

Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 45 (1970)

Artikel: Validité dans les algèbres de Boole partielles.
Autor: Coray, Giovanni
DOI: <https://doi.org/10.5169/seals-34643>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 17.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Validité dans les algèbres de Boole partielles

par GIOVANNI CORAY

Introduction

Les algèbres de Boole donnent lieu à une interprétation naturelle de la logique propositionnelle classique; en particulier, on sait qu'une expression propositionnelle est valide dans toutes les algèbres de Boole si, et seulement si, elle est une tautologie. Par conséquent, certaines propriétés de la déduction dans le calcul propositionnel classique peuvent être démontrées à l'aide d'arguments de caractère algébrique. Les algèbres de Boole partielles (*ABP*) définies dans [1] permettent, de manière analogue, l'étude du calcul propositionnel partiel. Ce dernier est un affaiblissement du calcul propositionnel classique [2] suggéré par la mécanique quantique.

Il résulte de la semi-simplicité des algèbres de Boole qu'une expression propositionnelle est universellement valide si elle est valide dans l'algèbre de Boole simple \mathbf{Z}_2 . On ne retrouve pas cette situation privilégiée dans le cas des *ABP*; en effet, il n'est pas possible d'établir la validité des expressions propositionnelles (ou des règles de déduction) par la vérification dans une algèbre finie déterminée.

Cependant, on dispose d'un autre procédé de décision pour la validité dans les algèbres de Boole; il consiste à vérifier l'expression propositionnelle donnée à l'aide d'une seule évaluation dans une algèbre libre adéquate. Nous proposons, dans ce travail, une définition des *ABP* libres permettant d'étendre ce critère au cas des *ABP*.

Ainsi, le problème central de cette étude est la représentation et la construction effective de certaines *ABP* libres.

La méthode de représentation est basée sur deux faits: d'une part, toute *ABP* peut être caractérisée par une famille d'algèbres de Boole finies et d'isomorphismes partiels; d'autre part, on peut décrire un tel isomorphisme partiel par une relation binaire définie dans l'espace dual des algèbres de Boole. Cette manière de représenter les *ABP* facilite la mise au point d'un algorithme pour la construction d'une *ABP* libre déterminée. L'emploi de cet algorithme conduit toutefois à une suite d'opérations à l'aide de relations binaires de domaine fini, pour lesquelles l'emploi d'un ordinateur se révèle judicieux.

Pour chaque expression propositionnelle (et plus généralement pour toute règle de déduction) donnée, une calculatrice dûment programmée peut ainsi construire l'*ABP* libre adaptée et exécuter l'évaluation décisive. Les tautologies déduites dans *Principia Mathematica* ont été soumises à ce test (sur la machine CDC 1604A du Centre de Calcul, EPF, Zurich). Il en résulte que seules les trois expressions 2.81,

3.47 et 4.38 (ainsi que 3.48 et 4.39, obtenues par simple substitution dans 3.47 et 4.38) ne sont pas valides dans les *ABP*.

Il est à noter que ces expressions ont quatre variables. D'autre part, on sait que les identités Booléennes en une ou deux variables sont également valides dans les *ABP* [1], alors que les identités à trois variables ont fait jusqu'ici l'objet de conjectures. Nous en démontrons la validité à l'aide d'une classification des *ABP* libres à trois éléments générateurs.

Dans les *ABP* produites à cet effet, on peut observer la présence fréquente d'une sous-algèbre très particulière: l'analyse plus détaillée de ces *ABP* suggère une démonstration «algébrique» de leur plongeabilité dans une algèbre de Boole. Outre cet élément heuristique, l'ordinateur apporte une information indispensable, par l'énumération de quelques 60 cas traités isolément, pour la preuve complète que toute *ABP* libre à trois générateurs est plongeable dans une algèbre de Boole.

Le sujet est présenté en trois chapitres. Les *ABP* ont un trait caractéristique: les opérations à deux arguments n'y sont définies que pour certaines paires d'éléments. Cependant, comme les algèbres de Boole classiques, elles ont deux unités. Pour les structures de ce type nous donnons, dans la première partie de ce travail, une définition idoine des notions de satisfaction et de validité. L'usage continu de ces notions permet une démonstration concise de quelques propriétés algébriques. Nous dégagons de celles-ci plusieurs critères pratiques pour la plongeabilité dans une algèbre de Boole.

La deuxième partie est consacrée à une méthode de représentation des *ABP* à l'aide de relations binaires finies. Nous y développons ensuite un procédé de construction pour certaines *ABP*, sous forme aisément traduite dans un langage de programmation.

Ce procédé s'applique, en particulier, aux *ABP* libres introduites dans la troisième partie de cette étude. C'est dans ce dernier chapitre que nous démontrons la validité, dans les *ABP*, de certaines règles du calcul propositionnel classique, en particulier des identités Booléennes en trois variables.

I. Propriétés algébriques des algèbres de Boole partielles

I.1. Structures et algèbres de Boole partielles

DÉFINITION. Une *structure* (ou structure d'algèbre partielle) est un système d'ensembles et de relations du type

$$A = (S, C, 0, 1)$$

où S est un ensemble et C une relation ternaire univoque en son dernier argument, interprétée comme une fonction à deux variables définie sur une partie de $S \times S$, tandis que 0 et 1 sont deux éléments distingués de S .

Par exemple, une algèbre de Boole, dont S est l'ensemble de tous les éléments, 0 l'élément minimal, 1 l'élément maximal et C l'opération définie pour tous a, b dans S par $C(a, b) = \neg a \vee b$, est une structure.

La généralisation suivante des algèbres de Boole, où l'opération C n'est pas partout définie, est proposée dans [1]. Soit D la relation binaire de base S telle que aDb ssi $C(a, b)$ est définie dans A . D est la relation de *compatibilité* entre éléments de A .

DÉFINITION. Une *algèbre de Boole partielle* (*ABP*) est une structure $A = (S, C, 0, 1)$ telle que

- D est réflexive et symétrique. Pour tout élément a de S : $aD1$ et $aD0$.
- tout triplet a, b, c de S tel que aDb, bDc, aDc engendre une algèbre de Boole dans A .

Soit A une *ABP*. Une famille quelconque d'éléments de A deux à deux compatibles engendre une algèbre de Boole. En particulier, les restrictions de A aux parties maximales de S formées d'éléments deux à deux compatibles sont des algèbres de Boole; l'ensemble de ces restrictions induit à son tour l'opération C de A . Cette idée est développée dans le § II.1, en vue de la représentation des *ABP*.

D'autre part, on peut caractériser les *ABP*, parmi les structures, par la validité de certaines règles du calcul propositionnel classique. Une remarque analogue vaut pour les structures plongeables dans une algèbre de Boole. La notion de validité s'avère ainsi très efficace pour la construction de nouvelles *ABP* et l'établissement de critères de plongeabilité. Enfin, le concept d'*ABP* libre est étroitement lié à la notion de satisfaction. Ces éléments sont introduits, dans le paragraphe suivant, à l'aide de *définitions* détaillées.

I.2. Validité dans les structures partielles

Soit V un ensemble dénombrable, fini ou vide. Les éléments de V seront appelés *variables* et notés x, y, z, x_1, x_2, \dots . Le cas le plus fréquent sera $V = \{x, y, z\}$. L'ensemble des *expressions propositionnelles*, pour V donné, est noté FV . C'est l'ensemble minimal d'expressions formées avec un alphabet contenant les symboles C, f , ainsi que les variables, tel que: $f \in FV$, $V \subseteq FV$ et $Cpq \in FV$ lorsque $p, q \in FV$. Les expressions propositionnelles sont notées p, q, r, p_1, p_2, \dots et aussi Cpq pour la «concaténation» de C avec deux expressions propositionnelles p, q . On utilisera également les «abréviations» courantes:

$\neg p$	pour	Cpf
$p \vee q$	pour	$CCpfq$
$p \wedge q$	pour	$CCpCqff$
$p \equiv q$	pour	$Cpq \wedge Cqp$

ainsi que $p \circ q$ pour $CfCpq$.

Soit $A = (S, C, 0, I)$ une structure et V un ensemble de variables. Une *valuation* dans A est une application v de V dans S , notée $v: V \rightarrow A$.

Une *valuation étendue* dans A est une application \bar{v} de \bar{V} dans S , notée $\bar{v}: \bar{V} \rightarrow A$, telle que:

- a) $V \subseteq \bar{V} \subseteq FV$
- b) pour tous p, q dans $FV: Cpq \in \bar{V}$ ssi C est définie pour $\langle \bar{v}(p), \bar{v}(q) \rangle$ dans A , $p \in \bar{V}$ et $q \in \bar{V}$.
- c) pour tous p, q dans FV tels que $Cpq \in \bar{V}: \bar{v}(Cpq) = C(\bar{v}(p), \bar{v}(q))$.
- d) $f \in \bar{V}$ et $\bar{v}(f) = 0$.

PROPOSITION 1. Pour une valuation $v: V \rightarrow A$ donnée, il existe une valuation étendue unique $\bar{v}: \bar{V} \rightarrow A$, dont la restriction à V coïncide avec v . Son domaine de définition \bar{V} est déterminé univoquement par v .

\bar{v} sera appelée *l'extension* de v . La démonstration est ramenée au cas classique si on ajoute à A un élément auxiliaire α et si on donne à C la valeur α chaque fois que C n'a pas de valeur définie dans A . On obtient ainsi une application de FV dans $S \cup \{\alpha\}$ dont il suffit de prendre la restriction à S .

Une expression propositionnelle p est *satisfaite par* une valuation v , ou v *satisfait à* p , si $p \in \bar{V}$ et $\bar{v}(p) = I$.

Une *règle*, dans l'acception la plus générale, est un couple d'ensembles M, M' d'expressions propositionnelles; les éléments de M sont appelés prémisses, ceux de M' conclusions.

Une règle est *valide* dans une structure A si ses conclusions sont satisfaites par toute valuation dans A qui satisfait à l'ensemble des prémisses. On note $A: M \Vdash M'$ une règle $\langle M, M' \rangle$ valide dans A . Une règle valide dans toutes les ABP est notée $M \Vdash M'$; pour $M = \{p_1, \dots, p_m\}$ fini et $M' = \{q\}$ l'usage est d'écrire $p_1, \dots, p_m \Vdash q$ au lieu de $M \Vdash M'$.

THÉORÈME 1. Une structure $A = (S, C, 0, I)$ est une ABP ssi les règles suivantes y sont valides pour un ensemble V d'au moins trois variables:

- R₁ $p \Vdash Cf p$
 - R₂ $Cf Cq p \Vdash Cf p$
 - R₃ $CCpff \Vdash p$
 - R₄ $Cf Cp q \Vdash Cp Cq p$
 - R₅ $p \circ q, p \circ r, q \circ r \Vdash CCp Cq r CCp q Cpr$
 - R₆ $p, Cp q \Vdash q$
 - R₇ $p \circ q, Cq r, Cr q \Vdash p \circ r$
- pour tous p, q, r dans FV , ainsi que
- R₈ $\Vdash Cf p$
- pour les variables p dans V .

Démonstration. On vérifie aisément la validité de R_1 – R_8 dans toute ABP . Réciproquement, la validité de R_8 dans une structure A fait que, pour toute valuation $v: V \rightarrow A$, $\bar{v}(p) D \bar{v}(q)$ ssi v satisfait à $p \perp q$. Si V a trois variables ou plus, on peut toujours trouver une valuation v telle que $v(p)=a$, $v(q)=b$, $v(r)=c$ dans A ; les propriétés qui définissent les ABP (Déf. fin §I. 1) découlent alors des règles S_{27} , S_1 , S_8 , S_2 et des métarègles M_1 , M_2 [3], dérivées de R_1 – R_7 .

Le théorème reste vrai si on remplace p, q, r par des variables x, y, z respectivement, avec $V = \{x, y, z\}$. La validité de R_8 entraîne alors celle de R_1 et R_2 ; on peut d'ailleurs omettre également R_7 . Cependant, le système R_1 – R_8 est complet dans le sens suivant:

Une règle $M \vdash M'$ est valide dans toutes les ABP ssi elle est dérivable de R_1 – R_8 .

La démonstration, donnée dans [3] pour le cas $Cfp \vdash p$, consiste à construire une structure A et une valuation $v: V \rightarrow A$ telles que $p \in FV$ soit satisfaite par v ssi la règle $M \vdash p$ est dérivable de R_1 – R_8 . Elle repose essentiellement sur la règle S_{40} dérivée de R_1 – R_7 et peut être généralisée pour M quelconque. (Cf. § III.1, Existence de l' ABP universelle.)

THÉORÈME 2. Une structure $A = (S, C, 0, 1)$ est plongeable dans une algèbre de Boole ssi

$$A: Cfp, Cfq \vdash p \equiv q$$

pour toutes les expressions p et q de FV , V dénombrable, telles que $p \equiv q$ est une identité Booléenne (valide dans Z_2).

La démonstration donnée dans [4] Th. 4, p. 84 pour les ABP , trouve sa «généralisation» naturelle dans le cas des structures. La condition suffisante pour la plongeabilité dans une algèbre de Boole peut être affaiblie; il suffit d'examiner les identités $p \equiv q$, valides dans Z_2 , où p et q sont des expressions propositionnelles formées à l'aide de variables et de l'opérateur C uniquement (à l'exclusion de la «constante» f):

COROLLAIRE. Une ABP est plongeable dans une algèbre de Boole ssi $A: Cfp, Cfq \vdash p \equiv q$ pour toutes les expressions p et q de FV , qui ne contiennent pas le symbole f , et pour lesquelles $p \equiv q$ est valide dans Z_2 .

