les tables d'addition et de multiplication, faciles à construire pour chaque valeur numérique de m , font apparaître une possibilité remarquable. Pour $m=4$, on a : $2 \cdot 2 = 0$; pour $m=6$, on a : $2 \cdot 3 = 0$. D'une façon générale, toutes les fois que le module m n'est pas premier, $C/(m)$ n'est pas un domaine (ou anneau) d'intégrité ; $C/(p)$, au contraire, pour p premier, en est un ; c'est même un corps (nous y reviendrons dans un instant).

Dans le corps Ω des nombres complexes, portons notre attention sur les nombres de la forme $\alpha + \beta i$ où α et β sont *rationnels* : $\alpha, \beta \in \Gamma$. L'ensemble de ces nombres est, visiblement, un corps, désigné par $\Gamma(i)$. Cette notation exprime que c'est le plus petit sous-corps de Ω contenant à la fois le corps Γ et le nombre i ; on dit qu'il se déduit de Γ par l'*adjonction* de i . On peut, sans utiliser Ω , construire directement ce corps $\Gamma(i)$ à partir de Γ , par la méthode suivante, qui est un cas particulier de l'*adjonction symbolique* que nous étudierons plus loin.

Dans l'anneau de polynômes $\Gamma[x]$, considérons le polynôme $x^2 + 1$ et faisons-lui jouer le rôle que jouait plus haut, dans l'anneau C des entiers, le module m ; soit donc R la relation entre deux polynômes $\varphi(x), \psi(x)$ de $\Gamma[x]$ vérifiée si, et seulement si, $\varphi - \psi$ est un multiple de $x^2 + 1$. R est une relation d'équivalence, régulière par rapport à l'addition et à la multiplication des polynômes. Les classes de polynômes équivalents s'ajoutent et se multiplient comme les polynômes qu'elles contiennent, donc forment un *anneau*, appelé anneau quotient, ou anneau des classes résiduelles, et désigné par $\Gamma[x]/R$ ou $\Gamma[x]/(x^2 + 1)$. Les différents éléments de Γ appartiennent à des classes différentes, avec lesquelles on peut les identifier. Chaque classe contient un polynôme du premier degré, $\alpha x + \beta$, reste commun de la division des différents polynômes de la classe par $x^2 + 1$; et si l'on désigne par i la classe contenant le polynôme x , la classe contenant $\alpha x + \beta$ est $\alpha i + \beta$ (en raison de la régularité). Comme $x^2 + 1$ et 0 sont deux polynômes équivalents, on a : $i^2 + 1 = 0$. Enfin, si α et β ne sont pas tous deux nuls, $\alpha + \beta i (\neq 0)$ a l'inverse : $\alpha - \beta i$

— ; notre anneau quotient est bien un *corps* contenant Γ et un élément i solution de l'équation $x^2 + 1 = 0$ (et il n'existe visiblement pas de corps plus petit ayant ces propriétés).

En remplaçant le corps des rationnels Γ par le corps des réels P , on construit le corps des nombres complexes $\Omega = P(i)$ par cette méthode purement algébrique, qui remonte à Cauchy. On peut aussi remplacer -1 par un entier d non carré parfait et construire, toujours par cette méthode, les corps $\Gamma(\sqrt{d}) = \Gamma[x]/x^2 - d$, en particulier définir par un

procédé purement algébrique des nombres irrationnels de la forme $\sqrt{d}$. Nous verrons plus loin comment la méthode, sous le nom d'adjonction symbolique, s'étend à la définition de nombres algébriques quelconques. Dès maintenant, notons l'importance des *relations d'équivalence régulières par rapport à l'addition et à la multiplication dans un anneau* : pour simplifier le langage et rappeler l'origine arithmétique de la notion, nous leur donnerons le nom de *congruences*.

Dans un des corps $\Gamma(\sqrt{d})$ ainsi construits, on voit apparaître un anneau simple et remarquable : celui des nombres $a + b\sqrt{d}$, où a, b sont des entiers (relatifs) : $a, b \in \mathbb{C}$. En particulier, les nombres $a + bi$ sont les *entiers de Gauss* ; l'anneau qu'ils constituent est représenté par le « réseau des points entiers » du plan, c'est-à-dire des points à coordonnées entières.

