LES MATHEMATIQUES « MODERNES » DANS L'ENSEIGNEMENT DU SECOND DEGRE (*)

par André HUISMAN
Inspecteur de l'Académie de Paris

II. — RELATIONS D'EQUIVALENCE. LOIS DE COMPOSITION

Nous avons remarqué que l'égalité entre ensembles possède les trois qualités : réflexivité, symétrie, transitivité. Lorsqu'une relation entre deux éléments d'un ensemble possède ces trois qualités, on dit que c'est une relation d'équivalence.

Exemples : En géométrie, l'égalité et la similitude entre figures sont des relations d'équivalence. Dans l'ensemble des fractions, la relation d'équivalence entre b/a et d/c est : $bc = ad$.

Si, dans un ensemble E, *on définit une relation d'équivalence, on détermine dans* E *une partition.*

Soit R la relation d'équivalence ; pour exprimer que deux éléments x et x' de E vérifient R (sont équivalents module R), nous écrirons : xRx'. Soit x un élément de E ; formons une partie Cx de E avec tous les éléments x' tels que xRx'. Ceci fait, s'il y a encore des éléments de E qui ne sont pas dans Cx, soit y l'un d'eux, et formons la partie Cy avec tous les éléments y' tels que yRy', et ainsi de suite. Finalement, tous les éléments de E seront ainsi classés, et il reste à montrer que les classes obtenues ne sont pas vides, et sont deux à deux disjointes. En effet :

1) la classe Cx n'est pas vide, elle contient au moins x puisque xRx (réflexivité) ;

2) les classes Cx et Cy sont disjointes, car si elles avaient un élément a commun, on aurait :

$$xRa \text{ et } yRa \text{ ou : } xRa \text{ et } aRy \Rightarrow xRy \text{ (transitivité de R)},$$

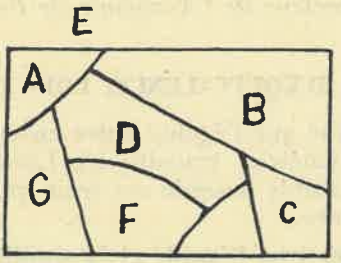
ce qui est impossible car, d'après la construction de Cx et Cy, la relation xRy est fausse.

Les parties Cx obtenues sont les classes d'équivalence, et l'ensemble formé par les classes d'équivalence est l' « ensemble quotient » noté E/R.

(*) La première partie de cette étude, consacrée aux ensembles, a paru dans le *Bulletin* n° 223, de juin 1962.
La rédaction du *Bulletin* prie l'auteur et les lecteurs d'excuser plusieurs négligences coupables que nous essayons, ici, de corriger :
— p. 279 : le nom de l'auteur a été omis.
— p. 286, 13e ligne, il faut lire 8 classes (et non 16).
— p. 288, 11e ligne, il faut lire 8 classes (et non 16).
Il faut croire qu'en fin d'année scolaire, le calcul exact de 2^3 est au-dessus des forces de la Rédaction !

Réciproquement, *si l'on a déterminé une partition de* E, *on a défini une relation d'équivalence dans* E.

Soit une partition de E en classes A, B, . . , L. Définissons dans E une relation R : nous dirons que $x \in E$ et $y \in E$ vérifient R, (xRy), si (et seulement si) x et y appartiennent à une même classe de la partition. Il faut prouver que R est une relation d'équivalence, ce qui est immédiat, car on vérifie sans difficulté les trois qualités (réflexivité, symétrie, transitivité).



Exemples : Dans le plan, nous nous donnons, entre points a et b, la relation : $Oa = Ob$, O étant un point fixe du plan. C'est une relation d'équivalence, les classes étant les cercles de centre O.

Dans le plan (ensemble de points) donnons-nous une droite D, et entre les points a et b, la relation R : aRb si la droite ab est parallèle à D. C'est une relation d'équivalence, les classes sont les droites parallèles à D.

Dans le plan (ensemble de droites) donnons-nous une relation R : nous dirons qu'entre les droites d et d' on a dRd' si d et d' sont parallèles (en convenant, pour la réflexivité, que deux droites confondues sont parallèles : parallélisme au sens large). C'est une relation d'équivalence, les classes sont les directions de droite du plan.

De même dans l'espace, le parallélisme (au sens large) des plans est une relation d'équivalence ; l'ensemble quotient est l'ensemble des directions de plan.

1. — L'ensemble des entiers naturels.

Dans l'ensemble N des entiers naturels sont définies deux lois de composition, l'addition et la multiplication, pour lesquelles nous prendrons les axiomes suivants :

Relation d'équivalence : c'est l'égalité.

$$a = a \; ; \; a = b \Rightarrow b = a \; ; \; a = b \text{ et } b = c \Rightarrow a = c.$$

Addition : 1) Il existe une loi de composition interne appelée addition : $a \in N$, $b \in N$, il existe $c = a + b \in N$; l'ensemble N est fermé pour l'addition.

2) La relation d'égalité est compatible avec l'addition :

$$a = a' \text{ et } b = b' \Rightarrow a + b = a' + b'.$$

3) Commutativité : $a + b = b + a$.

4) Associativité : $(a + b) + c = a + (b + c)$.

5) Il existe un élément neutre, zéro : quel que soit $a \in \mathbf{N}$, $a + 0 = a$.

Multiplication : 1) Il existe une loi de composition interne appelée multiplication : $a \in \mathbf{N}, b \in \mathbf{N}$, il existe $d = a.b \in \mathbf{N}$; l'ensemble N est fermé pour la multiplication.

2) La relation d'égalité est compatible avec la multiplication :

$$a = a' \text{ et } b = b' \quad \Rightarrow \quad ab = a'b'.$$

3) Commutativité : $ab = ba$.

4) Associativité : $(ab)c = a(bc)$.

5) Existence d'un élément neutre : $a.1 = a$ quel que soit $a \in \mathbf{N}$.

6) Distributivité de la multiplication pour l'addition :

$$a(b + c) = ab + ac.$$

7) Tout élément non nul de N est simplifiable pour la multiplication :

$$c \neq 0 \text{ et } ca = cb \quad \Rightarrow \quad a = b.$$

Remarques : 1) L'élément neutre pour l'addition est unique, car : $a + x = a$ quel que soit a, donne, pour $a = 0$: $0 + x = 0$, et comme : $0 + x = x$, on en déduit, par transitivité : $x = 0$.

2) L'élément neutre pour la multiplication est unique, car : $ax = a$ quel que soit a donne, pour $a = 1$: $1x = 1$, et comme $1x = x$, on en déduit : $x = 1$.

3) L'axiome 2 de l'addition permet d'écrire :

$$a = b \text{ et } c = c \quad \Rightarrow \quad a + c = b + c,$$

nous verrons plus loin la réciproque.

4) L'axiome 2 de la multiplication permet d'écrire :

$$a = b \text{ et } c = c \quad \Rightarrow \quad ac = bc,$$

l'axiome 7 de la multiplication énonce la réciproque, pour $c \neq 0$.

2. — Symétrisation de N pour l'addition.

Le seul élément de N qui ne puisse pas être obtenu par addition est l'élément neutre 0 ; il n'existe pas d'entiers naturels a et b tels que l'on ait : $a + b = 0$, sauf bien entendu $a = b = 0$.