Démonstration. Soient $Cfp, Cfq \vdash p \equiv q$ une règle valide dans Z_2 et $v: V \rightarrow A$ une valuation satisfaisant à Cfp, Cfq , mais pas à $p \equiv q$; on a donc $\bar{v}(p) \neq \bar{v}(q)$ dans A . Nous montrons l'existence d'une règle $Cfp', Cfq' \vdash p' \equiv q'$ et d'une valuation v' avec les mêmes propriétés, p' et q' étant des expressions propositionnelles où f n'apparaît pas. Soient $y \in V$ une variable n'apparaissant pas dans p, q et p_y l'expression propositionnelle obtenue en substituant y à f dans p (de même pour q_y). $p' = CCp_yyy$, $q' = CCq_yyy$ et la valuation $v': V \rightarrow A$, où v' coïncide avec v pour les variables de p et q tandis que $v'(y) = 0$, ont les propriétés requises.

D'autres propriétés remarquables des *ABP* peuvent être définies par la validité de certaines règles; tel est le cas de la transitivité: une structure $A = (S, C, 0, 1)$ est *transitive* si la relation \leq , telle que $a \leq b$ ssi $C(a, b) = 1$, est transitive. Lorsque A est une *ABP*, $A : Cxy, Cyz \vdash Cxz$ est équivalente à $A : Cxy, Cyz \Vdash x \leq z$, Cf. [2]

I.3. Sous-algèbres, centre et idéaux d'une *ABP* (définitions)

Les termes (*en italique*) définis dans cette section se réfèrent à une *ABP* $A = (S, C, 0, 1)$.

Une *sous-algèbre* de A est un système $A' = (S', C', 0', 1')$ tel que $S' \subseteq S$, $C' \subseteq C$, $0' = 0$ et $1' = 1$. On note $A' \subseteq A$. L'opération C' de la sous-algèbre A' est univoque; A' est une structure. Par contre, A' n'est pas forcément une *ABP*.

Une sous-algèbre $A' \subseteq A$ est *fermée* si C' est définie pour tout couple d'éléments de S' pour lequel C est définie.

Une sous-algèbre fermée $A' \subseteq A$ est une restriction de la structure A , $C' = C \cap (S')^3$. Toutes les règles valides dans A le sont également dans A' ; en particulier, A' est une *ABP* et, si A est transitive, A' l'est également.

Les sous-algèbres fermées de A où l'opération induite est définie partout sont des algèbres de Boole. L'intersection des sous-algèbres Booléennes maximales de A est encore une algèbre de Boole, appelée *centre de A* et notée ZA . Le centre ZA est formé des éléments $c \in S$ compatibles avec tout élément de A . $ZA = A$ ssi A est une algèbre de Boole.

Le centre ZA contient l'algèbre Z_2 à deux éléments 0 et 1, sauf dans le cas où A est l'algèbre de Boole dégénérée à un seul élément. Lorsque $ZA = Z_2$ on dit que A est une *ABP centrale* (les éléments idempotents d'une K -algèbre centrale forment une *ABP centrale*, où K est le corps des réels ou des complexes).

Soit D le domaine de définition de l'opération C et \leq la relation binaire telle que $a \leq b$ ssi $C(a, b) = 1$; a, b et c désignent des éléments de l'*ABP* A .

Un *idéal* de A est une partie non vide J de S telle que:

- aDb et $b \in J$ entraînent $a \wedge b \in J$
- aDb et $a, b \in J$ entraînent $a \vee b \in J$.

Dans le cas où aDb pour tout élément b de J et tout a de A , on appelle J un *idéal fermé*. Un idéal J est fermé ssi $J \subseteq ZA$.

Un *idéal centré* de A est une partie non vide J de S telle que:

- $a \leq b$ et $b \in J$ entraînent $a \in J$,
- pour tous $a, b \in J$, il existe un élément c dans le centre ZA tel que $a \leq c$, $b \leq c$, $c \in J$.

Un idéal centré est évidemment un idéal, un idéal fermé est centré.

Pour un élément c du centre ZA l'ensemble $(c) = \{a \mid a \leq c\}$ est un idéal centré. (c) est appelé *idéal principal*. Dans une *ABP* transitive, l'ensemble (c) est un idéal quel que soit c . Ce n'est pas le cas dans les *ABP* non transitives; d'ailleurs, seul le

cas de l'idéal centré présente un intérêt dans la suite, de sorte que l'élément « principal » c sera toujours pris dans le centre.

Un idéal J est *premier* si, pour tout élément a de A , a est dans J ssi le complément $\neg a$ n'y est pas.

Les idéaux premiers de A correspondent aux homomorphismes de A à valeurs dans Z_2 . A est plongeable dans une algèbre de Boole ssi, pour toute paire d'éléments distincts a, b dans A , il existe un idéal premier qui les sépare ([4], th. 0, p. 67). Tout idéal premier est maximal mais la réciproque est fausse, par exemple dans l'ABP finie D (Cf. [4], th. 1, p. 70), où il n'existe pas d'idéaux premiers. Par contre, un idéal est premier s'il induit un idéal maximal dans chaque sous-algèbre Booléenne maximale.

I.4. Quotients

DÉFINITION. La structure $A' = (S', C', 0', 1')$ est *quotient* (ou image homomorphe) de l'ABP A s'il existe une relation d'équivalence R , de base S , compatible avec l'opération C , telle que :

- $S' = S/R$
- C' est induite par C
- 0 et 1 appartiennent aux classes $0'$ et $1'$ respectivement.

Dans ce cas, on note $A' = A/R$. A/R est un *quotient fermé* si, de plus, pour tous a, b, c dans S , aRb et bDc entraînent aDc .

Un quotient d'une ABP n'est pas, en général, une ABP. Les quotients fermés ont, par contre, des propriétés moins inattendues.

LEMME 1. Soient A une ABP et A' un quotient fermé de A . Alors :

- une règle valide dans A et dont toutes les prémisses sont de la forme Cfp est également valide dans A' .
- une règle valide dans A' et dont les conclusions sont toutes de la forme Cfp est également valide dans A .

Démonstration. Toute valuation $v: V \rightarrow A$ induit une valuation $v': V \rightarrow A'$ par le passage aux classes de R -équivalence. Réciproquement, toute valuation $v': V \rightarrow A'$ est induite par une valuation $v: V \rightarrow A$, qu'on obtient par le choix arbitraire d'un système de représentants.

On démontre, par induction sur le nombre d'occurrences de C dans les expressions propositionnelles de FV , que, pour les deux extensions $\bar{v}: \bar{V} \rightarrow A$ et $\bar{v}': \bar{V}' \rightarrow A'$, on a $\bar{V} = \bar{V}'$.

De plus, si v satisfait à $p \in \bar{V}$, il en est de même pour v' , à cause de la compatibilité de R avec C , 0 et 1 .

Inversément, si v' satisfait à Cfp , pour p dans FV , on a $Cfp \in \bar{V}' = \bar{V}$ donc $p \in \bar{V}$. Cfp est alors satisfaite par v à cause de la validité de R_8 dans l'ABP A .

Les deux affirmations du lemme découlent de ces diverses remarques.

PROPOSITION 1. Un quotient fermé d'une *ABP* est une *ABP*.

Démonstration. Tout quotient d'une *ABP* peut être recouvert par des sous-algèbres de Boole; les règles R_1, R_3, R_6, R_7 et R_8 y sont donc valides. Le résultat ci-dessus s'applique aux règles R_2, R_4, R_5 du théorème 1, § I.2.

PROPOSITION 2. Si une *ABP* a un quotient fermé transitif, elle est transitive.

Démonstration. Les *ABP* transitives peuvent être caractérisées par la validité d'une règle dont la conclusion a la forme *Cfp*.

PROPOSITION 3. Si une *ABP* est plongeable dans une algèbre de Boole, ses quotients fermés le sont également.

Démonstration. Une *ABP* est plongeable dans une algèbre de Boole ssi toutes les règles *Cfp*, $Cfq \vdash p \equiv q$ valides dans \mathbf{Z}_2 , avec V dénombrable, y sont également valides (th. 2, § I.2).

LEMME 2. Soient A une *ABP* et J un idéal centré de A . La relation R , définie par

$$aRb \text{ ssi il existe } c \text{ dans } J \text{ tel que } C(a, c) = C(b, c)$$

est une équivalence compatible avec l'opération C .

Démonstration. La symétrie de R est évidente; la réflexivité découle de $0 \in J$. Pour la transitivité soit: $C(a, c) = C(a', c)$, $C(a', c') = C(a'', c')$, c et c' dans J . Il existe donc un élément c'' du centre avec $c \leq c''$, $c' \leq c''$ et $c'' \in J$ pour lequel $C(a, c'') = C(a', c'') = C(a'', c'')$. De même, pour la compatibilité de R avec l'opération C , soit: $a'' = C(a, a')$, $b'' = C(b, b')$, $C(a, c) = C(b, c)$, $C(a', c') = C(b', c')$, avec c et c' dans J ; on peut remplacer c et c' par un élément c'' du centre, avec $c \leq c''$, $c' \leq c''$ et $c'' \in J$. L'identité Booléenne $CCxyz \equiv (CCxzz) \wedge (Cyz)$, satisfaite pour les trois valeurs compatibles a, a', c'' (ainsi que b, b', c'') données à x, y, z respectivement, fournit alors $C(a'', c'') = C(b'', c'')$.

DÉFINITION. Le quotient de l'*ABP* A par la relation R définie (ci-dessus) à l'aide de l'idéal centré J est appelé *quotient de A par J* et noté: A/J . Dans le cas où J est l'idéal principal (c) , on l'appelle *quotient de A par l'élément c* et on note: $A/J = A/(c) = A_c$.

Remarques. Les éléments de A appliqués sur 0 dans le quotient A/J sont exactement ceux de J ; on vérifie en effet: $aR0$ ssi $a \in J$.

A' est un quotient fermé de A ssi il existe un idéal fermé J de A tel que $A' \cong A/J$.

Certaines propriétés des quotients fermés se retrouvent dans le cas, un peu plus général, du quotient de A par un idéal centré.

LEMME 3. Soient A une *ABP* et J un idéal centré de A . Une règle valide dans

A est également valide dans A/J , si elle a un nombre fini de prémisses, toutes du type Cfp , où p est une expression propositionnelle dans laquelle f n'apparaît pas.

Démonstration. Soit $A:M \Vdash M'$, pour un tel ensemble M de prémisses, et soit $v:V \rightarrow A/J$ une valuation satisfaisant à M . Soit p_1, \dots, p_n une suite d'expressions propositionnelles dans lesquelles f n'apparaît pas, telle que :

- pour chaque prémisses $Cfp \in M$, p figure dans la suite p_1, \dots, p_n
- pour tout $i \leq n$ on a $p_i \in V$ ou alors $p_i = Cp_j p_k$ pour deux indices $j, k < i$.

On peut alors trouver, dans A , des éléments a_i, b_i et c_i ($i \leq n$) tels que, pour tout $i \leq n$:

- si $p_i \in V$, l'image de a_i dans A/J coïncide avec $v(p_i)$
- si $p_i = Cp_j p_k$, on a $a_i = C(b_i, c_i)$ et l'image, dans A/J , de a_i, b_i et c_i coïncide avec $\bar{v}(p_i), \bar{v}(p_j)$ et $\bar{v}(p_k)$ respectivement.

Pour tout triplet i, j, k tel que $p_i = Cp_j p_k$ on a, par conséquent, $b_i Ra_j$ et $c_i Ra_k$; d'où l'existence d'éléments d_i, e_i dans J tels que

$$C(b_i, d_i) = C(a_j, d_i) \quad \text{et} \quad C(c_i, e_i) = C(a_k, e_i).$$

Les deux éléments d_i, e_i de l'idéal centré J peuvent être remplacés, dans ces deux équations, par un élément g_i du centre ZA , avec $d_i \leq g_i, e_i \leq g_i$ et $g_i \in J$. Soit g le suprémum des g_i dans ZA ; on a alors

$$C(b_i, g) = C(a_j, g) \quad \text{et} \quad C(c_i, g) = C(a_k, g) \quad (*)$$

pour tout i tel que $p_i = Cp_j p_k$. A l'aide de l'élément g du centre, on modifie les valeurs de a_i, b_i, c_i ; pour tout $i \leq n$ on pose: $a'_i = a_i \vee g, b'_i = b_i \vee g, c'_i = c_i \vee g$. Avec ces nouvelles valeurs on a: $a'_i = C(a'_j, a'_k)$, pour tout $i \leq n$ tel que $p_i = Cp_j p_k$; en effet, (*) entraîne $b' = a'_j$ et $c'_i = a'_k$ tandis que $a'_i = C(b'_i, c'_i)$ découle de $a_i = C(b_i, c_i)$ et de l'identité Booléenne $(Cxy) \vee z = C(x \vee z)(y \vee z)$.

On peut finalement construire une valuation $v': V \rightarrow A$ compatible avec $v: V \rightarrow A/J$, en posant $v'(p_i) = a'_i$ pour $p_i \in V$. L'extension $\bar{v}': \bar{V}' \rightarrow A$ de v' est définie, notamment, pour p_i et prend la valeur $\bar{v}'(p_i) = a'_i$ (pour tout $i \leq n$).

Ainsi $M \subseteq \bar{V}'$; la forme particulière des prémisses fait qu'elles sont satisfaites par v' dans $L'ABP A$. Les conclusions sont donc également satisfaites par v' , et a fortiori par v , dans le quotient. c.q.f.d.

La démonstration des propositions 1 et 3 ci-dessus peut être reprise, pour le quotient par un idéal centré, en remplaçant le théorème 2, § I.4, par son corollaire:

PROPOSITION 4. Le quotient d'une ABP par un idéal centré est une ABP .

PROPOSITION 5. Si une ABP est plongeable dans une algèbre de Boole, c'est également le cas pour son quotient par un idéal centré.

I.5. Homomorphismes

De manière générale, on distingue deux notions d'homomorphisme.

DÉFINITION. Un *homomorphisme* $h: A \rightarrow A'$ entre les ABP A et A' est une application de S dans S' qui conserve les éléments distingués 0 et 1 , ainsi que la relation ternaire C . h est un *homomorphisme fermé* si, pour chaque paire d'éléments a, b dans S , on a :

C' est définie pour $h(a), h(b)$ ssi C est définie pour a, b .