Bien que nous nous limitons aux anneaux commutatifs, mentionnons que les matrices carrées d'ordre n (avec les règles classiques d'addition et de multiplication), à éléments dans un anneau A (qui peut en particulier être un corps), forment un anneau (non commutatif pour $n > 1$).

3. Domaines d'intégrité

Un domaine (ou anneau) d'intégrité est, rappelons-le, un anneau commutatif D dans lequel un produit xy ne peut être nul que si l'un au moins des facteurs x, y est nul. Autrement dit : *deux éléments de $D - \{0\}$ ont leur produit dans $D - \{0\}$* , $D - \{0\}$ est « *multiplicativement fermé* ». En outre, $ab = ac$ et $a \neq 0$ entraînent $b = c$; toute égalité de la forme $ab = ac$ dans $D - \{0\}$ peut être *simplifiée*. Si $D - \{0\}$ est fini et si l'on écrit sa table de multiplication, on voit qu'un élément figure au plus une fois dans chaque ligne ou chaque colonne, donc exactement une fois ; cela signifie que l'équation $ax = b$ a toujours une solution, ce qui entraîne que $D - \{0\}$ est un groupe multiplicatif (abélien bien entendu) : D est donc un corps : *tout domaine d'intégrité fini est un corps*. Tel est le cas pour $\mathbb{C}/(p)$, p premier.

Si D est un domaine d'intégrité non fini, la considération des fractions (a, b) ou $\frac{a}{b}$ ($a, b \in D, b \neq 0$) permet de construire un corps (minimum) contenant D et appelé *corps des quotients* du domaine d'intégrité D : les éléments de ce corps sont les classes de fractions équivalentes (4).

(4) Voir la conférence sur les structures algébriques, par Henri Cartan, § 7 et 8. L'existence d'un élément-unité dans D n'est pas nécessaire (on considérera les fractions $\frac{m}{m}$ au lieu de $\frac{1}{1}$, $\frac{am}{m}$ au lieu de $\frac{a}{1}$). La construction du corps des quotients d'un domaine d'intégrité dérive de la construction, plus simple, du plus petit groupe contenant un *semi-groupe abélien* donné S (c'est-à-dire un ensemble S muni d'une opération associative, commutative et satisfaisant à la règle de simplification : $ab = ac$ entraîne $b = c$, dans la notation multiplicative). Cette dernière construction a l'intérêt de s'appliquer aussi bien à la définition des entiers relatifs à partir des entiers naturels, ou des nombres réels de signe quelconque à partir des nombres réels positifs, l'opération considérée étant alors l'addition. Voir [2], chap. V, § 2 et 3, p. 224 (on peut, très facilement, éviter l'utilisation du § 1).

Soit K un corps (commutatif) ; si $x, y \in K$ et si l'on a $xy = 0$, $x \neq 0$, x admet dans K un inverse x^{-1} et on a :

$$0 = x^{-1}(xy) = (x^{-1}x)y = y.$$

Par suite, *tout anneau contenu dans K , en particulier le corps K lui-même, est un domaine d'intégrité.*

Si l'on considère l'anneau de polynômes $D[x]$, où D est un domaine d'intégrité, le produit d'un polynôme $f(X) = a_0 + a_1X + \dots + a_nX^n$ de degré n ($a_n \neq 0$) par un polynôme $g(X) = b_0 + b_1X + \dots + b_pX^p$ de degré p ($b_p \neq 0$) est un polynôme $a_0b_0 + \dots + a_nb_pX^{n+p}$ de degré $n+p$ exactement, puisque a_nb_p est différent de 0. Si A est un anneau quelconque, dans l'anneau $A[n]$, le produit d'un polynôme de degré n par un polynôme de degré p est *au plus* de degré $n+p$; et si A n'est pas un domaine d'intégrité, il existe effectivement des cas où le degré du produit s'abaisse. Autre accident très remarquable, quand A n'est pas un domaine d'intégrité : on ne peut plus affirmer qu'un polynôme $f(x) \in A[x]$, nul pour $x = a$ et $x = b$, $a, b \in A$, $b \neq a$, est divisible par $(x - a)(x - b)$; et un polynôme $f(x)$ de degré n peut très bien s'annuler pour plus de n valeurs distinctes de x : ainsi, prenons $A = \mathbb{C}/(4)$; le polynôme $2x$, du premier degré, s'annule pour $x = 0$ et $x = 2$.