Nous allons définir un ensemble Z dont les éléments sont les entiers relatifs, de manière qu'à tout élément x de Z corresponde un élément « symétrique » x' tel que l'on ait : $x + x' = 0$.

On sait que cet ensemble Z peut être construit rigoureusement à partir des couples d'entiers (a, b) entre lesquels on se donne une relation d'équivalence. On montre alors qu'on peut identifier N à une partie de Z.

A un point de vue plus élémentaire, on peut, après avoir défini le symétrique x' de l'entier naturel x, poser que tous les axiomes énoncés plus haut restent valables dans l'ensemble Z formé par N et les éléments symétriques des éléments de N, à condition, bien entendu, d'avoir convenablement défini les opérations d'addition et de multiplication.

Intuitivement, les entiers naturels peuvent être représentés par des points d'une demi-droite Ox, mais l'ensemble N ne permet pas de numéroter en même temps les points de la demi-droite opposée Ox'. Il est alors

naturel d'associer à tout point M de Ox son symétrique M′ par rapport à O, et de désigner par 1′, 2′, ... les entiers représentés par les points symétriques de ceux qui représentent 1, 2, ... Deux entiers relatifs seront, par définition, égaux s'ils sont représentés par un même point de $x'x$.

L'interprétation géométrique de la relation : $a + a' = 0$ conduit aux règles connues de l'addition :

$$2 + 3' = 1' \; ; \quad 2' + 3 = 1 \; ; \quad 2' + 3' = 5',$$

et en général :

$a + b' = (a - b)$ si $a \geqslant b$; $a + b' = (b - a)'$ si $a \leqslant b$; $a' + b' = (a + b)'$ quels que soient a et b.

Remarquons qu'une relation telle que : $a + b' = (a - b)$ justifie dans la suite la notation $-b$ au lieu de b' *.

Remarque : Dans **N**, la soustraction n'est pas partout définie ; $b - a$ n'a de sens que si $b \geqslant a$. Avec l'introduction des entiers relatifs, l'opération devient toujours possible (mais son résultat n'appartient pas toujours à **N**). Si a et b sont des entiers naturels quelconques, $b - a$ est défini par l'équivalence :

$$x = b - a \iff b = x + a$$

et nous pouvons écrire (axiomes 2 et 4 de l'addition) :

$a' = a'$ et $b = x + a \Rightarrow b + a' = (x + a) + a' = x + (a + a') = x + 0 = x$.

Pratiquement, l'introduction des entiers x' perdrait beaucoup de ses avantages s'il fallait constamment distinguer les entiers x et x'. C'est pourquoi on convient de représenter par des lettres sans accent aussi bien les entiers naturels que leurs symétriques. Dans ces conditions x' représentera désormais le symétrique d'un entier relatif quelconque ; ce pourra donc être un entier naturel. Par exemple, si $x = 3'$, $x' = (3')' = 3$.

Théorème : Le symétrique de $b + a$ est $a' + b'$.

Car : $(b + a) + (a' + b') = b + (a + a') + b' = b + 0 + b' = b + b' = 0$.

Observons que la démonstration repose uniquement sur l'associativité de l'addition. La commutativité permet d'écrire aussi $b' + a'$.

Théorème : Tout entier relatif est simplifiable pour l'addition. C'est-à-dire : $a + b = a + c \Rightarrow b = c$.

En effet : $a' = a'$ et $a + b = a + c \Rightarrow a' + (a + b) = a' + (a + c)$

ou : $(a' + a) + b = (a' + a) + c$ ou : $0 + b = 0 + c$ ou enfin : $b = c$.

Remarque : Nous avons admis implicitement l'unicité du symétrique x' de x, ce qui est possible dans une étude intuitive. Notons cependant que cette unicité résulte des axiomes et du théorème précédent :

$$x + y = 0 \quad \text{et} \quad x + z = 0 \Rightarrow x + y = x + z \Rightarrow y = z.$$

Conclusion : Résumons ce qui précède : **Z**, muni de la seule addition, possède les propriétés suivantes : il est fermé pour l'addition ; l'addition est associative, elle possède un élément neutre, et tout élément de **Z** a un symétrique.

On résume ces propriétés en disant que **Z** est un groupe additif, qui est en outre commutatif.

(*) Nous laissons de côté la vérification des différents axiomes de l'addition.

3. — La multiplication dans Z.

Nous n'avons pas utilisé l'historique comparaison des nombres relatifs avec des gains et des pertes, car elle n'est d'aucun secours pour définir la multiplication. Nous nous contenterons de nous laisser guider par les axiomes relatifs à la multiplication dans **N**, et de définir la multiplication dans **Z** de manière que ces axiomes restent valables.

Tout d'abord, puisque nous admettons que **N** est une partie de **Z**, nous savons ce que signifie le produit ab lorsque $a \in \mathbf{N}$ et $b \in \mathbf{N}$. Il nous reste à préciser ce que signifient des produits tels que (en revenant momentanément à la première signification de l'accent) :

$$2.3' \quad \text{et} \quad 2'.3'.$$

Théorème : $a.0 = 0.a = 0$, quel que soit $a \in \mathbf{Z}$.
En effet (axiome 2) : $a = a$ et $a + 0 = a \Rightarrow a(a + 0) = aa$,
puis (axiome 6) : $a(a + 0) = aa + a.0$; enfin : $aa + a0 = aa \Rightarrow a0 = 0$.

Soit à définir $2.3'$; d'après le théorème précédent :

$$2(3 + 3') = 0,$$

donc : $2.3 + 2.3' = 0$, ce qui prouve que $2.3'$ est le symétrique de 2.3, d'où la règle : $2.3' = (2.3)'$.

On obtient de même la règle : $2'.3' = 2.3$.

Moyennant les règles précédentes, on pourra vérifier les autres propriétés : fermeture de **Z** pour la multiplication, associativité...

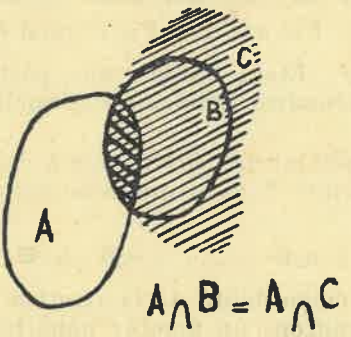
Théorème : $ab = 0$ et $a \neq 0 \Rightarrow b = 0$.
En effet : $ab = 0 = a0 \quad \Rightarrow \quad b = 0$ puisque $a \neq 0$ est simplifiable.

Conclusion : Outre l'addition, pour laquelle **Z** a la structure de groupe commutatif, **Z** est maintenant muni d'une multiplication associative, et distributive pour l'addition. On résume ces propriétés en disant que **Z** a une structure d'anneau.

Remarque : Les propriétés de l'addition dans **N** et **Z** présentent des analogies évidentes avec celles des opérations $\cap$ et $\cup$ appliquées à des parties d'un ensemble. Notons des différences :

a) pour toute partie, on a : $A \cap A = A$, $A \cup A = A$,
tandis que dans **Z** on n'a $x + x = x$ que pour $x = 0$, et $xx = x$ que pour $x = 0$ ou $x = 1$;

b) chacune des opérations $\cap$ et $\cup$ est distributive pour l'autre ;



c) pour les opérations $\cap$ et $\cup$, la règle de simplification n'est pas valable ; on n'a pas : $A \cap B = A \cap C \Rightarrow B = C$, ni : $A \cup B = A \cup C \Rightarrow B = C$.