Ainsi une sous-algèbre $A \subseteq A'$ est fermée ssi l'injection $S \subseteq S'$ est un homomorphisme fermé; le quotient $A' = A/R$ de A est fermé ssi l'application canonique $S \rightarrow S/R$ est un homomorphisme fermé; une application $h: S \rightarrow S'$ est un homomorphisme fermé de A vers A' ssi l'image de A par h est un quotient fermé de A et une sous-algèbre fermée de A' .

Un homomorphisme d'ABP $h: A \rightarrow A'$ est fermé ssi la préimage de toute sous-algèbre Booléenne de A' par h est une sous-algèbre Booléenne de A . En particulier, dans un quotient fermé A' de l'ABP A , les parties Booléennes maximales de A et de A' se correspondent de manière biunivoque. Par conséquent, le centre de A' est l'image du centre de A .

I.6. Produit d'ABP

Le produit cartésien d'une famille de structures $A_i, i \in J$, avec l'opération définie par composantes, est évidemment une structure; on la note $\prod_{i \in J} A_i$ (ou $A_1 \times A_2$, s'il y a deux facteurs).

LEMME. Toute règle valide dans chaque facteur $A_i, i \in J$, d'un produit $A = \prod_{i \in J} A_i$ est également valide dans A .

Réciproquement, toute règle valide dans A , dont l'ensemble des prémisses n'est pas contradictoire (satisfait par une valuation dans Z_2), est également valide dans chacun des facteurs $A_i, i \in J$.

Démonstration. Toute valuation $v: V \rightarrow A$ se décompose en une famille de valuations $v_i: V \rightarrow A_i$. Une expression propositionnelle de FV est satisfaite par v ssi elle est satisfaite par chaque $v_i, i \in J$. La première partie du théorème en découle immédiatement. Pour la seconde, soit M l'ensemble des prémisses d'une règle valide dans A et soit $v: V \rightarrow A_i$ une valuation dans A_i satisfaisant à M . On peut alors construire une valuation $v': V \rightarrow A$, satisfaisant à M et telle que $v'_i = v$; il suffit de donner à la i -ème composante de v' les valeurs de v . A toutes les autres composantes, on donne des valeurs dans Z_2 qui satisfont à M .

PROPOSITION 1. Un produit de structures est une ABP ssi chaque facteur est une ABP.

PROPOSITION 2. Un produit d' ABP est une ABP transitive ssi c'est le cas pour chacun des facteurs.

PROPOSITION 3. Un produit d' ABP est plongeable dans une algèbre de Boole ssi c'est le cas pour chacun des facteurs.

Les démonstrations découlent immédiatement du lemme et du § I.2.

La suite de ce § I.6 permet d'établir un critère de plongeabilité dans une algèbre de Boole (Prop. 5), qui généralise la proposition 3.

PROPOSITION 4. Soient A une ABP et J_1, \dots, J_n des idéaux centrés dont l'intersection est J . Alors A/J peut être plongé dans le produit $A' = \prod_{i=1}^n A/J_i$.

Démonstration. J est un idéal centré; soit $g: A \rightarrow A/J$ l'épimorphisme induit par J . D'autre part, soit $h: A \rightarrow A'$ l'homomorphisme dont la i -ème composante est donnée par la projection de A sur A/J_i ($i=1, \dots, n$). Alors $h=f \circ g$, pour une application bi-univoque $f: A/J \rightarrow A'$. En effet, pour a et b dans A avec $g(a)=g(b)$ il existe c dans J tel que $C(a, c)=C(b, c)$; dans ce cas $c \in J_i$ pour $i=1, \dots, n$ d'où $h(a)=h(b)$.

Réciproquement $h(a)=h(b)$ entraîne l'existence de $c_i \in J_i$ tels que $C(a, c_i)=C(b, c_i)$, pour $i=1, \dots, n$. L'intersection $c_1 \wedge c_2 \wedge \dots \wedge c_n$ est alors un élément de J et $g(a)=g(b)$ découle de l'identité Booléenne $Cx(z_1 \wedge \dots \wedge z_n)=Cxz_1 \wedge \dots \wedge Cxz_n$. f est un homomorphisme défini sur A/J puisque g est épimorphe.

COROLLAIRE 1. Pour tout élément c du centre d'une ABP A , on peut plonger A dans le produit $A_c \times A_{\neg c}$. Dans le cas d'une ABP transitive, on a $A \cong A_c \times A_{\neg c}$.

Démonstration. Les idéaux principaux (c) et $(\neg c)$ sont évidemment centrés et leur intersection est (0) . Pour montrer que $h: A \rightarrow A_c \times A_{\neg c}$ est surjectif pour A transitive, soit $(a, a') \in A_c \times A_{\neg c}$. Il existe donc b et b' dans A , dont les images sont a et a' dans les quotients respectifs par (c) et $(\neg c)$. Puisque A est transitive, on peut former $d=(b' \wedge c) \vee (b \wedge \neg c)$; on vérifie alors $C(b, c)=C(d, c)$ et $C(b', \neg c)=C(d, \neg c)$, d'où $h(d)=(a, a')$.

PROPOSITION 5. Une ABP finie est plongeable dans une algèbre de Boole ssi c'est le cas pour chacun de ses quotients $A_{\neg c}$, où c parcourt les atomes du centre.

Démonstration. Soit A une ABP dont chaque quotient $A_{\neg c}$ est plongeable dans une algèbre de Boole. L'algèbre $A \cong A/(0)$ peut être plongée dans le produit des $A_{\neg c}$, puisque l'intersection des idéaux $(\neg c)$, pour tous les atomes c de ZA , est nulle. La réciproque est contenue dans la proposition 5, § I.4.

Remarque. Cette proposition peut être généralisée aux ABP infinies complètes atomiques. Dans le cas des ABP transitives, elle est alors équivalente à la proposition 3; en vertu du corollaire 1, telle ABP est, en effet, le produit d'autant d' ABP centrales qu'il y a d'atomes dans le centre.

I.7. Isomorphisme partiel et somme d'ABP

DÉFINITION. Un *isomorphisme partiel* $h: A_1 \rightarrow A_2$ est une application biunivoque, définie sur une sous-algèbre Booléenne B de l'ABP A_1 , à valeurs dans l'ABP A_2 , qui conserve l'opération induite par A_1 .

L'application réciproque et le composé d'isomorphismes partiels sont encore des isomorphismes partiels. Soient A_1 et A_2 des sous-algèbres d'une ABP A ; si l'intersection $B = A_1 \cap A_2$ est une algèbre de Boole, la restriction de l'identité à B est un isomorphisme partiel.

DÉFINITION. Pour un isomorphisme partiel $h: A_1 \rightarrow A_2$ on appelle *somme* de A_1 et A_2 *modulo* h la structure A obtenue en identifiant, dans la réunion disjointe de S_1 et S_2 , les éléments correspondants de l'application h . Les opérations de A sont induites par A_1 et A_2 de manière univoque, puisque h est homomorphe.

On note $A = A_1 + A_2 (\text{mod } h)$. Lorsque h identifie les seuls éléments 0 et 1 de A_1 et A_2 , on appelle A la *somme directe* et on note $A = A_1 + A_2$.

Remarques. Si h est défini sur A_1 , alors $A_2 = A_1 + A_2 (\text{mod } h)$; en particulier $A_2 = Z_2 + A_2$, pour $A_1 = Z_2$. Si A_1 est formée d'un seul élément, alors $A = A_1 = A_2$.

La somme directe d'ABP est commutative et associative. La somme directe d'une famille quelconque d'algèbres de Boole peut toujours être plongée dans une algèbre de Boole assez grande.

A_1 et A_2 sont des sous-algèbres fermées de $A = A_1 + A_2 (\text{mod } h)$; par conséquent, toutes les règles valides dans A sont valides dans A_1 et A_2 . La réciproque est fautive; on vérifie cependant que la somme d'ABP est une ABP et que la somme directe d'ABP transitives est transitive. De plus, on a la propriété d'amalgamabilité suivante:

THÉORÈME. Soit $h: A_1 \rightarrow A_2$ un isomorphisme partiel et $A = A_1 + A_2 (\text{mod } h)$. Alors A est plongeable dans une algèbre de Boole ssi c'est le cas pour A_1 et A_2 .

Démonstration. On peut supposer que A_1 et A_2 sont des algèbres de Boole. Dans le cas contraire, on plongerait A_1 et A_2 dans les algèbres de Boole respectives B_1 et B_2 , de sorte que $A \subseteq B_1 + B_2 (\text{mod } h)$. Il s'agit de construire, pour deux éléments distincts a, b de A , un idéal premier J qui les sépare.

Si a et b se trouvent tous deux dans la même algèbre de Boole A_1 (par exemple), il existe un idéal maximal J_1 de A_1 séparant a de b . L'intersection $J_1 \cap A_2$ est un idéal propre de $A_1 \cap A_2$ et peut donc être étendu à un idéal maximal J_2 de A_2 , suivant un raisonnement classique. $J = J_1 \cup J_2$ est un idéal de A , premier et séparant a de b .

Reste le cas où $a \notin A_2$ et $b \notin A_1$. Soit $A_0 = A_1 \cap A_2$. Un lemme de A. Daigneault [1] affirme l'existence d'un idéal maximal J_0 de A_0 tel que l'idéal J_1 , engendré par J_0 dans A_1 , ne contient ni a , ni son complément. Soit alors J_2 un idéal maximal de A_2 contenant J_0 .

Si $b \in J_2$ on construit $J'_1 = \{C(a, c) \mid c \in J_1\}$. J'_1 est un idéal propre de A_1 ; sinon on

aurait $C(a, c) = I$ pour un élément c de J_1 , donc $a \leq c$ et $a \in J_1$; contradiction. D'autre part J'_1 contient $\neg a$, puisque $0 \in J_1$; il en est de même pour l'idéal maximal J''_1 de A_1 contenant J'_1 . J''_1 ne contient donc pas a et $J = J''_1 \cup J_2$ a les propriétés requises.

Si $b \notin J_2$ on remplace a et b par leurs compléments.

COROLLAIRE. Si une *ABP* est recouverte par trois algèbres de Boole, elle est plongeable dans une algèbre de Boole.

Démonstration. Soit A une *ABP* avec trois parties Booléennes maximales A_1 , A_2 et A_3 . On a alors $A_1 \cap A_2 \subseteq A_3$, avec une permutation éventuelle des indices. Sinon il y aurait trois éléments a_1, a_2, a_3 deux à deux compatibles, tels que $a_i \in A_k$ ssi $i \neq k$; l'algèbre de Boole engendrée par a_1, a_2 et a_3 n'est contenue dans aucune des A_i ($i = 1, 2, 3$), ce qui est contraire à l'hypothèse. Ainsi $(A_1 \cup A_3) \cap (A_2 \cup A_3) = A_3$ est une algèbre de Boole et le théorème s'applique à l'*ABP* $A = (A_1 \cup A_3) + (A_2 \cup A_3) \pmod{h}$, où h est l'identité sur A_3 .

Remarque. Les quotients $A_{\neg c}$ de la proposition 5, § I.6, sont en général beaucoup plus simples que l'*ABP* finie A ; on peut souvent leur appliquer le théorème ci-dessus ou son corollaire. De plus, leur construction est immédiate, elle revient à biffer certaines lignes et colonnes dans les matrices représentant A (Cf. Remarque à la fin des § II.3 et II.4). Nous disposons ainsi d'un critère de plongeabilité très pratique, employé systématiquement dans les cas 1 à 60 du § III.3.

II. Représentation des ABP

II.1. Généralisation de la somme d'*ABP*

La notion de somme peut être utilement étendue à certaines familles d'*ABP* et d'isomorphismes partiels. Soit $A_i, i \in J$, une famille d'*ABP* et $h_{ik}: A_k \rightarrow A_i, i$ et $k \in J$, une famille d'isomorphismes partiels telle que:

1. pour tout i de J : h_{ii} est l'identité de A_i
2. pour tous i, k de J : h_{ik} est la réciproque de h_{ki}
3. pour tous i, j, k de J : $h_{ik} \supseteq h_{ij} \circ h_{jk}$.

Alors la relation R , telle que aRb ssi il existe i, k dans J avec $a = h_{ik}(b)$, est une relation d'équivalence sur la réunion disjointe des $S_i (i \in J)$; réflexivité, symétrie et transitivité de R découlent directement des conditions 1, 2 et 3 ci-dessus. D'autre part, les applications h_{ik} sont homomorphes, de sorte que R est compatible avec les opérations des A_i . Le quotient par R est donc une structure, avec l'opération induite par les *ABP* de la famille. On l'appelle *somme* de la famille $\{A_i \mid i \in J\}$ modulo $\{h_{ik} \mid i, k \in J\}$.

Ici encore chaque *ABP* de la famille apparaît dans la somme comme sous-algèbre fermée; par contre, la somme n'est pas, en général, une *ABP*.

THÉORÈME. Une structure est une *ABP* ssi elle est la somme d'une famille d'algèbres de Boole $A_i, i \in J$, modulo une famille d'isomorphismes partiels h_{ik}, i et $k \in J$, telle que :

4. pour tous i, j, k il existe l dans J avec $h_{ij} = h_{il} \circ h_{lj}$, $h_{jk} = h_{jl} \circ h_{lk}$ et $h_{ki} = h_{kl} \circ h_{li}$

Démonstration. Soient $A = (S, C, 0, I)$ une *ABP* et $S_i (i \in J)$ les parties maximales de S dont les éléments sont deux à deux compatibles. Si $A_i = (S_i, C \cap S_i^3, 0, I)$ est l'algèbre de Boole obtenue par restriction de A à S_i et h_{ik} l'identité de A restreinte à $S_i \cap S_k (i, k \in J)$, on obtient une famille d'algèbres de Boole pour laquelle on vérifie 1., 2. et 3. La condition 4. est remplie parce que, pour i, j, k dans J , l'ensemble $(S_i \cap S_j) \cup (S_j \cap S_k) \cup (S_k \cap S_i)$ est formé d'éléments deux à deux compatibles; il est de ce fait contenu dans une partie maximale S_l .