4. Caractéristique

Soit A un anneau, possédant un élément-unité e . Soit n un entier relatif. Si n est positif et si $x \in A$, on pose :

$$nx = x + \dots + x \quad (n \text{ fois}).$$

Si $n = 0$ ($\in \mathbb{C}$), on pose $0x = 0$ ($\in A$). Si n est négatif, on pose :

$$nx = -(|n|x).$$

Puisque $x = ex$, on a :

$$nx = (ne)x.$$

Si donc il existe des entiers n non nuls tels que :

$$(1) \quad ne = 0$$

on aura :

$$nx = 0 \quad \text{pour tout } x \in A.$$

Parmi de tels entiers, il y en a de positifs, et, parmi ceux-ci, il y en a un plus petit que tous les autres, soit n_0 ; on dit, dans ce cas, que l'anneau A est de caractéristique n_0 .

S'il n'existe aucun entier n vérifiant l'équation (1), A est dit de caractéristique nulle (parce que 0 est le seul entier tel que $0e = 0$, $0x = 0$ pour tout $x \in A$).

La caractéristique d'un domaine d'intégrité D est ou bien 0, ou bien un nombre premier p . Si l'on avait en effet $n_0 = n'_0n''_0$ avec $n'_0, n''_0 \neq 0, 1$, on aurait $n'_0e = a \neq 0$, $n''_0e = b \neq 0$, et $ab = n_0e = 0$, D ne serait pas un domaine d'intégrité.

Notons bien que ce qu'on appelle dans l'enseignement, à tort je crois, les « règles du calcul algébrique » sont les règles de calcul valables dans les domaines d'intégrité de caractéristique nulle.

Examinons quelques particularités intéressantes dans les domaines d'intégrité de caractéristique $p \neq 0$.

Dans tout anneau commutatif, la formule du binôme :

$$(a + b)^n = a^n + C_n^1 a^{n-1} b + \dots + C_n^k a^{n-k} b^k + \dots + b^n$$

$$\text{avec : } C_n^k = \frac{n(n-1) \dots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

est valable. [Dans un anneau non commutatif, on peut seulement écrire par exemple : $(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2$].

Prenons, dans la formule du binôme $n = p$, caractéristique du domaine D considéré : pour $k \neq 0, p$, C_p^k est multiple de p , on a donc :

$$(a + b)^p = a^p + b^p.$$

En remplaçant a par $a - b$, il vient :

$$(a - b)^p = a^p - b^p.$$

Ces formules entraînent, de proche en proche :

$$(a_1 + \dots + a_r)^p = a_1^p + \dots + a_r^p$$

$$(a + b)^{p^f} = a^{p^f} + b^{p^f} \quad (\text{quel que soit l'entier naturel } f).$$

$$(a - b)^{p^f} = a^{p^f} - b^{p^f}$$

En supposant que D possède un élément-unité e , en prenant $a_1 = a_2 = \dots = a_r = e$ et en écrivant r pour re , il vient :

$$r^p = r,$$

quel que soit l'entier naturel r .

Cette relation est valable en particulier dans le corps des entiers modulo p , $C/(p)$. En revenant à l'anneau des entiers C , on voit qu'on a, pour tout nombre naturel x :

$$x^p \equiv x \quad (p)$$

(théorème de Fermat).