A et B étant donnés, $A \cap B = A \cap C$ est vérifié si l'on prend pour C la réunion de $A \cap B$ et d'un ensemble disjoint de A.

A et B étant donnés, $A \cup B = A \cup C$ est vérifié si l'on prend pour C la réunion de $B \cap \bar{A}$ et d'une partie de A ou B.

Par contre, la conjonction des deux égalités permet la simplication par A :

$$A \cap B = A \cap C \text{ et } A \cup B = A \cup C \quad \Rightarrow \quad B = C.$$

4. — Les classes résiduelles (module *m*).

Dans **Z**, l'ensemble des multiples d'un entier m est fermé pour l'addition. Ces multiples sont de la forme xm, où l'on peut supposer m positif, en transférant le signe sur x.

On a ainsi une partition de **Z** en deux classes, celle des entiers xm, et celle des autres (m est supposé différent de 0 et de 1).

On peut obtenir une partition plus fine en utilisant la division « euclidienne » et en définissant une relation d'équivalence entre entiers : nous dirons que deux entiers a et b sont équivalents (ou congrus) module m si, divisés par m, ils donnent le même reste, c'est-à-dire si leur différence est divisible par m. Nous noterons cette relation :

$$a \equiv b \pmod{m} \text{ (congruence).}$$

On vérifie aisément que c'est bien une relation d'équivalence, qui détermine dans **Z** une partition dont les classes sont les classes résiduelles (mod m).

Il y a m classes, qui correspondent aux restes 0, 1, .., $m - 1$ de la division par m.

On démontre alors que la relation d'équivalence est compatible avec l'addition et la multiplication :

$$a \equiv a' \text{ et } b \equiv b' \Rightarrow a + b \equiv a' + b' \text{ et } ab \equiv a'b' \pmod{m}.$$

L'ensemble quotient $\mathbf{Z}/m$ est ainsi muni des mêmes opérations que **Z** ; elles possèdent les propriétés déjà énumérées, sauf celle qui concerne la simplification pour la multiplication, sur laquelle nous reviendrons. Par contre, la règle de simplification pour l'addition subsiste :

$$a + b \equiv a + c \Rightarrow b \equiv c \pmod{m}.$$

Problème pratique : Etant donnée une partition de **Z** en classes mod m, comment reconnaître rapidement à quelle classe appartient un entier donné X ?

Les axiomes permettent de définir dans **Z** des polynômes ; en particulier, on peut représenter X dans une numération de base B (et d'une seule manière) :

$$X = a_0 + a_1 B + a_2 B^2 + \ldots + a_n B^n, \; a_i \in (0, 1, .., B - 1).$$

En vertu de la compatibilité de la relation d'équivalence avec les opérations, nous obtiendrons un nombre appartenant à la même classe

que X en remplaçant les a_i et B^k par des entiers équivalents (mod m). La méthode est particulièrement simple dans les cas suivants :

1) toutes les puissances de B appartiennent à la classe 0 ; alors :

$$X \equiv a_0 \pmod{m},$$

c'est le cas de $m = 2$ et $m = 5$ pour $B = 10$;

2) toutes les puissances de B appartiennent à la classe 1 ; alors :

$$X \equiv a_0 + a_1 + \ldots + a_n \pmod{m},$$

c'est le cas de $m = 9$ pour $B = 10$;

3) B appartient à la classe -1 (c'est-à-dire $m - 1$) ; alors :

$$B^{2k} \equiv 1,\ B^{2k+1} \equiv -1 \pmod{m},$$

et :
$$X \equiv a_0 - a_1 + a_2 - \ldots,$$

c'est le cas de $m = 11$ pour $B = 10$.

5. — Généralisation : l'ensemble $\{ xm + yn \}$.

Considérons l'ensemble $\{ xm + yn \}$, où l'on peut supposer que m et n sont des entiers naturels. Cet ensemble est fermé pour l'addition, et pour la multiplication par un entier :

$$(xm + yn) + (x'm + y'n) = (x + x')m + (y + y')n ;$$
$$k(xm + yn) = (kx)m + (ky)n.$$

Dans l'ensemble, considérons les nombres qui sont strictement positifs *. Parmi eux, il y en a un qui est plus petit que tous les autres, soit d. Divisons $xm + yn$ par d :

$$xm + yn = dq + r,\quad 0 \leqslant r < d.$$

Cette relation montre que $r = (xm + yn) + (-q)d$ appartient à l'ensemble, et il est $\geqslant 0$. Il ne peut être > 0, car il serait inférieur à d, ce qui est contraire à la définition de d ; r est donc nul, et :

$$xm + yn = qd.$$

Tous les nombres de l'ensemble sont donc multiples de d ; on est ramené au premier cas.

Propriétés de d : 1) d appartient à l'ensemble, il est donc de la forme $am + bn$. Par suite, tout entier qui divise à la fois m et n divise aussi d.

2) m et n appartiennent à l'ensemble :

$$m = 1.m + 0.n\ ;\quad n = 0.m + 1.n\ ;$$

par suite, tout entier qui divise d divise à la fois m et n.

En résumé, l'ensemble des diviseurs communs à m et n est égal à l'ensemble des diviseurs de d, ce qui justifie le nom de « plus grand diviseur commun » donné à d. Nous le désignerons aussi par $D(m, n)$.

Cas particuliers : 1) si d n'a pas d'autres diviseurs que 1 et d, on dit qu'il est premier ;

2) si $d = 1$, m et n n'ont pas d'autre diviseur commun que 1 ; on dit qu'ils sont premiers entre eux. Dans ce cas, il existe des entiers relatifs

---

(*) Nous supposons définie une relation d'ordre dans **N** et **Z**.

a et b tels que : $am + bn = 1$. Et une telle relation entraîne évidemment que m et n sont premiers entre eux, d'où :

Théorème de Bezout : m et n sont premiers entre eux si (et seulement si) il existe des entiers relatifs a et b tels que l'on ait :

$$am + bn = 1.$$

Corollaire : Soit $D(m, n) = d$; posons : $m = m'd$, $n = n'd$, d'où :

$$d = am + bn = am'd + bn'd \Rightarrow 1 = am' + bn' \Rightarrow D(m/d, n/d) = 1.$$

La règle de simplification multiplicative dans $\mathbf{Z}/m$.

Pour abréger, convenons d'écrire : $a|b$ pour exprimer que a divise b.

Théorème de Gauss : $a|bc$ et $D(a, b) = 1 \Rightarrow a|c$.

Car $D(a, b) = 1$ se traduit par : $xa + yb = 1$ d'où : $xac + ybc = c$. a divisant ac et bc, il divise c.

Revenons alors à la règle de simplification multiplicative dans $\mathbf{Z}/m$. Soit la congruence : $ca \equiv cb \pmod m$ ou : $c(a - b) \equiv 0 \pmod m$.

Si $D(m, c) = 1$, le théorème précédent montre que :

$$c(a - b) \equiv 0 \Rightarrow a - b \equiv 0 \pmod m,$$

la règle de simplification est donc valable dans ce cas. En particulier si m est premier, tout entier qui n'appartient pas à la classe 0 de $\mathbf{Z}/m$ (on dit, pour abréger, tout entier non nul) est simplifiable pour la multiplication :

$$c \not\equiv 0 \quad \text{et} \quad ca \equiv cb \Rightarrow a \equiv b \pmod m$$

en tout point comparable à l'axiome 7 de la multiplication.