Pour la réciproque, soit A la somme d'une famille d'algèbres de Boole $A_i (i \in J)$ remplissant les conditions 1. à 4. Si on considère A_i comme sous-algèbre de A , la relation de compatibilité D dans la structure A revient à: aDb ssi il existe $i \in J$ avec $a, b \in A_i$. A a les propriétés caractérisant les *ABP* (§ I.1): par exemple, pour a, b et c dans A , deux à deux compatibles, il existe i, j, k dans J avec a et b dans A_i , a et c dans A_j , c et a dans A_k ; 4. entraîne alors l'existence d'une sous-algèbre Booléenne A_l contenant a, b et c .

Au lieu des parties Booléennes maximales on aurait pu prendre, dans la démonstration, toutes les restrictions de A qui sont des algèbres de Boole finies. Toute *ABP* se laisse ainsi représenter comme somme d'une famille ayant les propriétés 1. à 4. ci-dessus, ainsi que

5. pour tout i de J : A_i est une algèbre de Boole finie.

Pour décrire une *ABP* finie, il suffit de numéroté ses sous-algèbres Booléennes maximales A_1, \dots, A_n et de donner les isomorphismes partiels $h_{ik}: A_k \rightarrow A_i$ pour $1 \leq i < k \leq n$. Une telle description est compliquée à cause du nombre élevé d'éléments; elle gagne à être remplacée par une représentation «duale» qui fait intervenir, au lieu d'une algèbre de Boole, l'ensemble de ses atomes et, au lieu d'un isomorphisme partiel, une relation binaire qui le caractérise (§ II.2).

II.2. Représentation d'un isomorphisme partiel par une relation binaire

DÉFINITION. Soient E, E' deux ensembles et R une partie du produit cartésien $E \times E'$. Nous écrirons $a'Ra$ au lieu de $\langle a, a' \rangle \in R$.

R est *surjective* si, pour tout a de E , il existe a' dans E' (et réciproquement) de sorte que $a'Ra$.

R est *droite* si, pour tous a, b dans E et a', b' dans E' , tels que $a'Ra, b'Rb$ on a: $a'Rb$ ssi $b'Ra$.

R est une *équivalence de E vers E'* si R est surjective et droite.

Nous noterons R^* la transposée de R , $R(X)$ l'ensemble des $a' \in E'$ tels que $a'Ra$ pour au moins un élément a de l'ensemble X et $id(E)$ la relation d'égalité sur E . Une relation binaire R est une équivalence de E vers E' ssi $R(E) = E'$, $R^*(E') = E$ et $R \circ R^* \circ R = R$.

Dans le cas où $E' = E$ et $id(E) \subseteq R$, R est dite *réflexive*. Une relation réflexive est droite ssi elle est symétrique et transitive.

Une relation $R \subseteq E \times E'$ est droite ssi on peut trouver deux familles d'ensembles disjoints, $E_i \subseteq E (i \in J)$ et $E'_i \subseteq E' (i \in J)$, telles que $R = \bigcup_{i \in J} E_i \times E'_i$.

Le choix des termes définis ci-dessus est suggéré par ces remarques.

PROPOSITION 1. Soient R une équivalence de E vers E' , $P(E)$ et $P(E')$ l'algèbre Booléenne des parties de E et E' respectivement. Soit h l'application définie par $h(X) = R(X)$ pour les éléments X de $P(E)$ tels que $R^* \circ R(X) = X$. Alors h est un isomorphisme partiel $h: P(E) \rightarrow P(E')$. On écrira: $h = P(R)$.

Démonstration. Il suffit de démontrer que h est univoque et définie sur une algèbre de Boole.

a) Le domaine de définition de h est une algèbre de Boole; il est fermé par rapport à la réunion, puisque $R(X \cup Y) = R(X) \cup R(Y)$, et par rapport au complément. En effet $R^* \circ R$ est réflexive, symétrique et transitive, donc $R^* \circ R(X) = X$ ssi X est la réunion d'un certain nombre de classes de $R^* \circ R$ -équivalence; il en est alors de même pour le complément de X dans E .

b) h est biunivoque; soit $Z = h(X) = h(Y)$ avec $R^* \circ R(X) = X$ et $R^* \circ R(Y) = Y$. Alors $X = R^* \circ R(X) = R^*(Z) = R^* \circ R(Y) = Y$.

L'image de l'isomorphisme partiel $h: P(E) \rightarrow P(E')$ est formée des parties $Y = R(X)$ de E' telles que $X = R^* \circ R(X)$. Ce sont exactement les $Y \subseteq E'$ tels que $R \circ R^*(Y) = Y$; l'isomorphisme h^* réciproque de h est induit par l'équivalence R^* de E' vers $E: P(R)^* = P(R^*)$.

L'isomorphisme partiel $h = P(R)$ est défini sur une sous-algèbre Booléenne complète de $P(E)$ et il conserve évidemment le supremum d'une famille non vide quelconque d'éléments pris dans ce domaine. Ces conditions s'avèrent suffisantes pour l'existence d'une équivalence R «duale» de h .

DÉFINITION. Un isomorphisme partiel $h: A \rightarrow A'$ est *complet* si A et A' sont des algèbres de Boole complètes atomiques et si le domaine et l'image de h sont des sous-algèbres complètes de A et A' respectivement.

PROPOSITION 2. Un isomorphisme partiel $h: P(E) \rightarrow P(E')$ est complet ssi h provient d'une équivalence de E vers E' .

Démonstration. Pour la construction de l'équivalence R duale de h on considère $P(E)$, $P(E')$ comme sous-algèbres de $A = P(E) + P(E') \pmod{h}$, avec l'intersection $B = P(E) \cap P(E') \subseteq A$; tandis que E et E' sont traités comme l'ensemble des atomes

de $P(E)$ et $P(E')$ respectivement. Soit $R \subseteq E \times E'$ définie par: $a'Ra$ ssi il existe un atome b de B tel que $a \leq b$ et $a' \leq b$.

La relation R est droite. Pour $a'Rc$, $c'Rc$, $c'Ra$ il existe en effet trois atomes b_1, b_2, b_3 de B avec $a' \leq b_1 \leq c$, $c \leq b_2 \leq c'$, $c' \leq b_3 \leq a$. D'où $b_1 \wedge b_2 \leq c$ dans $P(E)$ et $b_2 \wedge b_3 \leq c'$ dans $P(E')$, les atomes b_1, b_2, b_3 de B sont donc confondus et on a $a' \leq b_1 \leq a$, soit $a'Ra$.

La relation R est surjective. Soit a un atome de $P(E)$. B est une sous-algèbre complète de $P(E)$ et de ce fait totalement distributive et atomique ([6], p. 86). Il existe un atome b de B tel que $b \geq a$; sinon on aurait $a \wedge b = 0$ pour tout atome b de B et le supremum des $a \wedge b$, où b parcourt les atomes de B , serait également 0. Or, le supremum de l'ensemble des atomes b vaut 1 et, par distributivité, le supremum des $a \wedge b$ est $a \neq 0$. Finalement, il existe a' dans E' tel que $a \leq b \leq a'$ du fait que $P(E')$ est atomique.

La relation R est duale de h , $h = P(R)$. Il suffit de remarquer que tout élément de B est le supremum de l'ensemble des atomes qu'il couvre, aussi bien dans $P(E)$ que dans $P(E')$.

Tout isomorphisme partiel entre algèbres de Boole finies est complet; il peut être représenté par une équivalence d'un ensemble d'atomes vers l'autre.

Toute sous-algèbre complète d'une algèbre de Boole complète atomique peut être donnée par une partition de l'ensemble des atomes. Par exemple, pour $E = \{1, 2, 3, 4, 5\}$ la partition (12/34/5) représente la sous-algèbre engendrée par les éléments $\{1, 2\}$, $\{3, 4\}$ et $\{5\}$ de $P(E)$.

COROLLAIRE. Un homomorphisme $h: P(E) \rightarrow P(E')$ est complet (conserve les suprema de familles quelconques: [6], p. 70), ssi il existe une application $g: E' \rightarrow E$ telle que $h(X) = g^*(X)$, pour tout $X \subseteq E$, où g^* est la relation binaire transposée (ou réciproque) de g .

Pour la démonstration, remarquer que, si h est complet, l'image $h(P(E))$ est une sous-algèbre complète de $P(E')$.

II.3. Représentation d'une ABP par une famille de relations binaires

Soient R une équivalence de E vers E' et R' une équivalence de E' vers E'' . La composition habituelle $R' \circ R$ (produit relatif) ne donne pas, en général, une équivalence de E vers E'' ; on peut cependant «rectifier» $R' \circ R$ de manière à avoir $P(R' \perp R) = P(R') \circ P(R)$ pour l'isomorphisme partiel $P(R' \perp R)$ associé au produit droit $R' \perp R$.

DÉFINITION. On appelle *produit droit* $R' \perp R$ la relation binaire droite minimale, de E vers E'' , contenant $R' \circ R$.

L'existence de $R' \perp R$ est évidente, puisque $E \times E''$ est une relation droite et l'intersection d'une famille non vide de relations droites est encore droite. Le produit droit

d'équivalences R et R' contient la relation surjective $R' \circ R$, c'est donc une équivalence.

$R' \perp R$ peut être construit comme réunion d'une suite $R_n (n=0, 1, 2, \dots)$ de parties de $E \times E''$:

$$R_0 = R' \circ R, \quad R_{n+1} = R_n \circ R_n^* \circ R_n.$$

Si E ou E'' est de cardinal c fini, on a $R' \perp R = R_n$ pour n suffisamment grand (n tel que $3^n \geq 2 \cdot c$). On a également

$$R' \perp R = \bigcup_{n=0}^{\infty} R' \circ R \circ (R^* \circ R'^* \circ R' \circ R)^n$$

où la n -ième puissance est l'identité lorsque $n=0$, le produit relatif avec n facteurs identiques, lorsque $n \geq 1$.

Les trois lemmes suivants aboutissent à la démonstration de $P(R' \perp R) = P(R') \circ P(R)$. Pour les deux premiers, on fait les hypothèses et conventions suivantes.

Soient C une algèbre de Boole complète atomique, A et B des sous-algèbres complètes de C et d un atome de l'intersection $D = A \cap B$. Soit S l'ensemble des atomes de A bornés par d et T l'ensemble des atomes de B bornés par d . Pour $X \subseteq S$ et $Y \subseteq T$ on conviendra que:

- X' est le complément de X dans S , tandis que Y' est le complément de Y dans T .
- $X \cdot Y$ est l'ensemble des produits $a \wedge b$ dans C des éléments a de X et b de Y .
- $X \cdot Y = 0$ ssi $a \wedge b = 0$ pour tout a dans X et b dans Y ; X et Y peuvent être vides.

LEMME 1. Pour deux ensembles $X \subseteq S$ et $Y \subseteq T$ tels que $X \cdot Y' = 0$ et $X' \cdot Y = 0$, on a $X = Y = \emptyset$ ou $X' = Y' = \emptyset$.

Démonstration. Les algèbres A , B et C sont complètement distributives en vertu du théorème 25.2 [6], p. 86.

Soit $X \cdot Y' = 0$, $X' \cdot Y = 0$ et $c = \text{Sup} \{a \wedge b \mid a \in X \text{ et } b \in Y\}$. On a évidemment $c \leq d$ puisque $d = \text{Sup } S = \text{Sup } T = \text{Sup} \{a \wedge b \mid a \in S \text{ et } b \in T\}$.

Or $c = \text{Sup} \{a \wedge b \mid a \in X \text{ et } b \in Y\} = \text{Sup} \{a \wedge b \mid a \in X \text{ et } b \in T\} = \text{Sup} \{a \wedge \text{Sup } T \mid a \in X\} = \text{Sup} \{a \wedge d \mid a \in X\} = \text{Sup } X \in A$, puisque, par hypothèse, $a \wedge b = 0$ pour $a \in X$ et $b \in Y'$; de même $c = \text{Sup } Y \in B$ et par conséquent $c \in D$.

d étant un atome, $c \leq d$ entraîne $c = 0$ ou $c = d$. Dans le premier cas, $X \cdot Y = 0$; $X \cdot Y' = 0$ et $X' \cdot Y = 0$ ne sont alors possibles qu'avec $X = Y = \emptyset$. Dans le second cas soit $c' = \text{Sup} \{a \wedge b \mid a \in X' \text{ et } b \in Y'\}$; on a évidemment $c' \leq d$, d'où:

$$\begin{aligned} c' &= d \wedge c' = c \wedge c' = \text{Sup} \{a \wedge b \mid a \in X, b \in Y\} \wedge \text{Sup} \{a' \wedge b' \mid a' \in X', b' \in Y'\} \\ &= \text{Sup} \{a \wedge b \wedge a' \wedge b' \mid a \in X, b \in Y, a' \in X', b' \in Y'\} = 0 \end{aligned}$$

puisque, par hypothèse, $a \wedge b' = 0$ et $a' \wedge b = 0$ pour $a \in X$, $b' \in Y'$, $a' \in X'$ et $b \in Y$. Donc $X' \cdot Y' = 0$; on en déduit, comme dans le premier cas, $X' = Y' = \emptyset$.

LEMME 2. Pour tout atome a dans S et tout b dans T il existe un entier $n \geq 0$, des atomes a_0, \dots, a_n dans S et des atomes b_0, \dots, b_n dans T tels que $a_0 = a$, $b_n = b$,
 $a_i \wedge b_i \neq 0 \quad (0 \leq i \leq n)$,
 $a_i \wedge b_{i-1} \neq 0 \quad (1 \leq i \leq n)$.