A étant un anneau commutatif quelconque, on peut définir d'une façon purement algébrique, dans l'anneau de polynômes $A[x]$, la dérivée d'un polynôme $f(x)$ comme le coefficient de h dans $f(x + h)$ ordonné suivant les puissances de h :

$$f(x + h) = f(x) + hf'(x) + h^2(\dots), \quad f(x + h) \in A[x, h].$$

Les règles de calcul des dérivées s'obtiennent aisément ; si

$$f(x) = a_n x^n + \dots + a_1 x + a_0,$$

on a :

$$f'(x) = na_n x^{n-1} + \dots + a_1$$

et $f'(x)$ est de degré $n - 1$ au plus ; exactement de degré $n - 1$ lorsque A est un anneau de caractéristique 0, mais, dans le cas contraire, le degré de f' est certainement inférieur à n si A est de caractéristique n_0 et si n est multiple de n_0 . En particulier, si A est un domaine d'intégrité avec élément-unité ou un corps de caractéristique p , tout polynôme en x^p :

$$f(x) = a_r x^{pr} + \dots + a_1 x^p + a_0$$

a une dérivée nulle (au sens de « identiquement nulle »). Cette circonstance, on le conçoit, n'est pas sans apporter des perturbations notables dans la théorie des équations algébriques ; si l'on prend pour A certains corps de caractéristique p , elle n'est pas incompatible avec l'irréductibi-

lité de $f(x)$ dans $A[x]$. Exemple (5) : A est le corps $k(t)$ des fractions rationnelles d'une indéterminée t à coefficients dans le corps $k = C/(p)$; et $f(x) = x^p - t$.

5. Idéaux

Dans un anneau commutatif A , soit R une congruence (c'est-à-dire une relation d'équivalence régulière pour l'addition et la multiplication de A). L'ensemble des classe d'équivalence ou ensemble quotient A/R est, comme on l'a vu dans la conférence sur les structures algébriques, un anneau, désignons-le plus simplement par $\bar{A}$. Soit $\bar{x}$ la classe contenant l'élément x de A . L'application $x \rightarrow \bar{x}$ est une application de A sur $\bar{A}$ (tout élément $\bar{x}$ de $\bar{A}$ est obtenu comme image d'au moins un élément de A) ; de plus, elle respecte l'addition et la multiplication des anneaux $A, \bar{A}$, c'est-à-dire :

$$\overline{x + y} = \bar{x} + \bar{y} \qquad \overline{xy} = \bar{x} \bar{y}.$$

On donne le nom d'*homomorphisme* (d'anneaux) à toute application $A \rightarrow \bar{A}$ ayant les propriétés précédentes ; l'anneau $\bar{A}$ est dit *homomorphe* à A , ou *image homomorphe* de A , on écrit :

$$A \sim \bar{A}.$$

Toute congruence R dans A fournit donc un anneau homomorphe $\bar{A}$, qui n'est autre que l'anneau-quotient A/R .

Considérons la classe d'équivalence $\bar{0}$ à laquelle appartient l'élément 0 de A ; c'est manifestement l'élément zéro de l'anneau A/R . Mais c'est aussi un sous-ensemble M de A doué de deux propriétés remarquables :

1° M est un sous-groupe additif de A ; en effet, M contient 0 par définition, $x + y$ en même temps que x et y , — x en même temps que x . (On peut, plus rapidement, dire que M contient $x - y$ en même temps que x et y et utiliser une proposition simple caractérisant les sous-groupes d'un groupe) (6).

2° M est multiplicativement permis dans A , puisque $m \in M$ et $a \in A$ entraînent $am = a0 = 0$ (R).

Puisque R est régulière par rapport à l'addition, les relations $x \equiv y$ (R) et $x - y \equiv 0$ (R), c'est-à-dire $x - y \in M$, sont vraies en même temps : si l'on connaît la classe-zéro, M , la congruence R en résulte.

On donne le nom d'*idéal* à tout sous-ensemble de l'anneau commutatif A possédant les propriétés 1° et 2° ; d'après ce qui précède, toute classe-zéro par rapport à une congruence est un idéal. Mais il est immédiat que si, inversement, nous nous donnons *a priori* un idéal M dans A

(5) L'étude de cet exemple repose sur des propositions que nous ne pouvons donner ici.

(6) Voir par exemple [2], p. 108.

et si nous considérons la relation R vérifiée par les couples d'éléments x, y de A tels que $x - y \in M$, et ceux-là seulement, R est une relation d'équivalence, et que cette relation est régulière pour l'addition et la multiplication : R est donc une congruence, et sa classe-zéro est précisément M .