Si $D(c, m) = d \neq 1$, posons : $c = c'd$, $m = m'd$, $D(c', m') = 1$; alors : $c(a - b) \equiv 0 \pmod m \Rightarrow c'(a - b) \equiv 0 \pmod{m'} \Rightarrow a - b \equiv 0 \pmod{m'}$.

Dans ce cas, la règle de simplification n'est pas valable dans $\mathbf{Z}/m$; on peut avoir : $xy \equiv 0 \pmod m$ sans que l'on ait $x \equiv 0$ ni $y \equiv 0 \pmod m$. Nous allons en voir des exemples.

6. — Tables d'opérations dans $\mathbf{Z}/m$.

L'ensemble $\mathbf{Z}/m$ étant fini, on peut représenter complètement les deux opérations par leurs tables.

Soit par exemple la table d'addition pour $\mathbf{Z}/6$. Dans cette table, $2'$ désigne la classe équivalente à 2, c'est-à-dire que $2'$ désigne les entiers de la forme : $2 + 6k$, $k \in \mathbf{Z}$.

On remarque :

— les rangées se déduisent de la première par permutations circulaires successives ;

	$0'$	$1'$	$2'$	$3'$	$4'$	$5'$
$0'$	$0'$	$1'$	$2'$	$3'$	$4'$	$5'$
$1'$	$1'$	$2'$	$3'$	$4'$	$5'$	$0'$
$2'$	$2'$	$3'$	$4'$	$5'$	$0'$	$1'$
$3'$	$3'$	$4'$	$5'$	$0'$	$1'$	$2'$
$4'$	$4'$	$5'$	$0'$	$1'$	$2'$	$3'$
$5'$	$5'$	$0'$	$1'$	$2'$	$3'$	$4'$

— $0'$ est l'élément neutre de Z/6 pour l'addition ;

— $0'$ figure une fois, et une seule, dans chaque rangée ; autrement dit, tout élément de Z/6 a un symétrique, et un seul, pour l'addition.

En résumé, Z/6, fermé pour l'addition, a la structure de groupe additif.

La table permet de résoudre des « équations » telles que :

$$x + a \equiv b \pmod 6,\ a, b, x \in \mathrm{Z}/6$$

par exemple, $2' + x \equiv 1'$ a pour solution $x \equiv 5'$. D'une manière générale, si a' est le symétrique de a :

$$x + a \equiv b \Longleftrightarrow x + a + a' \equiv b + a' \quad \text{ou :} \quad x \equiv b + a' \pmod 6.$$

Considérons maintenant la table de multiplication dans Z/6.

	$0'$	$1'$	$2'$	$3'$	$4'$	$5'$
$0'$	$0'$	$0'$	$0'$	$0'$	$0'$	$0'$
$1'$	$0'$	$1'$	$2'$	$3'$	$4'$	$5'$
$2'$	$0'$	$2'$	$4'$	$0'$	$2'$	$4'$
$3'$	$0'$	$3'$	$0'$	$3'$	$0'$	$3'$
$4'$	$0'$	$4'$	$2'$	$0'$	$4'$	$2'$
$5'$	$0'$	$5'$	$4'$	$3'$	$2'$	$1'$

On remarque :

$1'$ est l'élément neutre pour la multiplication ;

seul $5'$ a un « inverse », c'est-à-dire qu'il existe x' tel que : $5'.x' \equiv 1'$, c'est $5'$ lui-même puisque :

$$5'.5' \equiv 1 \pmod 6.$$

$1'$ ne figure dans aucune des rangées relatives aux autres éléments ; il peut arriver que l'on ait $xy \equiv 0 \pmod 6$ sans que l'on ait $x \equiv 0$, ni $y \equiv 0$; par exemple :

$$2'.3' \equiv 0,\ 3'.4' \equiv 0 \pmod 6$$

(on dit que Z/6 a des diviseurs de zéro).

En résumé, Z/6, muni des deux opérations, a la structure d'anneau.

Problème : A quoi reconnaît-on que Z/m n'a pas de diviseurs de 0 ?

Nous avons vu que :

$$xy \equiv 0 \pmod m \quad \text{et} \quad \mathrm{D}(x, m) = 1 \Rightarrow y \equiv 0 \pmod m$$

autrement dit, si m est premier, on ne peut avoir $xy \equiv 0 \pmod m$ que si $x \equiv 0$ ou $y \equiv 0 \pmod m$. Z/m n'a pas de diviseur de zéro.

Si m n'est pas premier, soit $m = ab$; a et b appartiennent à des classes (mod m) a' et b' qui ne sont pas nulles ; il y a donc des diviseurs de zéro. En résumé :

Pour que Z/m n'ait pas de diviseur de 0, il faut et il suffit que m soit premier.

Problème : Dans Z/m, quels sont les éléments qui ont un inverse, c'est-à-dire les éléments a pour lesquels il existe x tel que : $ax \equiv 1 \pmod m$. Cette congruence équivaut à l'égalité : $ax + my = 1$, qui exprime que $\mathrm{D}(a, m) = 1$. Donc :

1) si m est premier, tous les éléments non nuls ont un inverse ;

2) si m n'est pas premier, seules les classes premières avec m ont un inverse, c'est-à-dire celles qui ne sont pas diviseur de zéro. C'est ainsi que, dans Z/6, seule 5′ a un inverse.

7. — Autre exemple : la table de multiplication dans Z/7.

La table d'addition dans Z/7 ne présente pas d'intérêt particulier ; elle nous montrerait que Z/7, comme Z/6 et en général Z/m, a la structure de groupe additif. Etudions la table de multiplication.

	0′	1′	2′	3′	4′	5′	6′
0′	0′	0′	0′	0′	0′	0′	0′
1′	0′	1′	2′	3′	4′	5′	6′
2′	0′	2′	4′	6′	1′	3′	5′
3′	0′	3′	6′	2′	5′	1′	4′
4′	0′	4′	1′	5′	2′	6′	3′
5′	0′	5′	3′	1′	6′	4′	2′
6′	0′	6′	5′	4′	3′	2′	1′

Nous constatons que tout élément non nul a un inverse ; nous pouvons résoudre des équations telles que :

$$ax \equiv b \pmod 7.$$

Soit par exemple : $3'x \equiv 4'$; sa solution est : $x \equiv 6'$ **(mod 7)**.

D'une manière générale, si $a = 0$, soit a' son inverse ; nous aurons :

$$ax \equiv b \Rightarrow a'ax \equiv a'b, \quad x \equiv a'b \pmod 7.$$

En résumé, dans Z/7, fermé pour la multiplication, les éléments non nuls forment un groupe.

Lorsqu'un ensemble muni d'une addition et d'une multiplication possède les propriétés suivantes : c'est un groupe commutatif pour l'addition ; la multiplication est associative, et distributive pour l'addition ; l'ensemble, privé de l'élément neutre de l'addition, est un groupe pour la multiplication ; on dit que cet ensemble est un corps. Il en est ainsi pour Z/m lorsque m est premier.

