MATHÉMATIQUES ET SCIENCES HUMAINES

B. MONJARDET

Combinatoire et structures algébriques. I

Mathématiques et sciences humaines, tome 18 (1967), p. 33-40

<http://www.numdam.org/item?id=MSH_1967__18__33_0>

B. MONJARDET

COMBINATOIRE ET STRUCTURES ALGEBRIQUES I.

INTRODUCTION

Cet article est le premier d'une série où l'on se propose de présenter certains problèmes combinatoires plus ou moins classiques. Faisons dans le désordre l'inventaire de notions que nous rencontrerons: carrés latins, configurations, géométries finies, plans en blocs, réseaux, graphes réguliers ... Adoptant une méthode systématique, nous exposerons d'abord chacune de ces notions et certains des problèmes qu'elles posent. Nous réserverons pour la fin un des aspects les plus intéressants: l'équivalence de plusieurs de ces problèmes combinatoires en apparence étrangers. D'autre part plusieurs de ces problèmes peuvent être traités par des méthodes algébriques et notre premier article étudiera les structures algébriques utiles en de tels domaines.

Il est bien connu que plusieurs structures combinatoires ou algébriques que nous rencontrerons ont été étudiées ou réétudiées à propos de problèmes concrets; par exemple nécessité d'élaborer des plans d'expérience économiques en statistique ou recherche de certains codes en théorie de l'information. Au point de vue des méthodes, cette suite d'articles voudrait illustrer une remarque valable pour tout chercheur ayant à résoudre des problèmes mathématiques; la formulation du problème risque de dépendre encore trop des situations concrètes d'où il provient; il est alors recommandé d'essayer de traduire ce problème dans d'autres langages mathématiques; au mieux, on s'apercevra alors peut-être que le problème a déjà été traité, et dans tous les cas le problème aura été beaucoup approfondi dans cet exercice de traduction.

Signalons pour terminer que nous abordons des sujets très vastes dont nous ne traiterons qu'une faible partie renvoyant à des exercices et à une bibliographie pour le reste du sujet.

CORPS DE GALOIS - QUASI-CORPS - PRESQUE-CORPS

I. CORPS DE GALOIS

1.1. Définition

Un corps de Galois est un corps dont le nombre d'éléments est fini.

Nous rappelons d'abord la notion de corps.

Un ensemble K a une structure algébrique de corps si on a défini sur K deux lois de composition binaires vérifiant certaines propriétés. Notons + et $\times$ ces deux lois: ces propriétés s'énoncent, par exemple, ainsi:

- K est un groupe abélien pour la loi +, donc

  $\forall$ a, b, c $\in$ K $(a+b)+c = a+(b+c)$

  $\forall$ a, b $\in$ K $a+b = b+a$

  $\forall$ a, b $\in$ K l'équation $a+x = b$ a une solution unique

  (Il en résulte en particulier qu'il existe un élément neutre que nous noterons 0 : $0+x = x, \forall\, x \in K$)

- $K - \{0\}$ est un groupe pour la loi $\times$, donc

  $\forall$ a, b, c $\in K - \{0\}$ $(a\times b)\times c = a\times(b\times c)$

  $\forall$ a, b $\in K - \{0\}$ les équations $a\times x = b$ et $y\times a = b$ ont une solution unique. (Il en résulte l'existence d'un élément neutre pour la loi $\times$; nous le noterons 1)

- La loi $\times$ est distributive par rapport à la loi +, donc

  $\forall$ a, b, c $\in$ K $a\times(b+c) = (a\times b) + (a\times c)$

  $(a+b)\times c = (a\times c) + (b\times c)$

De ces axiomes on déduit toutes les règles de calcul dans un corps; par exemple, l'élément 0 est absorbant: $0\times x = x\times 0 = 0$, $\forall\, x \in K$. (Le démontrer).

Ces règles de calcul sont bien connues et utilisées couramment puisque, par exemple, l'ensemble des nombres rationnels est un corps (pour les opérations d'addition et de multiplication usuelles). Dans cet exemple le nombre d'éléments du corps est infini: il en est de même dans le cas du corps des nombres réels ou du corps des nombres complexes.