Ainsi, on a une correspondance biunivoque entre les congruences R et les idéaux M d'un anneau commutatif A . Pour cette raison, l'anneau-quotient A/R s'écrit également A/M .

Partons maintenant d'un homomorphisme d'anneaux :

$$A \rightarrow \bar{A}$$

dans lequel l'élément x de A admet pour image l'élément $\bar{x}$ de $\bar{A}$. Considérons la relation R portant sur les éléments x, y de A et vérifiée par les couples (x, y) tels que $\bar{x} = \bar{y}$, et ceux-là seulement. R est une équivalence (appelée *équivalence d'homomorphisme*), et on vérifie aisément que c'est une congruence. Mais alors on peut former l'anneau-quotient A/R et, par construction, les classes suivant l'équivalence R , éléments de A/R , correspondent *biunivoquement* aux éléments de $\bar{A}$. Comme cette correspondance biunivoque respecte l'addition et la multiplication, c'est un *isomorphisme* : $\bar{A}$ est donc isomorphe à l'anneau-quotient $A/R = A/M$. L'idéal M , classe-zéro modulo R , est ici l'ensemble des éléments de A que l'homomorphisme applique sur le zéro de A (on dit que M est le *noyau* de l'homomorphisme).

On voit donc qu'à des isomorphismes près, les *congruences* ou, ce qui revient au même, les *idéaux* de A fournissent tous les anneaux homomorphes à A .

6. Cas particuliers et exemples

On définit, sur les idéaux d'un anneau commutatif A , des *opérations* qui sont l'*intersection* (au sens de la théorie des ensembles) ou p.p.c.m., la *somme* ou p.g.c.d., et le *produit*. La somme $a + b$ de deux idéaux a, b de A est l'ensemble des éléments $a + b$ où a décrit a , b décrit b : c'est visiblement un idéal contenant a et b . Le produit ab est l'idéal engendré par les produits ab , c'est-à-dire l'ensemble des sommes $a_1b_1 + \dots + a_rb_r$ (r non fixé) où $a_i \in a$, $b_i \in b$. Pour ne pas alourdir cet exposé, nous n'insisterons pas davantage sur ce *calcul des idéaux*, à vrai dire fort important (7), et dans lequel on définit également un quotient ou, mieux, une résiduation.

Bornons-nous à étudier un mode de génération fondamental ; pour simplifier un peu, nous supposons que l'anneau A possède un *élément-unité* e .

Si nous nous donnons dans l'anneau A , h éléments fixes $a_1, \dots, a_h$ l'ensemble des éléments $a = x_1a_1 + \dots + x_ha_h$, où les x_i décrivent A ,

(7) Voir par exemple [2], chap. IV, § 11, p. 188, [3], § 17, p. 57-59, et § 85, t. 2, p. 22-25.

est, comme on le vérifie sans peine, un idéal a , qu'on désigne par la notation :

$$a = (a_1, \dots, a_h)$$

On dit que a est engendré par les a_i , qu'il admet la base (finie) $a_1, \dots, a_h$. Tout idéal engendré par un seul élément, $a = (a)$, est dit *principal*. L'idéal (e) engendré par l'élément-unité coïncide avec l'anneau A : on lui donne souvent le nom d'*idéal-unité*. L'idéal engendré par l'élément 0 se réduit à cet élément : on l'appelle *idéal-zéro*.

Dans un corps K , il n'y a pas d'autres idéaux que l'idéal-zéro et l'idéal unité. Soit en effet M un idéal de K ; supposons $M \neq 0$. Alors M contient au moins un élément $a \neq 0$; cet élément a possède un inverse a^{-1} , puisque K est un corps, et nous avons $e = a^{-1}a \in M$, $K = (e)$ est donc contenu dans M , d'où $M = K = (e)$.

Dans l'anneau C des entiers, dans l'anneau $k[x]$ des polynômes en x à coefficients dans un corps k , tout idéal est principal.

Montrons-le pour l'anneau $A = k[x]$ par exemple. L'idéal-zéro est bien un idéal principal. Si maintenant a est un idéal $\neq (0)$, soit f un des polynômes non nuls de degré minimum appartenant à a ; g désignant maintenant un polynôme quelconque appartenant à a , divisons g par f : $g = qf + r$, où le degré de r est inférieur à celui de f . Le polynôme r appartient à l'idéal a , il est donc nécessairement nul, et g appartient à l'idéal principal (f) , qui coïncide par conséquent avec a .

