

LES STRUCTURES ALGEBRIQUES OU ORDONNÉES DANS L'ENSEIGNEMENT ÉLÉMENTAIRE

Léonce LESIEUR

I. — RELATION D'ORDRE NATUREL DANS N.

Dès la première étude de l'arithmétique à l'école primaire, on compare les entiers. Cette comparaison définit une *relation d'ordre naturel dans l'ensemble N des entiers* 1, 2, ..., n, ..., satisfaisant aux trois axiomes :

$$(1) \left\{ \begin{array}{ll} \forall a \in N & a \leq a \quad \text{réflexivité,} \\ a \leq b \text{ et } b \leq a \Rightarrow & a = b \text{ antisymétrie,} \\ a \leq b \text{ et } b \leq c \Rightarrow & a \leq c \text{ transitivité.} \end{array} \right.$$

La relation est dite d'ordre strict si l'égalité est impossible ; nous considérons ici la relation d'ordre large qui n'exclut pas l'égalité. Remarquer aussi que la relation d'ordre naturel est improprement dite « d'inégalité » ; elle n'est pas la contradictoire de l'égalité.

La relation d'ordre naturel dans N jouit d'une propriété supplémentaire : deux éléments quelconques étant pris dans N, ou bien ils sont égaux, ou bien l'un est plus grand que l'autre. On peut écrire :

$$(2) \quad \forall a, b \in N \Rightarrow \exists a \leq b \text{ ou } b \leq a.$$

C'est une relation d'ordre *total* ; N est dit *totalelement ordonné*.

D'un point de vue algébrique, nous pouvons considérer deux lois de composition sur les éléments de N. Etant donné deux entiers naturels quelconques *a* et *b*, le plus grand des deux sera noté $\text{Max}(a, b) = a \vee b$; le plus petit des deux nombres *a* et *b* sera noté $\text{Min}(a, b) = a \wedge b$. Deux opérations sur les entiers sont ainsi définies : la formation du maximum, notée $\vee$, et celle du minimum, notée $\wedge$.

Au moyen de ce symbolisme, la distributivité de la deuxième opération par rapport à la première s'écrirait :

$$(3) \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Soit avec les notations Max et Min :

$$(3') \quad \text{Min}(a, \text{Max}(b, c)) = \text{Max}(\text{Min}(a, b), \text{Min}(a, c)).$$

Pour la justifier, on peut remarquer d'abord la symétrie des rôles de *b* et de *c* ; on peut donc supposer $b \leq c$. Alors, de trois choses l'une :

- 1) $a \leq b \leq c$: on vérifie que les deux membres de (3) valent *a* ;
- 2) $b \leq a \leq c$: on vérifie que les deux membres de (3) valent *a* ;
- 3) $b \leq c \leq a$: on vérifie que les deux membres de (3) valent *c*.

On démontre de même :

$$(3'') \quad a \mathbf{V} (b \mathbf{\wedge} c) = (a \mathbf{V} b) \mathbf{\wedge} (a \mathbf{V} c).$$

On remarque ici la simplicité des énoncés écrits symboliquement et, en contraste, la complexité des phrases qui exprimeraient les propositions (3) et (3''). Sous leur forme abstraite, ces propositions restent encore valables dans tout ensemble totalement ordonné : par exemple, $\mathbb{N} + \{0\}$, l'ensemble des entiers naturels complété par zéro ; $\mathbb{Z}$, l'ensemble des entiers relatifs (positifs, négatifs ou nul) ; etc...

II. — RELATION DE DIVISIBILITE DANS $\mathbb{N}$.

a et b étant des entiers naturels, nous écrirons que a divise b (ou que b est un multiple de a) : $a|b$ ou $a \leq b$. Cette deuxième notation est justifiée : la relation de divisibilité est une relation d'ordre qui satisfait aux axiomes (2), mais cet ordre n'est pas total, car il ne satisfait pas à l'axiome (3) ; pour deux entiers a et b quelconques, il peut ne pas y avoir relation de divisibilité, par exemple : $a = 4$, $b = 6$. Une relation d'ordre non total est dite d'ordre partiel.