1.2. Corps de restes dans Z

Nous recherchons maintenant s'il existe des corps K_n finis à n éléments; K_n est dit alors d'ordre n. Puisque dans K, il existe toujours deux éléments particuliers distincts 0 et 1, on a $n \geqslant 2$. Si $n = 2$, l'ensemble K_2 sera égal à $\{0, 1\}$. En raison des propriétés du 0 et du 1, les tables de l'addition et

de la multiplication de K_2 sont complètement déterminées ci-dessous:

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Le lecteur vérifiera que K_2 est bien un corps et s'assurera aisément qu'il ne peut exister d'autre corps à deux éléments.

Donnons une illustration (ou "représentation") de K_2: considérons l'anneau Z des entiers relatifs et faisons une partition de Z en deux classes: P classe des nombres pairs, I classe des nombres impairs. Soit E l'ensemble de ces deux clases; $E = \{P, I\}$; définissons sur E une addition $\dot{+}$ et une multiplication $\dot{\times}$; d'après les "règles de parité" la somme de deux nombres pairs est un nombre pair, le produit de deux nombres pairs est un nombre pair etc ...; on obtient les deux tables suivantes:

$\dot{+}$	P	I
P	P	I
I	I	P

$\dot{\times}$	P	I
P	P	P
I	P	I

Il est alors immédiat de vérifier que l'application de K_2 sur E, qui envoie 0 en P et 1 en I est un isomorphisme (application f bijective telle que $f(x+y) = f(x) \dot{+} f(y)$ et $f(x \times y) = f(x) \dot{\times} f(y)$.

Jusqu'ici nous n'avons obtenu que le corps à 2 éléments K_2 ; existe-t-il d'autres corps à n éléments K_n ? L'exemple précédent se généralise et donne une première réponse à cette question. Nous avions défini une partition de Z en deux classes; à cette partition est associée une relation d'équivalence:

$$x \equiv y \iff x - y \text{ est multiple de } 2$$

On peut alors étudier les classes de la relation d'équivalence définie par:

$$x \equiv y \iff x - y \text{ est multiple de } n$$

Cette équivalence porte le nom de congruence modulo n; il est facile de voir qu'elle partitionne l'ensemble Z en n classes, les classes correspondant aux restes de la division par n dans Z. L'ensemble quotient noté $Z/_{(n)}$ est donc un ensemble à n éléments; on définit une addition et une multiplication sur $Z/(n)$ de la manière suivante: soient X et Y deux classes, x et y deux éléments appartenant à ces classes (ou "représentants"), on pose

$$X \dot{+} Y = \text{ classe de } (x+y)$$

$$X \dot{\times} Y = \text{ classe de } (x \times y)$$

(Le lecteur montrera que le résultat de ces opérations sur X et Y est indépendant du choix des représentants x et y).

Exercice 1.

Ecrire les tables des deux opérations $\dot{+}$ et $\dot{\times}$ pour $Z/(3)$, $Z/(4)$, $Z/(5)$. Montrer que dans $Z/(4)$, il existe des "diviseurs de zéro" (éléments non nuls dont le produit est nul).

Exercice 2.

Montrer que $Z/_{(n)}$ est un anneau: c'est à dire que $\dot{+}$ est une loi de groupe abélien et que $\dot{\times}$ est une loi associative, distributive par rapport à $\dot{+}$. Cet anneau est de plus commutatif et unitaire.

Exercice 3.

Démontrer que pour que $Z/_{(n)}$ soit un corps, il faut et il suffit que l'entier n soit un nombre premier.

1.3. Corps primaire

La proposition de l'exercice 3 montre par construction l'existence d'au moins un corps K_p, pour tout nombre premier p. Ce corps est-il unique (aux isomorphismes près) ? Existe-t -il des corps K_n pour n non premier ? La réponse à ces questions est un peu plus délicate; nous ne donnerons que les résultats et des indications en exercices, renvoyant à la note bibliographique pour l'étude complète du sujet. Le résultat fondamental est le suivant: il existe un corps K_n si et seulement si n est un nombre primaire c'est à dire une puissance d'un nombre premier: $n = p^k$; ce corps est unique. Pour $n = p^k$ (p premier, $k > 1$) on a une construction du corps correspondant K_n à partir du corps K_p ; K_n est obtenu comme "extension " de K_p par rapport à un polynome irréductible de degré k de K_p ; K_p sera alors un sous-corps de K_n et K_n un sur-corps de K_p.

Exercice 4.