Démonstration. On peut construire les suites de familles d'atomes suivantes:

$$\begin{aligned} S_0 &= \{a\}, \quad T_0 = \{e \in T \mid a \wedge e \neq 0\}, \\ S_{n+1} &= \{e \in S'_n \mid \{e\} \cdot T_n \neq 0\} = \\ &= \{e \in S \mid e \notin S_n \text{ et il existe } e' \text{ dans } T_n \text{ avec } e \wedge e' \neq 0\}, \\ T_{n+1} &= \{e \in T'_n \mid S_{n+1} \cdot \{e\} \neq 0\} = \\ &= \{e \in T \mid e \notin T_n \text{ et il existe } e' \text{ dans } S_{n+1} \text{ avec } e \wedge e' \neq 0\}. \\ X &= \bigcup_{n=0} S_n \subseteq S, \quad Y = \bigcup_{n=0} T_n \subseteq T. \end{aligned}$$

Par construction on a: $X' \subseteq (S_n \cup S_{n+1})' = S'_n \setminus S_{n+1}$, donc $X' \cdot T_n = 0$, pour tout n ; par conséquent $X' \cdot Y = 0$.

D'autre part $Y' \subseteq (T_n \cup T_{n+1})' = T'_n \setminus T_{n+1}$, donc $S_{n+1} \cdot Y' = 0$, pour tout n . De plus $Y' \subseteq T'_0$, donc $S_0 \cdot Y' = 0$ et par conséquent $X \cdot Y' = 0$.

Le lemme 1 s'applique ainsi à X et Y ; on a $X = Y = \emptyset$ ou alors $X' = Y' = \emptyset$. Or $S_0 \subseteq X$ n'est pas vide, donc $X' = Y' = \emptyset$ et $T = Y$. Pour tout b dans T il existe par conséquent un $n \geq 0$ avec $b \in T_n$.

Ceci permet de trouver une suite d'atomes $a_i \in S_i$, $b_i \in T_i$ ($0 \leq i \leq n$) par le procédé récursif suivant:

- $b_n = b$ est dans T_n ,
- soit b_{n-i} dans T_{n-i} pour $0 \leq i \leq n$, alors il existe un atome $e \in S_{n-i}$ tel que $e \wedge b_{n-i} \neq 0$ (définition de T_{n-i}), on prendra $a_{n-i} = e$.
- soit a_{n-i} dans S_{n-i} pour $0 \leq i < n$, alors on peut trouver un b_{n-i-1} dans T_{n-i-1} tel que $a_{n-i} \wedge b_{n-i-1} \neq 0$ (définition de S_{n-i}).

Pour $i = n$ on aboutit à a_0 dans S_0 , or $S_0 = \{a\}$, d'où $a = a_0$. D'autre part, aucun des produits $a_i \wedge b_i$ ou $a_i \wedge b_{i-1}$ ne s'annule.

LEMME 3. Pour deux équivalences R de E vers E' et R' de E' vers E'' , on a $P(R' \perp R) = P(R') \circ P(R)$.

Démonstration. Soit $h = P(R)$, $h' = P(R')$ et $h'' = h' \circ h$. D'après la proposition 2, § II.2, il existe une équivalence R'' de E vers E'' telle que $h'' = P(R'')$. Pour montrer $R'' = R' \perp R$ on construit l'ABP

$$P = \{P(E) + P(E') \pmod{h}\} + P(E'') \pmod{h'}$$

plongeable dans une algèbre de Boole selon le théorème du § I.7. $P(E)$, $P(E')$ et $P(E'')$ peuvent alors être considérées comme sous-algèbres de P avec l'intersection $A = P(E) \cap P(E')$, $B = P(E') \cap P(E'')$ et $D = A \cap B = P(E) \cap P(E'')$; les relations R , R' et R'' sont caractérisées, comme précédemment, par l'existence d'atomes dans A , B et D respectivement.

a) $R' \perp R \subseteq R''$. Puisque R'' est une équivalence, il suffit de montrer $R' \circ R \subseteq R''$. Soient $a \in E$, $a' \in E'$, $a'' \in E''$ tels que $a'' R' a'$ et $a' R a$; on a donc: $a \leq b \geq a'$ et $a' \leq b' \geq a''$, pour deux atomes, b dans A et b' dans B . Il existe dans D deux atomes d et d' tels que $d \geq b$ et $d' \geq b'$ (Cf. démonstration de la proposition 2, § II.2). Puisque $d \wedge d' \geq a'$, les atomes d et d' sont confondus; donc $a'' \leq d \geq a$ et $a'' R'' a$.

b) $R'' \subseteq R' \perp R$. Avec $R' \perp R = \bigcup_{n=0}^{\infty} R' \circ R \circ (R^* \circ R'^* \circ R' \circ R)^n$ cela revient à montrer que, pour $e \in E$, $e'' \in E''$ tels que $e \leq d \geq e''$ pour un atome d de D , il existe un entier n et des éléments

$$\begin{array}{ll} e_0, \dots, e_n & \text{dans } E \\ e'_0, \dots, e'_n & \text{dans } E' \\ e''_0, \dots, e''_n & \text{dans } E'' \\ e_1^*, \dots, e_n^* & \text{dans } E' \end{array}$$

tels que $e = e_0$, $e'' = e''_n$ et

$$\begin{array}{ll} - e_i \leq a_i \geq e'_i & \text{pour } 0 \leq i \leq n \text{ et un atome } a_i \text{ de } A \\ - e'_i \leq b_i \geq e''_i & \text{pour } 0 \leq i \leq n \text{ et un atome } b_i \text{ de } B \\ - e''_{i-1} \leq b_i^* \geq e_i^* & \text{pour } 1 \leq i \leq n \text{ et un atome } b_i^* \text{ de } B \\ - e_i^* \leq a_i^* \geq e_i & \text{pour } 1 \leq i \leq n \text{ et un atome } a_i^* \text{ de } A. \end{array}$$

Si l'on prend pour a un atome de A tel que $e \leq a$ et pour b un atome de B tel que $e'' \leq b$ (existence assurée du fait que R et R' sont surjectives) le lemme 2 ci-dessus fournit n , a_0, \dots, a_n et b_0, \dots, b_n . Le choix de $a_i^* = a_i$, $b_i^* = b_{i-1}$ pour $1 \leq i \leq n$ donne:

$$\begin{array}{ll} - a_i \wedge b_i \neq 0 & \text{d'où l'existence de } e'_i \text{ dans } E', 0 \leq i \leq n, \\ - a_i^* \wedge b_i^* \neq 0 & \text{d'où l'existence de } e_i^* \text{ dans } E', 1 \leq i \leq n. \end{array}$$

L'existence de $e_i \leq a_i^* = a_i$ et de $e''_{i-1} \leq b_i^* = b_{i-1}$, $1 \leq i \leq n$ provient du fait que $P(E)$ et $P(E'')$ sont atomiques. Restent $e_0 \leq a_0$ et $e''_n \leq b_n$ que l'on peut poser $e_0 = e$ et $e''_n = e''$, puisque $a_0 = a$ et $b_n = b$.

COROLLAIRE 1. Le produit droit d'équivalences est associatif.

COROLLAIRE 2. Si R_1 et R_2 sont deux équivalences de E vers E' et $h_1 = P(R_1)$, $h_2 = P(R_2)$ les isomorphismes partiels associés, on a

$$h_1 \subseteq h_2 \quad \text{ssi} \quad R_1 \supseteq R_2.$$

Démonstration. $h_1 \subseteq h_2 \Leftrightarrow h_1 \circ h_2^* \circ h_1 = h_1 \Leftrightarrow R_1 \perp R_2^* \perp R_1 = R_1$; un simple calcul montre que cette dernière égalité a lieu ssi $R_2 \subseteq R_1$.

THÉORÈME. Toute ABP est la somme d'une famille d'algèbres $P(E_i)$, $i \in J$, modulo une famille d'isomorphismes partiels $P(R_{ik})$, i et $k \in J$, telle que

- pour i, k dans J : R_{ik} est une équivalence de E_k vers E_i
- pour i dans J : R_{ii} est l'identité sur E_i
- pour i, k dans J : R_{ki} est la transposée de R_{ik}
- pour i, j, k dans J : $R_{ik} \subseteq R_{ij} \perp R_{jk}$

et, pour tout triplet i, j, k , il existe l dans J tel que:

$$\begin{aligned} R_{ij} &= R_{il} \perp R_{lj} \\ R_{jk} &= R_{jl} \perp R_{lk} \\ R_{ki} &= R_{kl} \perp R_{li}. \end{aligned}$$

Réciproquement, une telle somme est toujours une ABP .

La preuve découle du § II.1, du lemme 3 et du corollaire 2 ci-dessus.

Pour représenter une ABP finie comme somme d'algèbres $P(E_i)$ on prendra toujours les parties Booléennes maximales numérotées à l'aide de $J = \{1, 2, \dots, n\}$. Pour $i \leq n$ on prendra $E_i = \{1, 2, \dots, d_i\}$, (d_i = dimension de la i -ème partie Booléenne maximale) de sorte que R_{ik} est décrite à l'aide d'une matrice dont les $d_k \times d_i$ éléments ont les valeurs 0 ou 1. Dans le cas d'une ABP infinie, il suffit de prendre la famille de toutes les restrictions finies Booléennes. Ce n'est cependant pas toujours nécessaire; par exemple l' ABP $B(U^\omega)$ des sous-espaces fermés de l'espace d'Hilbert U^ω (Cf. [4], p. 65) est la somme de la famille d'algèbres $P(E_i)$ modulo les isomorphismes partiels $P(R_{ik})$, i et k dans J , lorsque:

- J est un ensemble indexant les bases orthonormées de U^ω ,
- pour chaque i de J , E_i est l'ensemble des vecteurs de la base d'indice i .
- pour i et k dans J , R_{ik} est la relation telle que $aR_{ik}b$ ssi les vecteurs a et b appartiennent au même sous-espace invariant, irréductible, de la transformation unitaire qui amène la base E_i sur E_k .

II.4. Représentation d'un homomorphisme par une famille d'applications

Pour la construction d' ABP universelles (§ III.1), il est nécessaire d'étendre aux homomorphismes le procédé de représentation «duale» donné, dans le théorème précédent, pour les ABP . On est ainsi conduit à considérer des familles d'homomorphismes compatibles avec les identifications imposées par certains isomorphismes partiels.

DÉFINITION. Soit Φ une famille d'algèbres de Boole A_i et d'isomorphismes

partiels $h_{ik}: A_k \rightarrow A_i$ (i et k dans J); de même pour Φ' , A'_i et h'_{ik} ($i, k \in J'$). Un *homomorphisme de Φ dans Φ'* , noté $f: \Phi \rightarrow \Phi'$, est une famille d'homomorphismes $f_i: A_i \rightarrow A'_{j(i)}$, i dans J , avec une application $j: J \rightarrow J'$, tels que, pour tous i, k dans J :

$$f_i \circ h_{ik} \subseteq h'_{j(i) j(k)} \circ f_k. \quad (1.)$$

Deux homomorphismes f, f' de Φ dans Φ' sont *équivalents* si, pour tout i dans J :

$$f_i \subseteq h'_{j(i) j'(i)} \circ f'_i \quad (2.)$$

Dans le cas où les familles Φ et Φ' ont les propriétés 1. à 4. du § II.1, on peut en former les sommes respectives A et A' . Les conditions (1.) expriment alors le fait que les valeurs de f_i et f_k dans A' coïncident sur la partie identifiée par h_{ik} dans A . L'extension commune des f_i est un homomorphisme de A dans A' .

Réciproquement, tout homomorphisme d'ABP peut être décomposé en une famille d'homomorphismes d'algèbres de Boole finies, en conséquence du § II.1. Cette décomposition n'est pas toujours unique; en fait, deux homomorphismes f et f' , de Φ dans Φ' , induisent le même homomorphisme d'ABP, de A dans A' , ssi ils sont équivalents.

La composition «naturelle» d'homomorphismes $f: \Phi \rightarrow \Phi'$ et $f': \Phi' \rightarrow \Phi''$ conserve la propriété (1.). On notera $f' \circ f: \Phi \rightarrow \Phi''$ l'homomorphisme composé. Dans le cas où les familles considérées ont les propriétés 1. à 4. (§ II.1), cette composition coïncide avec celle des homomorphismes d'ABP pour les sommes respectives.

LEMME. Soit R une équivalence de E_1 vers E_2 et $h = P(R)$; de même pour $R' \subseteq E'_1 \times E'_2$ et $h' = P(R')$. Soient $f_i: P(E_i) \rightarrow P(E'_i)$ deux homomorphismes complets tels que (d'après le corollaire fin § II.2) $f_i(X) = g_i^*(X)$ pour $X \subseteq E_i$ ($i = 1, 2$). Alors

$$f_2 \circ h \subseteq h' \circ f_1 \quad \text{ssi} \quad g_2 \circ R' \subseteq R \circ g_1$$

Démonstration. On peut remarquer tout d'abord qu'on a $g_2 \circ R' \subseteq R \circ g_1$ ssi $R' \circ g_1^* \subseteq g_2^* \circ R$, où g^* est la relation binaire transposée de l'application g_i ($i = 1, 2$). Soit $g_2 \circ R' \subseteq R \circ g_1$ et $X' = f_1(X)$ pour un $X \subseteq E_1$ tel que $R^* \circ R(X) = X$. Alors $R'^* \circ R'(X') = R'^*(R' \circ g_1^*(X)) \subseteq R'^*(g_2^*(R(X))) \subseteq g_2^* \circ R^*(R(X)) = X'$; ainsi $R'^* \circ R'(X') = X'$ puisque R' est surjective. Donc h' est défini pour $X' \subseteq E'_1$ et on a $h' \circ f_1(X) = f_2 \circ h(X)$ car, d'une part $R'(g_1^*(X)) \subseteq g_2^*(R(X))$ et, d'autre part, $g_2^*(R(X)) \subseteq R' \circ R'^* \circ g_2^* \circ R(X) \subseteq R'(X') = R'(g_1^*(X))$. On a ainsi montré $f_2 \circ h \subseteq h' \circ f_1$. Pour la réciproque soit $f_2 \circ h \subseteq h' \circ f_1$ c'est à dire $g_2^*(R(X)) = R'(g_1^*(X))$ pour tout $X \subseteq E_1$ tel que $R^* \circ R(X) = X$.