Raisonnement analogue pour l'anneau C des entiers : on voit que, dans cet anneau, n'existent pas d'autres congruences que les congruences arithmétiques, définies par un module m ; m est le générateur de l'idéal principal associé à la congruence.

On donne le nom d'*anneau euclidien* à un anneau dans lequel existe un algorithme de division avec reste ; d'*anneau à idéaux principaux* (plus brièvement, d'*anneau principal*), à un anneau dans lequel tout idéal est principal. Le raisonnement précédent s'étend sans peine : tout anneau euclidien est principal. L'anneau des entiers de Gauss est également un anneau euclidien (pour définir la division avec reste, on utilise la norme $N(a)$ d'un élément $a = a + ib$, qui est par définition $N(a) = a^2 + b^2$, et on lui fait jouer le rôle du degré dans la division des polynômes à une indéterminée).

Un anneau de polynômes A à plus d'une indéterminée, par exemple un anneau tel que $\Gamma[x, y]$, $\Omega[x, y]$, n'est plus un anneau principal : l'idéal (x, y) n'admet pas, en effet, un générateur unique ; notons que cet idéal a une signification géométrique simple : c'est l'ensemble des polynômes de A qui sont nuls à l'origine. La génération des idéaux dans les anneaux de polynômes à n variables $K[x_1, \dots, x_n]$, où K est un corps quelconque, obéit cependant encore à une loi simple : dans un tel anneau, tout idéal admet une base finie. Les anneaux ayant cette propriété sont dits *noëthériens* (du nom de la mathématicienne Emmy NOETHER, qui en a donné d'autres définitions axiomatiques au moyen de la « condition maximale » et de l'« axiome des chaînes de diviseurs », et a donné les résultats fondamentaux de la théorie des idéaux dans de tels anneaux).

C'est à HILBERT qu'est dû le théorème qui vient d'être cité : l'anneau $K[x_1, \dots, x_n]$ est noëthérien. En fait, le théorème de Hilbert, un peu plus précis, prend la forme d'un « théorème de transfert » : si un anneau A , possédant un élément-unité, est noëthérien, l'anneau $A[x]$ est, lui aussi, noëthérien (8).

7. Idéaux remarquables

Il est naturel de distinguer, parmi les idéaux M d'un anneau commutatif A , ceux pour lesquels l'anneau-quotient ou anneau des classes résiduelles A/M a des propriétés remarquables. Etudions les cas dans lesquels A/M est un corps ou un domaine d'intégrité.

L'idéal M est dit *sans diviseurs* ou *maximal* si A est le seul idéal contenant strictement M . On a le théorème suivant :

Pour que A/M soit un corps, il faut que l'idéal M soit sans diviseurs. Si A possède un élément-unité, cette condition nécessaire est aussi suffisante.

Démonstration.

1° Supposons que A/M soit un corps.

Soit M' un idéal contenant strictement M : $M \subset M'$. Soit $a \in M' \setminus M$. Désignons par $\bar{a}$ la classe contenant a : $\bar{a}$ est différent de la classe-zéro $M = \bar{0} \in A/M$. Si x est un élément quelconque de A et $\bar{x}$ la classe contenant x , il existe $\bar{y} (= \bar{a}^{-1}\bar{x})$, tel que $\bar{x} = \bar{a}\bar{y}$, d'où, y désignant un élément de A situé dans la classe y :

$$x = ay \pmod{M}$$

c'est-à-dire :

$$x = ay + m \quad m \in M \subset M'$$

Comme $a \in M'$, nous avons $x \in M'$, donc $A = M'$; M est sans diviseurs.