Application : théorème de Wilson : Soit m premier ; considérons les $m - 1$ classes non nulles (mod m), représentées par $1, 2, ..., m - 1$. Chacune d'elles ayant un inverse, on peut associer les nombres précédents deux par deux de manière que, pour un couple (a, b), on ait :

$$ab \equiv 1 \pmod m$$

1 est ainsi associé à lui-même, ainsi que $m - 1$, puisque :

$$(m-1)^2 \equiv 1 \pmod m.$$

En multipliant membre à membre les congruences :

$$ab \equiv 1,\ a_1b_1 \equiv 1,\ ...,\ m-1 \equiv 1 \pmod m,$$

nous obtenons :

$$(m-1)\,! \equiv -1 \pmod m.$$

Réciproquement, si un entier m vérifie cette dernière congruence, il est évidemment premier.

8. — Applications géométriques.

A. — *Groupe du triangle équilatéral*

Soit un triangle équilatéral ABC, dont les hauteurs se coupent en O. ABC reste globalement inchangé par les opérations suivantes : la rotation (O, + 120°) ; la rotation (O, + 240°) ; les symétries d'axes AO, BO, CO ; et, bien entendu, l'opération neutre (ou identique) qui transforme A, B, C en A, B, C.

Désignons ces opérations par : R pour la première rotation, R′ pour la seconde, H, H′, H″ pour les symétries d'axes AO, BO, CO. Convenons de représenter par RH l'opération qui consiste à faire subir au triangle la symétrie H, puis la rotation R.

Dans ces conditions, nous pouvons dresser une table de multiplication des six opérations I, R, R′, H, H′, H″. Elle est faite de manière que le résultat du produit RH se lit à l'intersection de la colonne intitulée H et de la ligne intitulée R.

	I	R	R′	H	H′	H″
I	I	R	R′	H	H′	H″
R	R	R′	I	H″	H	H′
R′	R′	I	R	H′	H″	H
H	H	H′	H″	I	R	R′
H′	H′	H″	H	R′	I	R
H″	H″	H	H′	R	R′	I

L'ensemble des six opérations possède la structure de groupe : le produit de deux éléments de l'ensemble appartient à l'ensemble ; I est l'élément neutre, et tout élément a un inverse. Mais le groupe n'est pas commutatif.

Le groupe peut être engendré par deux opérations seulement, car :

$$R' = R^2,\ I = R^3,\ H' = HR,\ H'' = RH.$$

On peut extraire du tableau précédent le suivant :

	I	R	R′
I	I	R	R′
R	R	R′	I
R′	R′	I	R

ou encore, en se servant uniquement de R et en convenant de remplacer R^3 ou I par R^0 :

	R^0	R^1	R^2
R^0	R^0	R^1	R^2
R^1	R^1	R^2	R^0
R^2	R^2	R^0	R^1

Nous constatons donc que les opérations I, R, R′ forment à elles seules un groupe, qui est un « sous-groupe » du groupe du triangle équilatéral. D'une façon générale, si un ensemble G a la structure de groupe pour une opération, on dit qu'une partie H de G est sous-groupe de G si elle est fermée pour l'opération du groupe, et si : $x \in H \Rightarrow x' \in H$, x' étant l'inverse de x dans G, pour l'opération du groupe.

Il résulte immédiatement de cette définition que l'élément neutre de H est celui de G, puisque : $xx' \in H$ et que $xx' = e$, e étant l'élément neutre de G.

Si nous utilisons la table du sous-groupe sous sa dernière forme (celle où l'on utilise uniquement R et ses puissances), et si nous faisons un tableau contenant uniquement les exposants de R, nous obtenons la table d'addition de Z/3. C'est ce qu'on exprime en disant que le sous-groupe (R) du triangle est isomorphe du groupe additif Z/3.

Du groupe du triangle, on peut encore extraire les sous-groupes : (I, H), (I, H′), (I, H″), tous trois isomorphes du groupe additif Z/2.

B. — *Groupe du carré*

Le carré admet huit opérations : l'opération neutre I ; trois rotations : R (O, 90°), R′ (O, 180°), R″ (O, 270°) ; quatre symétries : H, V, D, D′.

	I	R	R′	R″	H	V	D	D′
I	I	R	R′	R″	H	V	D	D′
R	R	R′	R″	I	D	D′	V	H
R′	R′	R″	I	R	V	H	D′	D
R″	R″	I	R	R′	D′	D	H	V
H	H	D′	V	D	I	R′	R″	R
V	V	D	H	D′	R′	I	R	R″
D	D	H	D′	V	R	R″	I	R′
D′	D′	V	D	H	R″	R	R′	I

Nous avons encore la structure de groupe non commutatif ; il peut être engendré par les seuls éléments R et H :

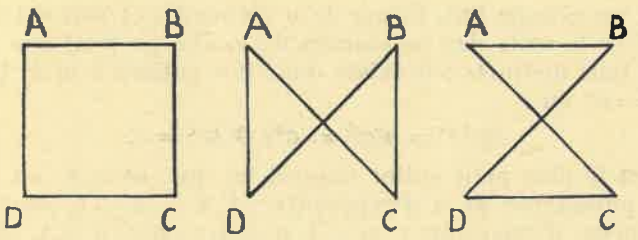
$$R' = R^2,\ R'' = R^3,\ I = R^4,\ \text{ou}\ R^0,$$
$$D = RH,\ D' = HR,\ V = HR^2.$$

On peut former avec I, R, R′ R″ un sous-groupe, isomorphe du groupe additif Z/4.

Remarque : Le groupe du triangle est formé de six éléments, et on constate aisément que les six opérations géométriques correspondent aux six permutations qu'on peut définir à partir de l'ensemble (A, B, C). Il n'en est pas de même pour le carré, car l'ensemble (A, B, C, D) engendre 24 permutations, alors que le groupe du carré n'en donne que 8. Cela s'explique : les 24 permutations de (A, B, C, D) peuvent se répartir en 6 parties formées chacune de 4 permutations circulaires ; elles corres-

pondent à un même quadrilatère parcouru dans le même sens à partir d'un sommet différent.

Ces six parties peuvent être groupées par deux, de manière à correspondre à un même quadrilatère parcouru dans des sens différents. Finalement, les 24 permutations se répartissent en 3 parties dont chacune correspond à un quadrilatère de sommets A, B, C, D.



D'une manière générale, avec n points, il y a n ! permutations, parmi lesquelles $(n-1)$! parties formées de permutations circulaires, et $\frac{1}{2}(n-1)$! polygones distincts dont les sommets sont les n points.

Remarques finales :

a) Le sous-groupe de rotations extrait du groupe du triangle est d'ordre 3, diviseur de l'ordre du groupe, 6. Il en est de même pour le sous-groupe (d'ordre 4) de rotations extrait du groupe (d'ordre 8) du carré. D'une manière générale :

Théorème : Dans un groupe d'ordre n, tout sous-groupe a pour ordre un diviseur de n.