Soit le corps K_3 . Montrer que l'équation $x^2+1 = 0$ n'a pas de racine dans K_3. On considère $\overline{K}$ ensemble des éléments de la forme x+iy, x et y éléments de K_3, i "racine formelle" du polynome x^2+1. On définit une addition et une multiplication sur $\overline{K}$ par:

$$(x+iy) \dot{+} (x'+iy') = (x+x') + i(y+y')$$
$$(x+iy) \dot{\times} (x'+iy') = (xx'-yy') + i(xy'+yx')$$

Montrer que $\overline{K}$ est un corps à 9 éléments qui contient un sous-corps isomorphe à K_3.

Exercice 5.

Soit le corps K_5 (isomorphe à $Z/(5)$). Dresser la table de la fonction $x \longrightarrow y = x^2$ dans ce corps. En déduire que les polynomes x^2+2 et x^2+3x+4 sont irréductibles dans K_5 (c'est-à-dire qu'ils ne s'annulent pour aucune valeur de K_5).

On considère $\overline{K}$ ensemble des éléments de la forme x+iy, x et y éléments de K_5, i racine formelle du polynome x^2+2; donc $i^2 = 3$.

On définit sur $\overline{K}$ une addition et une multiplication en posant

$$(x+iy) \dot{+} (x'+iy') = (x+x') + i(y+y')$$
$$(x+iy) \dot{\times} (x'+iy') = (xx'+3yy') + i(xy'+yx')$$

Montrer que $\overline{K}$ est un corps: c'est l'extension de degré 2 du corps K_5 par le polynome irréductible x^2+2. On considère de même $\overline{K}$ ensemble des éléments de la

forme x+jy, x et y éléments de K_5, j racine formelle du polynome x^2+3x+4; donc $j^2 = 2j+1$.

On définit sur $\overset{o}{K}$ l'addition et le multiplication par:

$$(x+jy) \dot{+} (x'+jy') = (x+x') + j(y+y')$$

$$(x+jy) \dot{\times} (x'+jy') = (xx'+yy') + j(yx'+xy'+2yy')$$

Montrer que $\overset{o}{K}$ est un corps isomorphe à $\overline{K}$.

Finalement on obtient le corps à p^r éléments par extension de K_p à partir d'un polynome irréductible de degré r sur K_p, toutes les extensions par des polynomes irréductibles de même degré étant isomorphes.

1.4. Remarques

- Pour n compris entre 2 et 10, il n'existe pas de corps K_n pour les valeurs 6 et 10.

- Signalons un résultat intéressant de l'étude des corps finis. Tout corps fini K est commutatif (c'est-à-dire $K - \{0\}$ est un groupe abélien pour la loi multiplicative) (Théorème de Wedderburn 1905).

- Les corps finis s'appellent corps de Galois. Ils ont été en effet introduits par ce mathématicien à propos de la résolution des équations algébriques. La théorie de l'extension des corps et de la correspondance entre corps et groupes liés à une équation algébrique a pris le nom de théorie de Galois. Le terme même de corps date de la fin du XIX^e siècle avec Dedekind et Steinitz.

- La solution des exercices 1, 2, 3, 4 se trouve dans PAPY-MATHEMATIQUES MODERNES-5 DIDIER 1966 - Chapitres VII et XII.

II. CORPS - QUASI-CORPS - PRESQUE-CORPS

Dans le plan habituel, muni d'un repère, l'assertion: le point (x,y) appartient à la droite (a,b) se traduit algébriquement par la relation y = ax+b. y, a, x, b sont des nombres réels.

Puisque par deux points distincts, il passe une droite et une seule, le système d'équations:

$$(1) \quad \begin{cases} y_1 = ax_1 + b & \text{avec } x_1 \neq x_2 \\ y_2 = ax_2 + b & \text{ou } y_1 \neq y_2 \end{cases}$$

doit admettre une solution unique (a,b). Appelons P_1 cette propriété.

De même puisque deux droites distinctes s'intersectent en un point unique, le système d'équations:

$$\begin{cases} y_1 = a_1x + b_1 & \text{avec } a_1 \neq a_2 \\ y_2 = a_2x + b_2 & \text{et } b_1 \neq b_2 \end{cases}$$

doit admettre une solution et une seule (x,y). Appelons P_2 cette propriété.

Que les systèmes (1) et (2) vérifient bien les conditions d'existence et d'unicité d'une solution, résulte immédiatement des propriétés du corps des nombres réels.