Pour X quelconque, on prend $X' = R^* \circ R(X)$ de sorte que $X \subseteq X'$, $R(X) = R(X')$ et $R^* \circ R(X') = X'$. On a alors

$$R'(g_1^*(X)) \subseteq R'(g_1^*(X')) = g_2^*(R(X')) = g_2^*(R(X))$$

pour $X \subseteq E_1$ quelconque, par conséquent $R' \circ g_1^* \subseteq g_2^* \circ R$.

Ce lemme contient l'essentiel de la démonstration du théorème suivant.

THÉORÈME. Soit Φ une famille d'algèbres de Boole $P(E_i)$ et d'isomorphismes partiels $P(R_{ik})$, avec i et k dans J ; de même pour Φ' , $P(E'_i)$ et $P(R'_{ik})$, avec i et k dans J' .

a) Alors tout homomorphisme $f: \Phi \rightarrow \Phi'$ peut être représenté par une famille d'applications $g_i: E'_{j(i)} \rightarrow E_i$, $j: J \rightarrow J'$, telles que $f_i(X) = g_i^*(X)$, pour tout $X \subseteq E_i$ ($i \in J$), et

$$\text{pour } i, k \text{ dans } J: \quad g_i \circ R'_{j(i) j(k)} \subseteq R_{ik} \circ g_k \quad (3.)$$

Réciproquement, les conditions (3.) sont suffisantes pour que la famille d'applications g_i ($i \in J$) détermine un homomorphisme de Φ dans Φ' .

b) Si Φ et Φ' ont les propriétés 1.-4. (§ II.1), deux homomorphismes f et f' , de Φ dans Φ' , sont équivalents ssi les applications g_i et g'_i ($i \in J$) qui les représentent sont telles que

$$g_i \circ R'_{j(i) j'(i)} \subseteq g'_i \quad (4.)$$

c) D'autre part, la composition $f' \circ f$ de deux homomorphismes $f: \Phi \rightarrow \Phi'$ et $f': \Phi' \rightarrow \Phi''$ est représentée par la famille des applications composées $g_i \circ g'_{j(i)}$ et $j' \circ j: J \rightarrow J''$ (l'ordre des facteurs est inversé).

Remarque. Tout homomorphisme d'ABP peut être ainsi représenté, en utilisant les résultats du § II.1. Le quotient d'une ABP finie A est représenté d'une manière particulièrement simple: si $P(E_i)$ est une sous-algèbre Booléenne maximale de A , son image dans A' est $P(E'_i)$, avec $E'_i \subseteq E_i$. Les applications g_i ($i \in J$) sont simplement les injections $E'_i \subseteq E_i$; les conditions (3.) deviennent: $R'_{ik} \subseteq R_{ik}$ ($i, k \in J$).

II.5. Construction d'une famille minimale

DÉFINITION. Soit Φ une famille d'algèbres de Boole et d'isomorphismes partiels donnés. Une famille Φ' ayant les propriétés 1. à 5. (§ II.1) est *minimale sur Φ* s'il existe un homomorphisme $f: \Phi \rightarrow \Phi'$ avec la propriété suivante:

pour toute famille Φ'' qui a les propriétés 1. à 5. et pour tout homomorphisme $f'': \Phi \rightarrow \Phi''$ il existe un homomorphisme $f': \Phi' \rightarrow \Phi''$ tel que $f'' = f' \circ f$, déterminé à l'équivalence près.

La famille Φ' minimale sur Φ n'est pas déterminée univoquement; toutefois, Φ' est caractérisée à l'isomorphie près, si l'on impose aux isomorphismes partiels h'_{ik} de ne pas être surjectifs (c'est à dire $A_k \not\supseteq A_i$). L'existence de Φ' n'est assurée que dans le cas où les algèbres A_i de Φ sont finies; au lieu d'en donner une démonstration générale, nous préférons décrire un procédé itératif qui, dans les cas qui nous intéressent, permet la construction effective de Φ' . Ce procédé s'applique aux ABP uni-

verselles (§ III.2) et aux successeurs d'une *ABP* finie (§ III.3), grâce à la propriété évidente:

PROPOSITION. Soit Φ une famille d'algèbres de Boole finies $A_i (i \in J)$ et d'isomorphismes partiels $h_{ik} (i, k \in J)$. Soient Φ' la famille minimale sur Φ et A' la somme de Φ' . Alors A' est une *ABP* et il existe une famille d'homomorphismes $f_i: A_i \rightarrow A'$ avec

$$f_i \circ h_{ik} \subseteq f_k \quad \text{pour tous } i, k \text{ dans } J$$

telle que, pour toute *ABP* A'' et toute famille d'homomorphismes $f_i'': A_i \rightarrow A''$ avec la propriété analogue, il existe un homomorphisme d'*ABP* unique $h: A' \rightarrow A''$ pour lequel $f_i'' = h \circ f_i (i \in J)$.

THÉORÈME. Soit Φ une famille d'algèbres finies $P(E_i)$ et d'isomorphismes partiels $P(R_{ik})$, avec $1 \leq i, k \leq n$ pour un entier n .

Soient $E' (i \in J')$ des ensembles finis, $R'_{ik} \subseteq E'_k \times E'_i$ des relations droites et g_1, \dots, g_n une suite d'applications $g_i: E'_{j(i)} \rightarrow E_i$, où $j(i) \in J'$ pour $1 \leq i \leq n$, avec les propriétés suivantes:

- 1*) pour tout i de J' $R'_{ii} = id(E'_i)$
- 2*) pour tous i, k de J' $R'_{ik} \subseteq (Ré)^*$
- 3*) pour tous i, j, k de J' $R'_{ik} \subseteq R'_{ki} \perp R'_{jk}$
- 4*) pour tous i, j, k de J' il existe l dans J' tel que

$$R'_{ij} = R'_{il} \perp R'_{lj}$$

$$R'_{jk} = R'_{jl} \perp R'_{lk}$$

$$R'_{ki} = R'_{kl} \perp R'_{li}$$

- 5*) pour $i' = j(i)$, $k' = j(k)$ et $1 \leq i, k \leq n$:

$$g_i \circ R'_{i'k'} \subseteq R_{ik} \circ g_k$$

6*) pour toute famille d'ensembles finis $E''_i (i \in J'')$, de relations droites $R''_{ik} \subseteq E''_k \times E''_i$ (i et k dans J'') et d'applications $g''_i: E''_{j''(i)} \rightarrow E_i (1 \leq i \leq n)$ satisfaisant aux mêmes conditions (1* à 5*), on peut trouver une famille d'applications

$$g'_i: E''_{j'(i)} \rightarrow E'_i \quad (i \in J'), \quad j': J' \rightarrow J'',$$

telle que pour $i' = j'(i)$, $k' = j'(k)$ et i, k dans J' : $g'_i \circ R''_{i'k'} \subseteq R'_{ik} \circ g'_k$ et pour $1 \leq i \leq n$: $g''_i = g_i \circ g'_{j(i)}$.

De surcroît, la famille $g'_i: E''_{j'(i)} \rightarrow E'_i (i \in J')$, $j': J' \rightarrow J''$ est déterminée à l'équivalence près; pour un autre choix d'applications

$$\bar{g}_i: E''_{j(i)} \rightarrow E'_i \quad (i \in J'), \quad \bar{j}: J' \rightarrow J'',$$

avec les mêmes propriétés, on a, pour tout $i \in J'$:

$$\bar{g}_i \circ R''_{j(i)j'(i)} \subseteq g'_i.$$

Alors la famille d'algèbres $P(E'_i)$ et d'isomorphismes partiels $P(R'_{ik})$, i et k dans J' , est minimale sur Φ .

Démonstration. Les relations R'_{ik} sont des équivalences; elles sont droites par hypothèse, d'où $R'_{ik} \perp (R'_{ik})^* = R'_{ik} \circ (R'_{ik})^*$. Les conditions 1*, 2* et 3* entraînent alors $id(E'_i) = R'_{ii} \subseteq R'_{ik} \perp R'_{ki} = R'_{ik} \circ (R'_{ik})^*$, soit $R'_{ik}(E_k) = E'_i$. Le reste est conséquence immédiate du théorème du § II.4.

La famille minimale sur Φ se trouve ainsi caractérisée d'une manière qui permet de l'«approcher» par une suite de modifications apportées à Φ .

Si les ensembles E_i et les relations R_{ik} , $1 \leq i, k \leq n$, de Φ ont les propriétés 1* à 4*, alors Φ est minimale elle-même; les conditions 5* et 6* sont trivialement satisfaites par le choix $g_i = id(E_i)$, $i \leq n$. Si l'une des conditions 1* à 4* n'est pas remplie, nous modifions n , E_i , R_{ik} ($i, k \leq n$) en n' , E'_i , R'_{ik} ($i, k \leq n'$) et nous donnons des applications $g_i: E'_{j(i)} \rightarrow E_i$, avec $j(i) \leq n'$ pour $i \leq n$, qui ont les propriétés 5* et 6*.

1er cas: $R_{ii} \neq id(E_i)$ pour un indice $i \leq n$.

$$n' = n;$$

$$E'_i = \{a \in E_i \mid aR_{ii}a\}, E'_k = E_k \text{ pour } k \neq i;$$

$$R'_{ii} = id(E'_{ii}), R'_{ik} = (E_k \times E'_i) \cap R_{ik} \text{ et } R'_{ki} = (E'_i \times E_k) \cap R_{ki} \text{ pour } k \neq i, R'_{jk} = R_{jk} \text{ pour } j \neq i \text{ et } k \neq i;$$

$$g_i: E'_i \subseteq E_i, g_k = id(E_k) \text{ pour } k \neq i.$$

2me cas: $R_{ik} \not\subseteq (R_{ki})^*$ pour un couple d'indices $i, k \leq n$.

$$n' = n;$$

$$E'_m = E_m \text{ pour tout } m \leq n;$$

$$R'_{ik} = R_{ik} \cap R_{ki}^*, R'_{jm} = R_{jm} \text{ pour tous } j, m \leq n \text{ tels que } (j, m) \neq (i, k);$$

$$g_m = id(E_m) \text{ pour tout } m \leq n.$$

3me cas: $R_{ik} \not\subseteq R_{ij} \perp R_{jk}$ pour trois indices i, j et k .

$$n' = n;$$

$$E'_m = E_m \text{ pour tout } m \leq n;$$

$$R'_{ik} = R_{ik} \cap (R_{ij} \perp R_{jk}), R'_{lm} = R_{lm} \text{ pour tous } l, m \leq n \text{ tels que } (l, m) \neq (i, k);$$

$$g_m = id(E_m) \text{ pour tout } m \leq n.$$

4me cas: pour les trois indices i, j et k il n'existe pas d'indice l tel que $R_{ij} = R_{il} \perp R_{lj}$, $R_{jk} = R_{jl} \perp R_{lk}$ et $R_{ki} = R_{kl} \perp R_{li}$.

$$n' = n + 1;$$

$$E'_m = E_m \text{ pour tout } m \leq n;$$

Pour construire E'_n , définissons l'ensemble E et la relation $R \subseteq E \times E$ de la manière suivante:

$$E = \{(a, b, c) \mid aR_{ij}b, bR_{jk}c \text{ et } cR_{ki}a\} \subseteq E_i \times E_j \times E_k,$$

$$(a, b, c) R (a', b', c') \text{ ssi } aR_{ij}b', bR_{jk}c' \text{ et } cR_{ki}a';$$

R est évidemment réflexive et droite, c'est donc une relation d'équivalence de base E (début § III.2). On peut former l'ensemble des classes d'équivalence:

$$E'_n = E/R;$$

$$R'_{lm} = R_{lm} \text{ pour tous } l, m \leq n; R'_{n'n} = id(E'_n);$$

$$R'_{mn'} = E_m \times E'_n \text{ pour tout } m \leq n \text{ tel que } m \neq i, m \neq j \text{ et } m \neq k;$$

$R'_{in'}$, $R'_{jn'}$ et $R'_{kn'}$ sont définies comme suit, pour $a \in E_i$, $b \in E_j$, $c \in E_k$ et $X \in E/R$:

$$aR'_{in'}X \text{ ssi il existe } (a', b', c') \in X \text{ tel que } aR_{ij}b' \text{ et } c'R_{ki}a;$$

$$bR'_{jn'}X \text{ ssi il existe } (a', b', c') \in X \text{ tel que } bR_{jk}c' \text{ et } a'R_{ij}b;$$

$$cR'_{kn'}X \text{ ssi il existe } (a', b', c') \in X \text{ tel que } cR_{ki}a' \text{ et } b'R_{jk}c;$$

$$R'_{n'm} = (R'_{mn'})^* \text{ pour tout } m \leq n;$$

$$g_m = id(E_m) \text{ pour tout } m \leq n.$$

Remarques. Les nouveaux ensembles E'_m ainsi formés sont finis, les relations R'_{ik} sont droites (la démonstration utilise seulement le fait que les R_{ik} sont droites).

Les modifications apportées rétablissent, dans chacun des cas, la propriété qui faisait défaut, éventuellement aux dépens de l'une des autres propriétés (1* à 4*) recherchées.

Toutefois, les applications g_i définies, dans chacun des cas traités ci-dessus, ont les propriétés 5* et 6*. De surcroît, lors de deux modifications successives, la composition des applications g_i correspondantes conserve ces deux propriétés.