D'un point de vue algébrique, on peut ici encore définir une loi de composition de deux entiers quelconques a et b : il suffit de chercher les entiers c vérifiant $a \leq c$ et $b \leq c$. Les c seront dits *majorants communs* (ou multiples communs). On sait qu'il en existe un, m , plus petit que tous les autres, et tel que tout autre majorant commun soit divisible par lui. On écrit :

$$\forall a \text{ et } b \in \mathbb{N}, \exists m \in \mathbb{N} \text{ tel que } a \leq m \quad b \leq m, \text{ et tel que } a \leq c \text{ et } b \leq c \Rightarrow m \leq c.$$

Le passage du couple (a, b) au nombre m est une opération algébrique qui sera notée $m = a \mathbf{V} b$ ou $m = \text{Sup}(a, b)$. Le symbole $\mathbf{V}$ est lu « union ». En m , on reconnaît le plus petit commun multiple de a et b .

De la même façon, on définira les MINORANTS COMMUNS à a et b (les diviseurs communs) ; le plus grand commun diviseur d sera le plus grand des minorants. On écrira :

$$\forall a, b \in \mathbb{N} \quad d = a \mathbf{\wedge} b = \text{Inf}(a, b) \in \mathbb{N} \text{ tel que } d \leq a, d \leq b \text{ et } c \leq a, c \leq b \Rightarrow c \leq d.$$

Les deux lois de composition introduites et notées $\mathbf{V}$ et $\mathbf{\wedge}$ sont-elles distributives l'une par rapport à l'autre ? La distributivité de l'opération notée $\mathbf{\wedge}$ par rapport à l'opération notée $\mathbf{V}$ s'écrirait :

$$(4) \quad a \mathbf{\wedge} (b \mathbf{V} c) = (a \mathbf{\wedge} b) \mathbf{V} (a \mathbf{\wedge} c).$$

Démonstration : a , b et c sont supposés décomposés en produits de facteurs premiers $p_1 \dots p_n$, ou p_i , i variant de 1 à n . Les décompositions s'écrivent :

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} = \prod_{i=1}^{i=n} p_i^{a_i},$$

$$b = \prod_{i=1}^{i=n} p_i^{b_i}, \quad c = \prod_{i=1}^{i=n} p_i^{c_i}.$$

(On peut supposer que les facteurs premiers sont les mêmes dans les trois décompositions, certains des exposants pouvant être nuls). En appliquant les règles de formation du plus petit commun multiple et du plus grand commun diviseur, on a :

$$b \vee c = \prod_{i=1}^{i=n} p_i^{\text{Max}(b_i, c_i)}; \quad b \wedge c = \prod_{i=1}^{i=n} p_i^{\text{Min}(b_i, c_i)}.$$

Le premier membre de (4) devient :

$$a \wedge (b \vee c) = \prod_{i=1}^{i=n} p_i^{\text{Min}(a_i, \text{Max}(b_i, c_i))},$$

et le second membre :

$$(a \wedge b) \vee (a \wedge c) = \prod_{i=1}^{i=n} p_i^{\text{Max}(\text{Min}(a_i, b_i), \text{Min}(a_i, c_i))}.$$

Il ne reste plus qu'à comparer les exposants qui sont égaux d'après la relation (3'). L'égalité (4) est vérifiée.

On démontrera de même :

$$(4') \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

III. — IDEaux DANS Z.

Une relation d'ordre partiel très intuitive est celle de l'inclusion des sous-ensembles extraits d'un ensemble. On peut ramener la relation de divisibilité à celle d'inclusion en introduisant la notion d'*idéal* dans l'ensemble Z des entiers relatifs.

a étant un élément quelconque de Z, on appellera idéal de base a dans Z l'ensemble des multiples de a ; on désignera cet idéal par (a).

$$(a) = \{ka\}, \quad k \text{ décrit } Z.$$

Si a = 0, l'idéal est nul ; si a est négatif, puisque k décrit Z, (a) = (—a). La base d'un idéal non nul peut donc être prise dans N.

On vérifie que la relation de divisibilité est logiquement équivalente à l'inclusion d'un idéal dans l'autre :

$$a|b \iff (b) \subseteq (a).$$

En effet, si a divise b, tous les multiples de b sont aussi des multiples de a ; donc, l'idéal de base b est inclus dans l'idéal de base a. Réciproquement, l'inclusion de (b) dans (a) implique que tous les multiples de b (donc b lui-même) soient des multiples de a.