2° Supposons que A possède un élément-unité e et que M soit sans diviseurs. Pour établir que A/M est un corps, il suffit de montrer que toute classe $\bar{a}$ différente de $\bar{0} = M$ admet un inverse. Un élément a situé dans la classe $\bar{a}$ n'appartient pas à M : l'idéal $M + (a)$ contient strictement M , d'où :

$$M + (a) = A.$$

En particulier, l'élément-unité e appartient au premier membre :

$$e = m + ra, \quad m \in M, r \in A,$$

d'où, en passant aux classes modulo M :

$$\bar{ra} = \bar{e}, \quad \text{c'est-à-dire } \bar{r} = \bar{a}^{-1}.$$

Une application importante de ce résultat est la suivante. Considérons un corps K et un polynôme irréductible $f(x)$ de l'anneau $K[x] = A$, c'est-à-dire un polynôme qui n'est pas le produit de deux polynômes du même anneau ayant des degrés au moins égaux à 1. L'idéal principal (f) est, dans A , un idéal sans diviseurs ; $A/(f)$ est donc un corps, K' . Les

(8) Voir par exemple [2], chap. VI, § 5, p. 331.

(*) Le signe $\notin$ a été utilisé à la place du signe $\in$ barré. $\notin$ signifie donc « n'appartient pas à ».

classes contenant les éléments de K correspondent biunivoquement à ces éléments, car deux éléments distincts de K ne peuvent pas être congrus modulo f ; ces classes forment un corps isomorphe à K , que nous identifions avec K ; K' est donc un sur-corps de K .

Si α est la classe qui contient le polynôme x , la classe contenant $f(x)$ est celle qui contient le polynôme $f(x)$ [en raison de l'homomorphisme $A \sim A/(f)$] ; mais la classe contenant $f(x)$ est l'élément zéro de K' . Donc, on a, dans K' , $f(x) = 0$, et on a construit un corps K' dans lequel l'équation $f(x) = 0$ a au moins une racine : telle est, réduite à l'essentiel, la méthode de l'adjonction symbolique.

Un idéal $\mathfrak{p}$ d'un anneau A tel que l'anneau $A/\mathfrak{p}$ soit un *domaine d'intégrité* est, par définition, un idéal premier. Il faut et il suffit que, dans $A/\mathfrak{p} = \bar{A}$, les relations :

$$\bar{x} \neq \bar{0}, \quad \bar{y} \neq \bar{0} \quad \text{entraînent} \quad \bar{x}\bar{y} \neq \bar{0},$$

donc que, dans A , les relations :

$$x \notin \mathfrak{p}, \quad y \notin \mathfrak{p} \quad \text{entraînent} \quad xy \notin \mathfrak{p},$$

ce qui signifie que l'ensemble complémentaire $A - \mathfrak{p}$ est multiplicativement fermé.

Cette notion d'idéal premier a une importance capitale, aussi bien dans les théories algébriques elles-mêmes que dans les applications arithmétiques ou géométriques.

Bornons-nous à constater que, dans un anneau A possédant un élément-unité, tout idéal sans diviseurs M est premier (A/M est en effet un corps, donc un domaine d'intégrité).

Pour terminer, prenons comme exemple l'anneau $\Omega[x, y, z] = A$ des polynômes à trois variables, à coefficients complexes, et considérons les idéaux :

$$\alpha_1 = (x, y, z) \quad \alpha_2 = (x, y) \quad \alpha_3 = (x).$$

A/α_1 est isomorphe à Ω , donc est un corps ; A/α_2 est isomorphe à l'anneau de polynômes $\Omega[z]$ qui est un domaine d'intégrité ; A/α_3 est isomorphe à l'anneau de polynômes $\Omega[y, z]$, c'est aussi un domaine d'intégrité. Les idéaux $\alpha_1, \alpha_2, \alpha_3$, qui vérifient les relations d'inclusion :

$$\alpha_3 \subset \alpha_2 \subset \alpha_1 \subset A = (1),$$

sont tous premiers, α_1 est sans diviseurs.

Paul DUBREIL,
Professeur à la Sorbonne.

BIBLIOGRAPHIE

- [1] N. BOURBAKI. — *Algèbre*, chap. I (Hermann, Paris, 1942).
- [2] P. DUBREIL. — *Algèbre*, t. I, 2^e éd. (Gauthier-Villars, Paris, 1954).
- [3] B. L. van der WAERDEN. — *Moderne Algebra*, 2^e éd. (Springer, Berlin).