On peut ainsi chercher à réaliser toutes les conditions 1* à 4* en réitérant les diverses opérations indiquées; si un nombre fini de pas y suffit, on aboutit, en vertu du théorème précédent, à la représentation duale de la famille minimale sur Φ .

Si, au contraire, on obtient une suite infinie de transformations, le procédé n'est pas utilisable pour la construction effective de la famille minimale; cette situation ne s'est jamais présentée dans les applications. D'autre part, si l'on se borne à réaliser les conditions 1* à 3*, un nombre fini de transformations élémentaires est suffisant (dans les trois premiers cas ces modifications sont «monotones»: $n' = n$, $E'_m \subseteq E_m$ et $R'_{lm} \subseteq R_{lm}$, pour tous $l, m \leq n$).

Nous résumons ces faits dans la conjecture suivante, équivalente à la *décidabilité du calcul propositionnel partiel*: toute suite de transformations décrites dans les cas 1 à 4, effectuées sur une famille finie d'ensembles finis E_i et de relations droites R_{ik} ($i, k \leq n$), est finie.

Si, pour deux indices différents $i, k \leq n$, la relation R_{ik} est univoque ($id(E_i) \supseteq R_{ik} \circ (R_{ik})^*$) on peut éliminer E_i de la famille, sans perdre les propriétés 1* à 6*. A cet effet soit $j: \{1, \dots, n\} \rightarrow \{1, \dots, n-1\}$ l'application surjective dont les valeurs sont données par:

$$j(m) = m \text{ pour } m < i, j(m) = m - 1 \text{ pour } i < m \leq n \text{ et } j(i) = j(k).$$

$$n' = n - 1;$$

$$E'_{j(m)} = E_m \text{ pour } m \neq i \text{ (en particulier } E'_{j(i)} = E_k);$$

$$R'_{j(l)j(m)} = R_{lm} \text{ pour } l \neq i \text{ et } m \neq i;$$

$g_m = id(E_m)$ pour $m \neq i$, $g_i: E_k \rightarrow E_i$ est donnée par $g_i = R_{ik}$.

L'élimination de ces redondances permet un gain de place et de temps lorsqu'on réitère les transformations indiquées à l'aide d'un ordinateur. Dans ce but, on peut encore améliorer les techniques décrites; par exemple, pour le 4^{me} cas, il suffit de parcourir les triplets d'indices i, j, k tels que $1 \leq i \leq j \leq k \leq n$.

III. ABP libres et validité des identités classiques

III.1. ABP universelle et ABP libre

La notion d'ABP universelle est liée à celles de satisfaction et d'homomorphisme; elle répond à l'idée de l'ABP «la plus générale» qui, munie d'une valuation déterminée, satisfait à un ensemble donné d'expressions propositionnelles. En particulier, elle fournit une définition plausible des ABP libres.

DÉFINITION. Soit $M \subseteq FV$. On appelle **ABP universelle relativement à M** , et on note $U(M)$, une ABP pour laquelle il existe une valuation $u: V \rightarrow U(M)$ satisfaisant à M et telle que, pour toute ABP A et toute valuation $v: V \rightarrow A$ satisfaisant à M , il existe un homomorphisme $h: U(M) \rightarrow A$ unique, tel que $h \circ u = v$.

THÉORÈME. Pour tout M donné, il existe une ABP universelle relativement à M , déterminée univoquement à l'isomorphie près.

Démonstration. L'existence de $U(M)$ est prouvée par «l'algèbre de Lindenbaum» $U(M) = E/R$ où $E = \{p \in FV \mid M \models Cfp\}$ et $R = \{(p, q) \mid M \models p \equiv q\}$. R est évidemment une relation d'équivalence sur E , compatible avec l'opération qui associe Cpq au couple $\langle p, q \rangle$ dans E . $U(M)$ est ainsi une structure dont les éléments distingués 0 et 1 sont les classes de R -équivalence contenant f et Cff respectivement. La valuation $u: V \rightarrow U(M)$, où $u(p)$ est la classe de R -équivalence contenant $p \in V$, est telle que

$$M \models p \text{ ssi } u \text{ satisfait à } p$$

pour tout p dans FV . Par conséquent:

a) la règle R_8 est trivialement satisfaite dans $U(M)$. La validité de R_1 – R_7 en trois variables se démontre par substitution; d'après le théorème 1, § I.2, $U(M)$ est donc une ABP;

b) l'extension de $u: V \rightarrow U(M)$ est définie exactement pour les expressions p de E , $\bar{u}: E \rightarrow U(M)$.

Pour une ABP A et une valuation $v: V \rightarrow A$ satisfaisant à M on a $E \subseteq \bar{V}$. Si $\bar{u}(p) = \bar{u}(q)$ dans $U(M)$ pour deux expressions p, q de E , la règle $M \models p \equiv q$ est valide dans toute ABP, d'où $\bar{v}(p) = \bar{v}(q)$ dans A . Ceci permet de construire une application $h: U(M) \rightarrow A$ avec $h(\bar{u}(p)) = \bar{v}(p)$ pour tout p de E . h est évidemment un homomorphisme, ses valeurs sont déterminées par celles que v attribue aux variables; les propriétés de l'ABP universelle sont ainsi vérifiées.

D'autre part, pour deux *ABP* U et U' universelles relativement à M il existe deux homomorphismes $h: U \rightarrow U'$, $h': U' \rightarrow U$ conservant les valeurs des variables; $h' \circ h$ et $h \circ h'$ ont également cette propriété et sont, de ce fait, confondus avec l'identité sur U et U' respectivement. h et h' sont donc des isomorphismes.

COROLLAIRE. Pour deux ensembles M, M' d'expressions de FV les trois propriétés sont équivalentes:

- $M \Vdash M'$
- M' est satisfait par $u: V \rightarrow U(M)$
- il existe un homomorphisme (nécessairement unique) $h: U(M') \rightarrow U(M)$ qui conserve les valeurs attribuées aux variables.

Exemples. Soit V un ensemble de n variables et $V^* = \{CfCpq \mid p, q \in V\}$; alors $U(V) = \mathbf{Z}_2$, $U(V^*)$ est l'algèbre de Boole libre à 2^{2^n} éléments, tandis que $U(\emptyset)$ est la somme directe de n facteurs isomorphes à \mathbf{Z}_2^2 .

DÉFINITION. Une *ABP* A est *libre* s'il existe V et un ensemble M d'expressions de la forme Cfp , p dans FV , tels que $A = U(M)$.

Remarques. Une algèbre de Boole est libre selon cette définition ssi elle est libre dans l'acception courante.

Une *ABP* universelle $U(M)$ est plongeable dans une algèbre de Boole ssi l'homomorphisme $U(M) \rightarrow U(M \cup V^*)$ est biunivoque. En particulier $U(\emptyset)$ est toujours une somme directe d'algèbres de Boole \mathbf{Z}_2^2 et se trouve donc plongée dans l'algèbre de Boole libre $U(V^*)$.

PROPOSITION. Toute *ABP* est le quotient fermé d'une *ABP* libre. Cette *ABP* libre a le même nombre d'éléments générateurs que son quotient.

Démonstration. Soit A une *ABP*, V un ensemble d'indices et $v: V \rightarrow A$ l'énumération d'un ensemble d'éléments générateurs de A . v est considérée comme une valuation de V dans A et son extension $\bar{v}: \bar{V} \rightarrow A$ permet de construire $M = \{Cfp \mid p \in \bar{V}\}$. Ainsi v satisfait à M dans l'*ABP* A ; il existe donc un homomorphisme $h: U(M) \rightarrow A$ tel que $v = h \circ u$. De plus, on remarque que l'extension \bar{u} est définie exactement sur \bar{V} et que $\bar{v} = h \circ \bar{u}$. Par conséquent, h est surjective et, pour tout $p, q \in \bar{V}$ tels que l'opération C de A est définie pour $\bar{v}(p), \bar{v}(q)$, on a $Cpq \in \bar{V}$; $\bar{u}(p)$ et $\bar{u}(q)$ peuvent ainsi être composés dans $U(M)$. h est donc un épimorphisme fermé.

Avec la proposition 2, § I.4, on a le corollaire suivant: toute *ABP* transitive est quotient fermé d'une *ABP* libre transitive.

III.2. Construction effective des *ABP* libres

Soient V un ensemble fini de variables, $M \subseteq FV$ un ensemble fini d'expressions

propositionnelles de la forme Cfp et $U(M)$ l'ABP libre correspondante. Nous voulons former une famille Φ d'algèbres de Boole finies et d'isomorphismes partiels, telle que la somme de la famille minimale sur Φ soit isomorphe à $U(M)$.

Soit p_1, \dots, p_n une suite d'expressions de FV telle que:

- pour tout $Cfp \in M$ l'expression p figure parmi les termes de la suite,
- pour tout $i \leq n$ on a $p_i \in V$, $p_i = f$ ou alors $p_i = Cp_j p_k$ pour deux indices j et k inférieurs à i .

Pour tout $i \leq n$ l'algèbre de Boole A_i et les éléments a_i, b_i, c_i de A_i sont définis de la manière suivante:

- si $p_i = f$ on prend $A_i \cong Z_2$ et $a_i = 0$;
- si $p_i \in V$ on prend $A_i \cong Z_2^2$, l'algèbre de Boole libre à un générateur, où a_i est justement l'élément générateur;
- si $p_i = Cp_j p_k$ on prend $A_i \cong Z_2^4$, l'algèbre de Boole libre à deux générateurs, b_i et c_i sont deux éléments générateurs et $a_i = C(b_i, c_i)$ dans A_i .

Pour tout triplet i, j, k tel que $p_i = Cp_j p_k$ on prend, pour $h_{ij}: A_j \rightarrow A_i$, l'isomorphisme partiel qui identifie l'élément a_j de A_j avec b_i de A_i (ainsi que les compléments respectifs et les unités), et, pour $h_{ik}: A_k \rightarrow A_i$, l'isomorphisme partiel qui identifie l'élément a_k de A_k avec c_i de A_i (ainsi que les compléments et les unités). Les autres isomorphismes partiels de Φ sont choisis de manière à n'identifier que les unités (0 et 1) entre les diverses algèbres de Boole.

La propriété caractéristique des algèbres de Boole libres permet alors d'étendre toute valuation $v: V \rightarrow A'$, satisfaisant à M dans l'ABP A' , à une famille d'homomorphismes $f_i: A_i \rightarrow A'$ (avec $f_i(a_i) = \bar{v}(p_i)$, $i \leq n$) compatibles avec les identifications imposées par h_{ik} ($i, k \leq n$). Réciproquement, une telle famille induit une valuation qui satisfait à M . La définition de $U(M)$ est donc équivalente à la propriété qui, dans la proposition du § II.5, caractérise la somme de la famille minimale sur Φ .

Le procédé décrit au § II.5 permet ainsi de construire directement la représentation duale de $U(M)$. La valuation $u: V \rightarrow U(M)$ est donnée par l'image $f_i(a_i)$ des générateurs a_i tels que $p_i \in V$; dans la représentation duale de $U(M)$ la valeur $u(p_i)$ est la préimage de a_i par g_i (avec $A_i = P(E_i)$ et $a_i \in E_i$).

Pour examiner la validité d'une règle $M \Vdash M'$, on peut évaluer les conclusions $q \in M'$ directement dans la représentation duale de $U(M)$; il suffit de tenir compte des identifications produites par les h_{ik} : $Y = h_{ik}(X)$ ssi $R_{ik} \circ R_{ik}(X) \subseteq X$ et $Y = R_{ik}(X)$.

La composition des ensembles E_i et des relations R_{ik} ($i, k \leq n$) correspondant à la famille Φ , la construction de la famille minimale (duale) sur Φ et l'évaluation des expressions de M' à l'aide de la valuation particulière \bar{u} ont été programmées, en Algol, pour la machine CDC 1604-A de l'Ecole Polytechnique Fédérale. La validité des règles $Cfp \Vdash p$ a été ainsi vérifiée pour toutes les expressions propositionnelles p déduites dans «Principia Mathematica», à l'exception de 2.81, 3.47, 3.48, 4.38 et 4.39. A noter que 3.48 et 4.39 sont obtenues de 3.47 et 4.38 respectivement, en rem-

plaçant les variables par leur négation. D'autre part, on utilise 3.47 (3.48) dans la déduction classique de 4.38 (4.39).

Remarque. Les *ABP* universelles $U(M)$, où M est un ensemble fini d'expressions propositionnelles quelconques, peuvent être construites de manière analogue.

On remplace, tout d'abord, M par $\bar{M} = \{Cfp \mid p \in M\}$ pour former la suite p_1, \dots, p_n et la famille Φ avec les éléments a_i, b_i, c_i dans A_i (comme pour la construction de $U(\bar{M})$). Il y a alors correspondance biunivoque entre les valuations $v: V \rightarrow A'$, satisfaisant à M dans une *ABP* A' , et les familles d'homomorphismes $f_i: A_i \rightarrow A'$, compatibles avec les h_{ik} et prenant la valeur $f_i(a_i) = 1$ pour tout $i \leq n$ tel que $p_i \in M$.

Les conditions $f_i(a_i) = 1$, pour $p_i \in M$, sont remplies ssi $g_i^*(a_i) = E'_i$ dans la représentation duale de A' (a_i est considéré comme une partie de E_i , $P(E_i) = A_i$); elles sont donc équivalentes à $g_i \circ R'_{iV} \subseteq R_{ii} \circ g_i$, si on prend $R_{ii} = id(a_i)$ au lieu de $id(E_i)$. La construction du § II.5 fournit, en partant de ces données, la représentation duale de l'*ABP* universelle $U(M)$.

III.3. *ABP* engendrées par trois éléments

La validité, dans les *ABP*, des identités Booléennes à une ou deux variables a été prouvée dans [2]. Avec quatre variables ou plus, il existe de nombreux contre-exemples: le cas où V est formé de trois variables restait ouvert. Le but de ce paragraphe est de montrer la validité des identités Booléennes en trois variables. Ce résultat est atteint par la classification des *ABP* libres à trois générateurs, qui s'avèrent toutes plongeables dans l'algèbre de Boole finie Z_2^8 .