L'énoncé classique : les multiples communs à deux entiers sont les multiples de leur plus petit commun multiple, conduit à la relation :

$$(a) \cup (b) = (a \vee b),$$

qui se traduit : l'intersection de deux idéaux non nuls est un idéal ayant pour base le majorant minimum des bases des deux idéaux donnés.

Remarque : Si (a) est l'idéal nul, $(a) \cap (b)$ est aussi l'idéal nul.

Par contre, la réunion de deux idéaux n'est pas un idéal. Si c'en était un, soit (p) , l'inclusion de (a) dans (p) signifierait $p|a$; de même $p|b$. Soit $a=3$ et $b=5$, alors $p=1$, et (1) n'est autre que $\mathbb{Z}$. Or, 4 n'appartient ni à (a) , ni à (b) ; 4 n'appartient donc pas à $(a) \cap (b)$.

On se posera alors le problème de chercher, s'il en existe, les idéaux (c) qui contiennent (a) et qui contiennent (b) ; les (c) seront dits idéaux majorants communs. Parmi tous ces (c) , il y en a un (d) qui est le *majorant commun minimum* ; il est obtenu en prenant pour d le plus grand commun diviseur de a et b .

On vérifie :

$$(d) = \{ma + nb\},$$

où m et n sont des entiers qui décrivent $\mathbb{Z}$; en effet, on montre d'abord que tout élément de la forme $ma + nb$ est inclus dans (d) , soit :

$$\{ma + nb\} \subseteq (d).$$

Il suffit de remarquer pour cela que $a = a'd$ et $b = b'd$ implique :

$$ma + nb = (ma' + nb')d \in (d).$$

On vérifie ensuite que tout élément de l'idéal (d) appartient à l'ensemble $\{ma + nb\}$. Il suffit pour cela d'utiliser la formule de Bezout qui exprime le plus grand commun diviseur d de a et b sous la forme :

$$\begin{aligned} d &= pa + qb, \quad \text{d'où} \\ kd &= kpa + kqb \in \{ma + nb\}. \end{aligned}$$

L'opération qui définit (d) doit être distinguée de la réunion et on la notera $+$.

$$(a) + (b) = (d).$$

Pour les deux lois notées $\blacktriangle$ (inter) et $+$ (union ou addition), on vérifiera la distributivité de l'une par rapport à l'autre, qui résulte des égalités (4) et (4') :

$$\begin{aligned} (a) + ((b) \blacktriangle (c)) &= ((a) + (b)) \blacktriangle ((a) + (c)), \\ (a) \blacktriangle ((b) + (c)) &= ((a) \blacktriangle (b)) + ((a) \blacktriangle (c)). \end{aligned}$$

IV. — TREILLIS.

L'ensemble N ordonné par la relation de divisibilité donne un exemple d'ensemble ordonné dans lequel deux éléments quelconques a et b possèdent un majorant minimum et un minorant maximum. D'une façon générale, on appelle *treillis* ou *ensemble réticulé* tout ensemble ordonné E jouissant de cette propriété. Le majorant minimum de a et b se note $a \vee b$ (union) et le minorant maximum $a \blacktriangle b$ (inter). E se trouve alors muni de deux opérations qui ont des propriétés algébriques intéressantes que nous n'étudierons pas ici.

Si ces opérations sont distributives l'une par rapport à l'autre, le treillis est dit distributif, et les exemples précédents : treillis formé par N muni de sa relation d'ordre naturel, treillis formé par N ordonné par la relation de divisibilité, treillis formé par l'ensemble des idéaux de Z ordonné par la relation d'inclusion, sont tous des treillis distributifs. Mais il existe aussi des treillis non distributifs ; en voici un exemple simple, d'origine géométrique.

Soit E l'ensemble des variétés linéaires de l'espace à trois dimensions :

$$E = \{\text{points, droites, plans, } E \text{ lui-même, } \emptyset\}.$$

La relation d'inclusion (ou d'incidence) est une relation d'ordre. Exemples : point A situé sur une droite D ($A \subseteq D$) ; droite D située dans un plan P ($D \subseteq P$). Mais cet ordre est partiel. A et B étant deux variétés linéaires de E peuvent ne pas être comparables par la relation d'inclusion.