Dans ce paragraphe nous allons rechercher des structures algébriques finies pour lesquelles les propriétés P_1 et P_2 sont vérifiées; de telles structures serviront à coordonner des "géométries planes finies", comme cela sera montré dans un article ultérieur.

Soit donc à trouver E ensemble fini devant être muni de deux opérations: addition et multiplication et devant vérifier P_1 et P_2 . Un premier exemple nous est fourni par les corps finis; on vérifie en effet immédiatement que pour un corps quelconque, en particulier fini, on a bien P_1 et P_2 .

Une autre structure algébrique classique faisant intervenir deux opérations + et o est la structure d'anneau: un anneau A est un groupe abélien muni en outre d'une multiplication associative et distributive par rapport à l'addition; cherchons alors si un anneau vérifie les propriétés P_1 et P_2.

Considérons, par exemple, le système d'équations

$$\begin{cases} y = a_1 x + b_1 \\ y = a_2 x + b_2 \end{cases} \qquad \begin{matrix} a_1 = a_2 \\ b_1 = b_2 \end{matrix}$$

Donc $a_1x + b_1 = a_2x + b_2$

$(a_1-a_2)x = b_2- b_1$

Posons $a_1-a_2 = c$, $b_2-b_1 = d$; on est ramené à l'étude de l'équation $cx = d$. Or dans un anneau une telle équation peut avoir 0, une ou plusieurs solutions. Par exemple, dans l'anneau $Z/(4)$ les équations $2x = 1$ et $2x = 2$ ont respectivement 0 et 2 solutions. Donc un anneau ne vérifie pas en général les propriétés P_1 et P_2. Pour qu'il les vérifie, il faut que l'équation $cx = d$ ait une solution et une seule; dans ce cas (A,o) est un quasi-groupe, et puisque la loi multiplicative o est associative, c'est un groupe. Donc finalement A est un corps, ce qui nous ramène à notre premier exemple.

Pour trouver d'autres exemples proches de la structure d'anneau, il faut donc modifier cette structure de façon adéquate. Soit E un ensemble muni de deux opérations + et • ; on supposera d'abord que (E,+) est un groupe abélien; d'après les lignes précédentes, nous posons (E, •) est un quasi-groupe, ou encore (E, .) est une boucle (quasi-groupe avec élément neutre); mais toujours dans les lignes précédentes le lecteur attentif remarquera que la distributivité à droite de la multiplication par rapport à l'addition a joué un rôle; il faut donc l'introduire. Finalement on va être amené à la structure suivante:

E est un ensemble muni de deux opérations + et • ;
(E,+) est un groupe abélien d'élément neutre 0
(E- {0}, •) est une boucle d'élément neutre 1
$(a+b) \bullet x = a \bullet x + b \bullet x$, pour tout (a,b,x) de E . (distributivité à droite de . par rapport à +)

$0 \bullet x = x \bullet 0 = 0$, pour tout x de E.

Un tel système s'appelle système de Veblen-Wedderburn droit, ou quasi -corps droit. (On définit de façon analogue un quasi-corps gauche).

On démontre que les axiomes précédents entraînent la propriété suivante: l'équation $x \cdot a = x \cdot b + c$ a une solution et une seule, pour tout (a, b, c) de E^3 avec $a \neq b$.

D'autre part on peut construire effectivement de tels systèmes ayant p^{2n} éléments: p premier, n entier quelconque: ce sont les systèmes de Hall. Nous donnerons en exercice un exemple de tel système à 9 éléments. On peut aussi construire des quasi-corps à p^n éléments: p premier impair, n impair >1 ; ce sont les systèmes d'Albert.

Peut-on trouver maintenant d'autres structures algébriques vérifiant P_1 et P_2? On peut songer à enrichir la structure de quasi-corps droit.

Une première méthode consiste à supposer la multiplication associative: $E^* = E - \{0\}$ est alors un groupe pour $\cdot$. Mais $(E, +, \cdot)$ n'est pas un corps, la distributivité à gauche de $\cdot$ par rapport à + n'étant pas vérifiée; une telle structure est appelée presque-corps droit; tous les presque-corps ont été déterminés (Zassenhaus - 1935); ils ont p^r éléments pour certaines valeurs de r.