Soit un groupe G, formé de n éléments, et un sous-groupe H de G, formé de n' éléments. Dans G, définissons une relation binaire : a et b seront congrus (mod H) s'il existe un élément $x \in H$ tel que l'on ait : $b = ax$. Démontrons que c'est une relation d'équivalence :

1) elle est réflexive, car : pour tout $a \in G$, $a = ae$ (e élément neutre de G, et de H) ;

2) elle est symétrique, car si x' est l'inverse de $x \in H$, nous avons :

$$b = ax \Rightarrow bx' = axx' = a \quad \text{ou : } a = bx' \quad \textbf{avec } x' \in H ;$$

3) elle est transitive, car:

$$b = ax \text{ et } c = by \Rightarrow c = a(xy) \quad \text{avec : } x \in H \text{ et } y \in H \Rightarrow xy \in H.$$

Cette équivalence détermine dans G une partition, et la classe d'un élément a de G contient : $ax_1, ax_2, \ldots, ax_i$, $x_i \in H$, éléments qui sont distincts, car : $ax_k = ax \Rightarrow x_k = x$, puisque les éléments d'un groupe sont simplifiables pour l'opération du groupe (voir la démonstration faite pour la simplification dans Z pour l'addition).

En résumé, toutes les classes de la partition sont formées d'un même nombre n' d'éléments, ce qui montre que l'ordre n de G est un multiple de l'ordre n' du sous-groupe H.

En particulier, si l'ordre de G est premier, G n'admet pas de sous-groupe proprement dit, c'est-à-dire autre que G lui-même et que le sous-groupe réduit à l'élément neutre e.

b) Le sous-groupe (R) du triangle présente cette particularité que tous ses éléments sont les puissances de l'un d'eux ; il en est de même du sous-groupe des rotations du carré. C'est ce qu'on appelle un « groupe cyclique ».

Soit G un groupe fini, formé de n éléments, et soit a l'un d'eux. Si l'on considère la suite des puissances de a, elle ne peut pas être formée d'éléments tous distincts ; il existe donc des entiers k et k' tels que l'on ait : $a^{k+k'} = a^k$ ou :

$$a^{k+k'} = a^k a^{k'} = a^k e \Rightarrow a^{k'} = e.$$

Si p est le plus petit entier naturel tel que $a^p = e$, on vérifie que toutes les puissances de a d'exposants : $1, 2, ..., p-1$, sont distinctes ; les puissances d'exposants : $p+1, p+2, ..., p+p-1$, donnent les mêmes éléments dans le même ordre, et ainsi de suite périodiquement.

En résumé, les puissances de a engendrent un groupe cyclique d'ordre p, et par suite p est un diviseur de n.

Nous pouvons considérer des exposants négatifs, en convenant de désigner l'inverse de a par a^{-1}. Dès lors, nous aurons :

$$a^x = a^y \Rightarrow x \equiv y \pmod{p}.$$

Si nous écrivons la table du groupe cyclique engendré par a, nous aurons celle du groupe $\mathbf{Z}/p$; donc :

Tout groupe cyclique d'ordre p est isomorphe du groupe additif $\mathbf{Z}/p$.

Remarque : Nous avons vu qu'un groupe fini d'ordre m premier ne peut avoir de sous-groupe proprement dit. Si a en est un élément, ses puissances engendrent un groupe cyclique dont l'ordre est diviseur de m. Donc, si a n'est pas l'élément neutre, ce sous-groupe cyclique doit coïncider avec le groupe lui-même. Autrement dit :

Tout groupe d'ordre premier est cyclique.

c) *Théorème de Fermat :* Soit $\mathbf{Z}/p$, p premier ; il y a $p-1$ classes non nulles, qui forment un groupe multiplicatif d'élément neutre 1. Si x est l'une d'elles, ses puissances engendrent un sous-groupe cyclique dont l'ordre est diviseur de l'ordre $p-1$ du groupe ; donc :

$$x^k \equiv 1 \Rightarrow x^{p-1} \equiv 1 \pmod{p} \qquad (\text{pour } x \not\equiv 0)$$

c'est le théorème de Fermat, qu'on peut encore traduire par :

$$x^p \equiv x \pmod{p}$$

quel que soit alors l'entier x.

Exercices

47) Une relation binaire R est dite « circulaire » si :

$$a\mathrm{R}b \text{ et } b\mathrm{R}c \Rightarrow c\mathrm{R}a.$$

Montrer qu'une relation R est réflexive et circulaire si, et seulement si, c'est une relation d'équivalence.

48) Examiner la validité du raisonnement suivant : soit R une relation binaire symétrique et transitive ; on a :

$$aRb \Rightarrow bRa, \text{ puis : } aRb \text{ et } bRa \Rightarrow aRa$$

donc, toute relation symétrique et transitive est aussi réflexive.

49) Peut-on réaliser une partition du plan considéré comme ensemble de points, de manière que les classes soient :

a) les droites issues d'un point donné A ;

b) les cercles d'un faisceau linéaire ?

50) Soit, dans le plan, une droite D. La relation entre points : $m\mathrm{R}m'$, lorsque m et m' appartiennent à un même demi-plan de frontière D, est-elle une relation d'équivalence ?

Entre les cercles du plan, on considère la relation : $c\mathrm{R}c'$ si les cercles c et c' sont confondus ou bien si leur axe radical est une droite fixe donnée. Cette relation est-elle une équivalence ?

51) Dans une population, on veut faire une classification basée sur les caractères suivants : être commerçant ; avoir une voiture ; avoir un réfrigérateur ; avoir une machine à laver. Enumérer les 16 classes de la partition qu'on peut construire à partir de ces caractères, en supposant qu'aucune ne soit vide.

52) Dans N, on envisage les lois de composition :

$$a^b \ ; \ a - b \ ; \ a\mathrm{T}b = ab - (a + b) \ ; \ a\mathrm{S}b = 2a - 3b.$$

($a\mathrm{T}b$ signifie que a et b sont associés par la loi désignée par T).

Etudier la commutativité et l'associativité.

53) Utiliser les tables d'addition et de multiplication de Z/7 pour vérifier les lois des deux opérations ; par exemple, calculer :

$$(3'.4').5' \ ; \ 3'.(4'.5') \ ; \ 3'(4' + 5') \ ; \ 3'.4' + 3'.5'.$$

54) Le groupe multiplicatif de Z/7 (c'est-à-dire l'ensemble des éléments non nuls) peut être engendré par les puissances du seul élément 3'. Il peut de même être engendré par les puissances de 5'.

55) Construire la table de multiplication de Z/12. Vérifier que les classes diviseurs de zéro correspondent à 2, 3, 4, 6, 8, 9, 10. Les classes 1, 5, 7, 11 ont un inverse et forment un groupe multiplicatif.

56) Nous avons énoncé l'axiome 6 de la multiplication sous forme de distributivité à gauche : $a(b + c) = ab + ac$. Etablir la distributivité à droite : $(b + c)a = ba + ca$.

57) L'axiome 7 de la multiplication admet que tout élément non nul est simplifiable pour la multiplication, et nous en avons déduit :

$$ab = 0 \Rightarrow a = 0 \quad \text{ou} \quad b = 0.$$

Montrer qu'inversement si l'on admet ce dernier énoncé, on peut démontrer l'axiome 7.

58) La congruence : $x^3 \equiv a \pmod 5$ a une solution, quel que soit l'entier a.

59) Quels sont les entiers a pour lesquels : $x^3 \equiv a \pmod 7$ a des solutions ?

60) Les 16 classes non nulles (mod 17) forment un groupe multipli-

catif qui peut être engendré par les puissances de la classe 3. Trouver les sous-groupes.

61) *Equations diophantiennes.* Soit l'équation : $5x - 7y = 1$; on peut la transformer en congruence : $5x \equiv 1 \pmod 7$. Si a est la solution de cette congruence, les x qui vérifient la première équation sont : $x = a + 7k$. En déduire les valeurs correspondantes de y.