Etant donné deux variétés A et B , il y a une variété maximum contenue dans A et dans B ; c'est l'intersection au sens de la théorie des ensembles ; on écrit :

$$A \cap B = A \wedge B.$$

On définit de même la variété minimum qui contient A et B , c'est-à-dire la variété minimum parmi les variétés majorantes de A et B . On l'écrit $A \vee B$, on lit le symbole $\vee$ « union » et on ne doit pas confondre avec l'opération de réunion (notée $A \cup B$).

Exemple : A et B sont deux droites ; leur réunion est l'ensemble des deux droites ; si les deux droites sont sécantes ou parallèles (mais non confondues), $A \vee B$ est leur plan ; si les deux droites ne sont pas coplanaires, $A \vee B$ est E tout entier ; si les deux droites sont confondues, $A \vee B = A = B$.

Dans le cas de E , il est facile de vérifier que les deux opérations notées $\wedge$ et $\vee$ ne sont pas distributives l'une par rapport à l'autre. En effet, prenons A , B , C , trois droites deux à deux non coplanaires. $B \vee C = E$, donc :

$$A \wedge (B \vee C) = A \wedge E = A.$$

D'autre part, $A \wedge B = \emptyset$ et $A \wedge C = \emptyset$, donc :

$$(A \wedge B) \vee (A \wedge C) = \emptyset \vee \emptyset = \emptyset.$$

Il est vérifié que $A \wedge (B \vee C) \neq (A \wedge B) \vee (A \wedge C)$.

V. — LA NOTION DE GROUPE.

Je termine par quelques mots sur la notion de groupe, qu'on ne peut passer sous silence, l'enseignement élémentaire, en donnant de nombreux exemples. Par exemple, l'addition dans Z est une loi de *groupe abélien* (ou groupe commutatif), parce qu'elle vérifie les axiomes suivants :

$$\left\{ \begin{array}{l} \forall a, b \in \mathbb{Z} \quad a + b \in \mathbb{Z}, \\ a + 0 = a \quad (\text{zéro est l'élément neutre du groupe}), \\ \forall a \in \mathbb{Z}, \exists a' \in \mathbb{Z} \quad a + a' = 0 \quad (a' \text{ est l'élément opposé à } a), \\ a + b = b + a \quad (\text{commutativité}), \\ (a + b) + c = a + (b + c) \quad (\text{associativité}). \end{array} \right.$$

L'étude des transformations géométriques fournit même des exemples de *groupes non commutatifs*. Soit T l'ensemble des transformations (ou applications) de l'espace E ; A et B étant des transformations, il leur est associé par la loi de composition notée $\circ$ la transformation $A \circ B$ (« composée » de A et de B ou « produit » des transformations A et B).

$$\left\{ \begin{array}{l} \forall A, B \in T, \quad A \circ B \in T, \\ A \circ I = I \circ A = A \quad (I \text{ est l'élément neutre du groupe} \\ \quad \text{ou la transformation identique}), \\ \forall A \in T, \exists A' \quad A \circ A' = A' \circ A = I \\ \quad (A' \text{ est la transformation inverse de } A), \\ A \circ (B \circ C) = (A \circ B) \circ C \quad (\text{associativité}). \end{array} \right.$$

Le groupe des déplacements est un sous-groupe du groupe des transformations.

Le groupe T n'étant pas commutatif : $A \circ B \neq B \circ A$, on peut se poser le problème de trouver X tel que :

$$A \circ B = B \circ A \circ X.$$

On trouve $X = A^{-1} \circ B^{-1} \circ B \circ A$; X est dit *commutateur* de A et de B . On vérifiera, par exemple, que les commutateurs du groupe des déplacements du plan forment le sous-groupe des translations.

A la suite de l'exposé, une discussion s'engage où sont évoquées en particulier les notions d'anneau, de corps et d'espace vectoriel qu'on rencontre aussi, bien entendu, dans l'enseignement élémentaire, mais qui ne peuvent être dégagées de façon abstraite qu'au niveau de la propédeutique. Voir pour ces notions et pour des compléments : « Structures algébriques et structures topologiques » (Monographie n° 7 de l'*Enseignement Mathématique*, éditée en commun avec l'A.P.M.).