Au lieu de supposer la multiplication associative, on peut supposer la distributivité vérifiée à gauche et à droite. Si de plus, on suppose la règle de simplification suivante: Pour tout $a \neq 0$, il existe a^{-1} tel que $(b \cdot a) \cdot a^{-1} = a^{-1} \cdot (a \cdot b) =$ on obtient un système de Moufang, ou anneau de division alternatif. Mais on démontre alors que dans le cas fini, on peut déduire de ces axiomes, l'associativité de la loi multiplicative. C'est le théorème d'Artin- Zorn: tout anneau de division alternatif fini est un corps.

En résumé, on a obtenu trois structures algébriques différentes vérifiant les propriétés P_1 et P_2 : système de Veblen-Wedderburn, presque-corps, corps finis; dans ces trois cas la loi + est une loi de groupe abélien, la loi $\cdot$ étant au moins une loi de boucle.

Exercice 6.

On considère le corps K_9 (cf.exercice 4); $K_9 = \{(a+bi),\ a,\ b \in K_3,\ i^2 = -1\}$.

On appelle conjugué de $z = a+bi$, l'élément $\bar{z} = a - bi$.

Sur cet ensemble à 9 éléments on définit une nouvelle structure. Pour cela on conserve l'addition de K_9 mais on définit une nouvelle multiplication o de la manière suivante:

$z \circ z' = \bar{z}\, z'$ si $z' = a' + ib'$, a' et b' différents de zéro

$z \circ z' = z\, z'$ si $a' = 0$ ou $b' = 0$

Ecrire la table de cette opération; montrer que o est une loi de boucle non associative, et que o est distributive à droite mais non à gauche par rapport à +. On obtient ainsi un système de Veblen-Wedderburn droit.

NOTE BIBLIOGRAPHIQUE

I. CORPS DE GALOIS

Pour l'historique des corps et de la théorie de Galois, on consultera le chapitre Polynomes et corps commutatifs de N. BOURBAKI - Eléments d'histoire des mathématiques - Hermann - Paris - 1960.

Le passage où Galois crée ses corps se trouve dans l'article sur la théorie des nombres - Bulletin de Ferusac - Oeuvres complètes de Galois.

Le premier exposé systématique de la théorie de Galois se trouve dans:L.E. DICKSON - Linear groups with an exposition of the Galois field theory -(1900 -Réédité en 1958 chez Dover - New-York 3121).

Les chapitres I, II et IV étudient les corps de Galois; l'ouvrage a vieilli mais est encore très lisible.

Un exposé très complet se trouve au chapitre IX de CARMICHAEL - Introduction to the groups of finite order - 1937 - Réédition Dover - 1956. Dans ces deux présentations, l'étude des corps finis est menée presque indépendamment de l'étude des extensions de ces corps. Il en est de même dans: D. DUGUE - Traité de statistique - Tome 2 - Algèbre aléatoire - Paris - Masson - 1958 - II 240-255.

Par contre dans les exposés plus récents la tendance est de présenter d'abord la théorie des extensions algébriques et d'utiliser ses résultats pour l'étude des corps finis; l'exposé y gagne en concision mais nécessite plus de connaissances préalables.

Dans ce style, on trouve:

A.A. ALBERT - Fundamental concepts of higher algebra - Chicago University Press - 1956 - 165 p.

Le but du livre est le dernier chapitre consacré aux corps finis; l'avant dernier chapitre traitant des extensions de corps.

B.L. VAN DER WAERDEN - Modern algebra - Vol. 1 - Frederick Ungar Publishing C - New York 1953.

Particulièrement recommandable par sa concision et sa clarté; les pages 115 à 119 traitent des corps finis et disent l'essentiel.

II. PRESQUE-CORPS, QUASI-CORPS

Ces structures algébriques sont liées aux géométries planes finies; on consultera donc la bibliographie de ces derniers (voir article ultérieur). Citons cependant déjà:

HALL - Theory of groups - Prentice Hall - 1959 où le dernier chapitre qui traite des plans projectifs contient des paragraphes spéciaux sur les systèmes de Veblen-Wedderburn et de Hall, sur la démonstration des théorèmes de Wedderburn et d'Artin-Zorn, et sur les presque-corps.

N. BOURBAKI - Eléments de Mathématiques - Livre II Algèbre, chapitre V (voir en particulier les pages 168-9).

A suivre.