De même, l'équation : $3x - 25y = 8$ donne : $y + 2 \equiv 0 \pmod 3$.

Résoudre :

$3x - 5y = 2$; $4x - 5y = 1$; $33x + 25y = 1$; $33x + 25y = 8$.

62) Résoudre les congruences :

$3x \equiv 2 \pmod 5$; $7x \equiv 4 \pmod{10}$; $243x + 17 \equiv 101 \pmod{725}$;
$4x + 3 \equiv 4 \pmod 5$; $6x + 3 \equiv 4 \pmod{10}$; $6x + 3 \equiv 1 \pmod{10}$.

63) Résoudre les systèmes de congruences :

$x \equiv 2 \pmod 5$ et $3x \equiv 1 \pmod 8$; $3x \equiv 2 \pmod 5$ et $2x \equiv 1 \pmod 3$.

64) Démontrer que : $D(ma, mb) = mD(a, b)$, m, a et $b \in \mathbf{N}$. En déduire :

$$a = a'd,\ b = b'd \text{ et } D(a', b') = 1 \Rightarrow D(a, b) = d.$$

65) Etudier l'ensemble : $xa + yb + zc$; en déduire que si a, b, c ont un pgcd d, il est de la forme : $d = ma + nb + pc$.

66) Démontrer que : $D[D(a, b), c] = D[a, D(b, c)] = D[D(a, c), b]$.

67) La règle de simplification est-elle valable pour la loi de composition $aTb = D(a, b)$? C'est-à-dire a-t-on :

$$D(a, b) = D(a, c) \Rightarrow b = c \text{ ?}$$

68) A partir de $D(a, b)$, chercher le plus petit commun multiple M de a et b. Montrer que : $Md = ab$.

A-t-on la règle de simplification :

$$M(a, b) = M(a, c) \Rightarrow b = c \text{ ?}$$

69) *Recherche pratique du pgcd.* Soit à déterminer $D(a, b)$. Si $b > a$ on divise b par a : $b = aq + r$. Si (a, b) désigne l'ensemble des diviseurs communs à a et b, montrer que : $(a, b) = (a, r)$. On recommence, en divisant le plus grand des deux entiers a et r par l'autre. Les nombres vont en décroissant ; on sera enfin amené à chercher les diviseurs communs à un entier d et à 0, qui sont ceux de d, lequel sera le pgcd de a et b.

Exemple : 77 715 et 37 215.

Au lieu d'employer la division ordinaire (q par défaut, r positif), on peut employer q par excès et r négatif, de manière à rendre le reste minimum en valeur absolue.

Comparer les deux méthodes avec les entiers 8382 et 1750 ; on a à faire 7 divisions dans un cas, 4 dans l'autre.

70) En utilisant la méthode précédente (algorithme d'Euclide), montrer que : $D(ma, mb) = mD(a, b)$.

71) Démontrer que pour que l'équation : $ax + by = c$ ait des solutions, il faut et il suffit que : $D(a, b) | c$.

Après avoir divisé les deux membres par $D(a, b)$, utiliser le théorème de Bezout, qui permet de trouver une solution particulière de l'équation. Montrer que la solution générale de l'équation affine $ax + by = c$ peut s'obtenir en ajoutant une solution particulière à la solution générale de l'équation linéaire associée $ax + by = 0$.

D'où une méthode pour résoudre les équations diophantiennes : on emploie l'algorithme d'Euclide pour chercher le pgcd de a et b, ce qui permet de l'obtenir sous la forme $ma + nb$; d'où une solution particulière de l'équation.

Exemples : $730x - 27y = 64$; $8x + 11y = 101$; $12x + 41y = 1$.

72) En utilisant l'algorithme d'Euclide, mettre le pgcd des deux nombres a et b sous la forme $ma + nb$ dans les cas suivants : 14 et 35 ; 11 et 15 ; 180 et 252 ; 2873 et 6643 ; 4148 et 7684 ; 1001 et 7655.

73) Si p est premier, $p|ab \Rightarrow p|a$ ou $p|b$.

74) Démontrer : $D(a, m) = D(b, m) = 1 \Rightarrow D(ab, m) = 1$.

75) Démontrer :

$$D(a, c) = d, \quad a|b \text{ et } c|b \Rightarrow ac|bd \text{ et } M(a, c) = ac/d.$$

76) Les produits des 12 classes de $Z/12$ par une classe diviseur de zéro, par exemple 9, ne donnent que quatre classes distinctes, toutes divisibles par 3.

D'une manière générale, si $D(a, m) = 1$, en multipliant par a les m classes (mod m), on obtient les mêmes m classes. Si $D(a, m) = d$, en multipliant les m classes par a, on a seulement m/d classes distinctes, toutes diviseurs de zéro et divisibles par d.

77) Si $D(a, m) = d$, la congruence : $ax \equiv b \pmod{m}$ a d solutions distinctes.

78) Ecrire les tables d'addition et de multiplication de $Z/9$; vérifier que les éléments autres que 0 et ses diviseurs forment un groupe multiplicatif.

79) Vérifier que le groupe additif $Z/6$ peut être engendré par les multiples de la classe 5' (groupe cyclique). Trouver les sous-groupes cycliques.

80) Pour tout entier x : $x^2 \equiv 0, 1$ ou $4 \pmod{8}$.

81) Montrer que $x^2 \equiv 35 \pmod{100}$ n'a pas de solution.

82) Si $x^2 \equiv a \pmod{65}$ a une solution, il en est de même pour

$$x^2 \equiv -a \pmod{65}.$$

83) Pour tout x impair non multiple de 3 : $x^2 \equiv 1 \pmod{24}$.

84) Montrer qu'aucun entier $x \equiv 7 \pmod{8}$ ne peut être une somme de trois carrés (utiliser l'exercice 80).

85) Si $D(m, m') = 1$, on peut résoudre les congruences simultanées : $x \equiv b \pmod{m}$ et $x \equiv b' \pmod{m'}$. Si x et x' sont deux solutions, on a :

$$x \equiv x' \pmod{mm'}.$$

86) Généralisation du 85 : étudier les congruences simultanées :

$$a_i x \equiv b_i \pmod{m_i} \text{ avec : } D(a_i, m_i) = 1,$$

les m_i étant premiers entre eux deux à deux.

87) Le groupe additif des classes (mod 60) peut être engendré par les multiples d'une classe première avec 60. Chercher les sous-groupes.

88) Sur Q, soit la loi de composition : $a\mathrm{T}b = (a + b)/2$. Montrer qu'elle n'est pas associative. Calculer :

$$a\mathrm{T}(b\mathrm{T}c)\ ;\ (a\mathrm{T}b)\mathrm{T}c\ ;\ (a\mathrm{T}c)\mathrm{T}b\ ;\ a\mathrm{T}(c\mathrm{T}b)\ ;\ \ldots.$$

Sur N, la même loi est-elle partout définie ?

89) Soit un ensemble E, sur lequel est définie une loi de composition T non associative. Etant donnés n éléments, pris dans un ordre déterminé, combien de « produits » différents peut-on former avec ces éléments, en les associant de diverses manières ? Faire le calcul pour $n = 3$, 4 et 5, pour lesquels les réponses sont respectivement 2, 5 et 12. Exemple : soit (dans Q) la loi : $a\mathrm{T}b = a + 1/b$. Etudier la commutativité, l'associativité. Pour 3 éléments a, b, c pris dans cet ordre, calculer les produits de l'exercice 88. Calculer les produits pour 4 éléments a, b, c, d pris dans cet ordre. Combien obtiendrait-on de produits en modifiant l'ordre des 4 éléments ?

90) Une loi de composition est définie par la table ci-dessous. Vérifier si elle est commutative : associative.

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

Résoudre des équations telles que : $x\mathrm{T}b = c$; $x\mathrm{T}x = x$; $x\mathrm{T}x = a$.

91) Dans Q, on considère la loi de composition : $a\mathrm{T}b = a + b + ab$. Etudier la commutativité ; l'associativité ; chercher s'il y a un élément neutre, les éléments qui ont un inverse ; la loi est-elle distributive pour l'addition ? Pour la multiplication ?

92) Dans l'ensemble des entiers naturels non nuls, on considère deux lois de composition : $a \circ b$ est le pgcd de a et b, $a\mathrm{T}b$ est le ppcm. Etudier la commutativité, l'associativité, montrer que la multiplication est distributive par rapport à chacune des deux lois.

93) En utilisant la distributivité des lois $\cup$ et $\cap$, démontrer formellement que, A et C étant des parties données de E, la relation $\mathrm{A} \cap \mathrm{B} = \mathrm{A} \cap \mathrm{C}$ est vérifiée par : $\mathrm{B} = \mathrm{A}' \cap \mathrm{C}$, A' étant le complément de A par rapport à E. Quelles sont les autres solutions ?

94) Soient les couples d'entiers (a, b) et (c, d), a et c non nuls. Montrer que la relation : $bc = ad$ est une relation d'équivalence.

95) Soient les couples d'entiers (a, b) et (c, d) ; montrer que la relation : $a + d = b + c$ est une relation d'équivalence.

96) Dans l'ensemble des entiers naturels, on considère les parties suivantes : les multiples de 7 ; les non multiples de 5 ; les impairs ; les entiers congrus à 2 (mod 5). Déterminer celles de ces parties qui sont fermées pour l'addition ; pour la multiplication.

97) Dans un groupe fini d'ordre pair, il existe, en dehors de l'élé-

ment neutre, un nombre impair d'éléments qui sont leurs propres inverses.

98) Etudier le groupe des opérations géométriques qui laissent invariant (globalement) un parallélogramme ; un rectangle.

99) Soit un polygone régulier de n côtés ; étudier le groupe des rotations qui laissent invariant le polygone.

100) Trouver l'ordre de chaque élément du groupe du carré.

101) Etudier le groupe de l'hexagone, et le sous-groupe qui laisse invariante une diagonale donnée.

102) Si G est sous-groupe de G' et G' sous-groupe de G", G est-il sous-groupe de G" ?

103) Dans le groupe du carré (avec les notations du texte), trouver X tel que : $RXR' = D$. Si l'on désigne par H^{-1} l'inverse de l'élément H de ce groupe, montrer que : $(RH)^{-1} = H^{-1} R^{-1}$ et vérifier que cette expression n'est pas égale à $R^{-1} H^{-1}$.

104) Montrer que le groupe du polygone régulier (ex. 99) peut être engendré par deux éléments R et H tels que : $R^n = I$ et $H^2 = I$.

105) Dans Z/6, les éléments autres que 0 et ses diviseurs forment un groupe multiplicatif ; à quel groupe connu est-il isomorphe ? Même question pour Z/9.

106) Dans Z/11, quels sont ceux des ensembles suivants qui forment un groupe multiplicatif :

(1, 3, 4, 5, 9) ; (1, 3, 5, 7, 8) ; (1, 8) ; (1, 10) ; (1, 10, 3).

107) Tout groupe d'ordre inférieur ou égal à 4 est commutatif.

108) Dans un groupe G, l'ensemble des éléments a tels que $ax = xa$ pour tout $x \in G$ est un sous-groupe de G, qu'on appelle centre de G. Chercher le centre du groupe du carré ; du groupe du polygone régulier de n côtés.

109) Chercher les sous-groupes des groupes suivants : Z/12 additif ; groupe du pentagone régulier ; de l'hexagone régulier.

110) Les éléments non nuls de Z/7 forment-ils un groupe cyclique ? Même question pour les éléments 1, 3, 5, 7 de Z/8 ; pour 1, 2, 4, 5, 7, 8 de Z/9.

111) Parmi les groupes suivants, y en a-t-il qui soient isomorphes : groupe du triangle équilatéral ; du carré ; des éléments non nuls du groupe multiplicatif Z/5 ; des rotations de l'hexagone régulier ; groupe additif Z/4 ; groupe additif Z/6.

112) Même question pour : le groupe des rotations du carré ; des symétries du rectangle ; des symétries du losange ; groupe multiplicatif de 1, 5, 8, 12 (mod 13) ; groupe multiplicatif de 1, 5, 7, 11 (mod 12).

113) A quelle condition un élément a d'un groupe cyclique d'ordre m engendre-t-il tout le groupe ? On dit alors que c'est un élément primitif. Chercher les éléments primitifs de Z/10, de Z/12.

114) Si un groupe formé de 6 éléments a un élément d'ordre 3, il est cyclique.

115) Soient deux entiers naturels a et b, et $D(a, b) = 1$. Le raison-

nement employé à propos des groupes cycliques montre que les puissances successives de a, divisées par b, donnent une suite périodique de restes ; le nombre de termes de la période est le plus petit entier k tel que : $a^k \equiv 1 \pmod{b}$.

Applications : On pourrait en déduire des règles de divisibilité pour les entiers écrits dans la numération décimale, par exemple par 7, mais elles ne seraient guère utilisables pratiquement.

Trouver les restes de : $3758^{79} \pmod{11}$; de $153^{21} \pmod{7}$.

116) Il existe deux types de groupes d'ordre 4 ; l'un est le groupe additif Z/4, l'autre le groupe des isométries du rectangle.

117) Chercher les groupes d'ordre 5, formé des éléments e, a, b, c, d. On remarquera qu'on doit associer à chacun des éléments a, b, c, d son inverse, et que le seul cas possible est celui où : $ab = cd = e$. La seule solution est un groupe isomorphe au groupe additif Z/5.

118) Quatre hommes possèdent en commun des cocotiers et un singe. Un jour, un premier homme prélève le quart des noix et comme il en reste une, il la donne au singe. Le deuxième jour, un deuxième homme prélève le quart des noix qui restent ; il y en a une de trop, il la donne au singe. Le jour suivant, un troisième homme fait de même. Enfin, le quatrième jour, les quatre hommes se partagent également les noix, et comme il y en a une de trop, ils la donnent au singe. Trouver le plus petit nombre de noix pour lequel le problème est possible.

Même question, en supposant que le quatrième homme agisse comme les trois premiers, et que le partage final se fasse le cinquième jour.

119) Sept personnes se partagent un nombre x d'objets, x n'étant pas divisible par 7. La première prend un objet et le septième du reste ; la deuxième prend 2 objets et 2/7 du reste, la troisième 3 objets et 3/7 du reste, ..., la septième prend 7 objets et 7/7 du reste. Trouver la plus petite valeur de x pour laquelle le problème est possible.