LEMME 1. Soit $V = \{x, y, z\}$. Alors les trois énoncés suivants sont équivalents.

1. Pour tous p et q dans FV l'identité $Cfq, Cfp \Vdash p \equiv q$ est valide dans les *ABP* si $p \equiv q$ est valide dans Z_2 .
2. Pour tout ensemble fini M d'expressions propositionnelles de la forme Cfp , $U(M)$ est plongeable dans Z_2^8 .
3. Toute *ABP* engendrée par trois éléments est plongeable dans une algèbre de Boole.

Démonstration. Montrons les implications $1. \Rightarrow 2.$, $2. \Rightarrow 3.$ et $3. \Rightarrow 1.$:

$1. \Rightarrow 2.$) La forme particulière de M dans l'énoncé 2. fait que $V^* \Vdash M$. Il existe de ce fait un homomorphisme $h: U(M) \rightarrow U(V^*)$ où $U(V^*)$ est l'algèbre de Boole libre Z_2^8 . Le contenu de 1. est précisément la biunivocité de h .

$2. \Rightarrow 3.$) Si, pour tout M fini, l'*ABP* libre $U(M)$ est plongeable dans Z_2^8 , il en est de même pour M infini; il suffit de former une suite croissante $M_1 \subseteq M_2 \subseteq \dots$ d'ensembles finis $M_i \subseteq FV$ dont la réunion est M . Les homomorphismes correspondants $U(M_i) \rightarrow U(M_{i+1})$ ($i = 1, 2, \dots$) sont tous compatibles avec le plongement dans Z_2^8 puisqu'ils conservent les valeurs des variables x, y, z . La réunion des $U(M_i)$ dans Z_2^8 est une *ABP* dont on vérifie les propriétés caractérisant $U(M)$. Ainsi, 2. a pour consé-

quence que toute *ABP* libre avec $V = \{x, y, z\}$ est plongeable dans une algèbre de Boole. 3. découle alors de la proposition du § III.1.

3. \Rightarrow 1.) Pour tous p et q de FV l'*ABP* universelle $U(Cfp, Cfq)$ est engendrée par trois éléments; selon 3. les identités Booléennes y sont donc valides. En particulier $p \equiv q$ y sera satisfaite si c'est une tautologie.

DÉFINITION. Soient A et A' deux *ABP*. A' est *successeur* de A , s'il existe un homomorphisme $h: A \rightarrow A'$ et deux éléments non compatibles a, b dans A , avec $h(a)$ et $h(b)$ compatibles dans A' , tels que:

1. pour tout homomorphisme $h': A \rightarrow A''$ dans une *ABP* A'' où $h'(a)$ et $h'(b)$ sont compatibles, il existe un homomorphisme unique $h'': A' \rightarrow A''$ tel que $h' = h'' \circ h$.
2. si A est plongeable dans une algèbre de Boole, la paire d'éléments a, b est minimale; pour a' et b' non compatibles dans A , tels que $h(a')$ et $h(b')$ sont compatibles dans A' , $a' \leq a$ et $b' \leq b$ entraînent $a' = a$ et $b' = b$.

LEMME 2. Tout successeur d'une *ABP* libre est une *ABP* libre; réciproquement, pour toute *ABP* libre $U(M)$ où V et M sont finis, il existe une suite finie d'*ABP* libres dont chaque terme est successeur du précédent, le premier étant $U(\emptyset)$ et le dernier $U(M)$.

Démonstration. Soient $A = U(M)$ une *ABP* libre avec la valuation canonique $u: V \rightarrow A$ et A' un successeur de A . Il existe alors p, q dans FV avec $\bar{u}(p) = a, \bar{u}(q) = b$ tels que $p \not\leq q$ ainsi que M soient satisfaits par la valuation $h \circ u$ dans A' . La condition 1. revient alors à la définition de l'*ABP* universelle relativement à $M \cup \{p \not\leq q\}$.

Pour la réciproque, soit $U(M)$ une *ABP* libre; on peut faire apparaître toutes les expressions $p \in FV$ pour lesquelles $Cfp \in M$ dans une suite finie p_1, \dots, p_n telle que, pour tout $i \leq n$: $p_i = f$, $p_i \in V$ ou alors $p_i = Cp_j p_k$ pour deux indices j, k inférieurs à i .

Soit $M_0 = \emptyset$, $M_i = M_{i-1} \cup \{Cfp_i\}$ pour $1 \leq i \leq n$, de sorte que $U(M_n) = U(M)$. Pour $1 \leq i \leq n$ il existe un homomorphisme $h_i: U(M_{i-1}) \rightarrow U(M_i)$ puisque $M_i \Vdash M_{i-1}$. Si $Cfp_1, \dots, Cfp_{i-1} \Vdash Cfp_i$ on a $U(M_i) = U(M_{i-1})$ et on peut omettre le i -ème terme de la suite. Supposons ces répétitions éliminées. Pour tout $i \leq n$ il y a, dans $U(M_{i-1})$, deux éléments non compatibles a, b dont les images dans $U(M_i)$ sont compatibles; en effet, Cfp_i est satisfaite dans $U(M_i)$ mais pas dans $U(M_{i-1})$, $p_i = f$ ou $p_i \in V$ sont ainsi exclus; reste $p_i = Cp_j p_k$ et on peut prendre pour a, b les valeurs de p_j, p_k . La condition 1. pour le successeur de $U(M_{i-1})$ découle de la définition de l'*ABP* universelle $U(M_{i-1} \cup \{p_j \not\leq p_k\}) = U(M_i)$.

Si la condition 2. n'est pas satisfaite, par exemple pour les éléments a et b de $U(M_{i-1})$, on peut modifier la suite d'*ABP* libres en intercalant de nouveaux termes entre $U(M_{i-1})$ et $U(M_i)$. $U(M_{i-1})$ est alors plongeable dans une algèbre de Boole et il existe deux éléments $a' \leq a$ et $b' \leq b$, non compatibles, tels que $h_i(a')$ est compa-

tible avec $h_i(b')$. Soient p et q des expressions de FV , prenant les valeurs a' et b' dans $U(M_{i-1})$; soit $U = U(M_{i-1} \cup \{p \circ q\})$. Par définition, U remplit la condition 1. pour les éléments a', b' de $U(M_{i-1})$; il existe notamment deux homomorphismes $h: U(M_{i-1}) \rightarrow U$ et $h': U \rightarrow U(M_i)$ tels que $h_i = h' \circ h$. Si la condition 2. n'est pas encore remplie par a', b' et h , on remplace le couple a', b' par un couple strictement inférieur, on aboutit ainsi à un successeur de l'ABP finie $U(M_{i-1})$. D'autre part, la condition 1. est également vérifiée par h' et les éléments $h(a), h(b)$ de U ; si la condition 2. n'y est pas remplie, la construction peut être recommencée en remplaçant $U(M_{i-1})$ par U . On obtient, par itération, une suite d'ABP libres et d'homomorphismes conservant les éléments générateurs. Cette suite est finie car chaque terme est plongeable dans l'ABP finie $U(V^*)$.

Remarque. La définition des «successeurs» convient donc à l'énumération des ABP libres $U(M)$ où M est fini. Les algèbres de Boole n'ont pas de successeur, le nombre des successeurs d'une ABP plongeable dans une algèbre de Boole est relativement petit (moins de vingt lorsque $V = \{x, y, z\}$). La construction des successeurs d'une ABP finie A peut se faire à l'aide du procédé exposé au § II.5. Pour chaque paire d'éléments a, b de A , on forme une famille Φ contenant, en plus des sous-algèbres Booléennes maximales de A , une algèbre de Boole libre engendrée par deux éléments. Ces derniers sont identifiés à a et b respectivement par des isomorphismes partiels adéquats. La somme de la famille minimale sur Φ remplit alors la condition 1. Si A est plongeable dans une algèbre de Boole, on élimine les paires a, b qui ne sont pas minimales; dans la plupart des cas, cette élimination peut s'effectuer sans la construction de Φ et de la famille minimale.

LEMME 3. Soit A l'ABP telle que $A = A_1 + A_2 \pmod{h}$ où A_1, A_2 sont deux algèbres de Boole isomorphes à Z_2^5 et $h: A_1 \rightarrow A_2$ est l'isomorphisme partiel qui identifie un atome c de A_1 avec le complément d'un atome de A_2 (Cf. liste en appendice). Alors toute ABP A' , contenant A et engendrée par A , est plongeable dans Z_2^8 .

Démonstration. A_1 et A_2 sont deux sous-algèbres de A' dont l'intersection est formée des éléments $0, 1, c$ et $\neg c$ (identifiés par h). On vérifie que c est dans le centre de A' et que, pour tout $a \in A'$,

$$a = (a \wedge \neg c) \vee (a \wedge c) \quad \text{avec} \quad a \wedge \neg c \in A_1 \quad \text{et} \quad a \wedge c \in A_2$$

par induction sur le nombre d'occurrences de C dans les expressions propositionnelles dont les valeurs parcourent A' :

- pour $a \in A$, par exemple $a \in A_1$, on a $c \in A_1$ et $a \wedge \neg c \in A_1$. D'autre part, $a \wedge c$ vaut 0 ou c puisque c est un atome de A_1 ; dans les deux cas $a \wedge c \in A_2$.
- pour $a = C(a', a'')$ avec $a' \wedge \neg c, a'' \wedge \neg c \in A_1$ et $a' \wedge c, a'' \wedge c \in A_2$, c est évidemment compatible avec a et on a:

$$a \wedge c = c \wedge C(a' \wedge c, a'' \wedge c) \in A_2$$

$$a \wedge \neg c = \neg c \wedge C(a' \wedge \neg c, a'' \wedge \neg c) \in A_1$$

à cause de l'identité Booléenne $(Cxy) \wedge z = z \wedge C(x \wedge z)(y \wedge z)$.

Chaque élément a de A' se laisse ainsi décomposer en deux «composantes» $a \wedge \neg c$ dans A_1 et $a \wedge c$ dans A_2 ; ceci a pour conséquence:

$$A'_c = A_1/(c) \quad \text{et} \quad A'_{\neg c} = A_2/(\neg c).$$

Or $A_1/(c)$ et $A_2/(\neg c)$ sont isomorphes au quotient de Z_2^5 par un atome, soit Z_2^4 . Avec le corollaire 1, § I.6, on a finalement $A' \subseteq Z_2^4 \times Z_2^4 = Z_2^8$.

THÉORÈME. Toute *ABP* engendrée par trois éléments est plongeable dans une algèbre de Boole.

La *démonstration* résulte naturellement (Cf. Lemmes 1 et 2) de la classification de toutes les *ABP* libres $U(M)$ avec M fini, obtenue par la construction itérée des successeurs de $U(\emptyset)$.

On réduit sensiblement le nombre de ces constructions en retenant un seul représentant de chaque classe d'*ABP* isomorphes ainsi obtenues. Le nombre de ces *ABP* dépasse largement la centaine; il convient donc de présenter la démonstration du théorème sous la forme d'une liste d'*ABP*, numérotées de 1 à 60 (Cf. appendice) et satisfaisant aux conditions suivantes:

- $U(\emptyset)$ est la première *ABP* de la liste;
- toute *ABP* de la liste, sauf la première, est le successeur d'une *ABP* précédente;
- tout successeur d'une *ABP* de numéro inférieur à 58 est isomorphe à l'une des 60 *ABP* de la liste complète;
- chacune des trois *ABP* 58, 59 et 60 est engendrée par l'*ABP* A (sans numéro) donnée en fin de liste.

L'application systématique du critère de plongeabilité (fin § I.7) montre que chacune des *ABP* de 1 à 60 est plongeable dans Z_2^8 . On peut donc décrire une telle *ABP* par l'image dans Z_2^8 de ses sous-algèbres Booléennes maximales, soit par les partitions correspondantes de l'ensemble des atomes de Z_2^8 (numérotés de 1 à 8).

Restent les successeurs itérés de 58, 59 et 60. Un raisonnement par induction montre que ceux-ci sont tous engendrés par une sous-algèbre isomorphe à A et tombent ainsi sous les hypothèses du lemme 3.

Remarque. La seule *ABP* transitive engendrée par A est Z_2^8 ; elle figure dans la liste sous le numéro 11. Les autres *ABP* transitives de la liste sont 1, 2, 42, 51 et 54; on peut les «décomposer» en produit d'*ABP* centrales (§ I.3), dans le même ordre: $Z_2^2 + Z_2^2 + Z_2^2$, $Z_2^4 + Z_2^2$, $Z_2^4 \times (Z_2^2 + Z_2^2)$, $Z_2^2 \times (Z_2^2 + Z_2^3)$ et $(Z_2^2 + Z_2^2) \times (Z_2^2 + Z_2^2)$.

Les quotients fermés de ces 6 *ABP* fournissent une classification complète des 20 *ABP* transitives engendrées par 1, 2 ou 3 éléments.

Appendice

Liste de 60 ABP libres à trois générateurs

ABP Succes-		Partitions de $\{1, 2, 3, 4, 5, 6, 7, 8\}$, correspondant aux			
No:	seur de	sous-algèbres Booléennes maximales de l'ABP			
1	—	(1357/2468)	(1256/3478)	(1234/5678)	
2	1	(15/26/37/48)	(1234/5678)		
3	2	(15/26/37/48)	(234/1/678/5)		
4	3	(15/26/37/48)	(234/1/678/5)	(15/2/6/34/78)	
5	4	(234/1/678/5)	(15/2/6/34/78)	(15/26/3/7/4/8)	
6	5	(15/2/6/34/78)	(15/26/3/7/4/8)	(234/1/6/78/5)	
7	6	(1/5/2/6/34/78)	(15/26/3/7/4/8)		
8	7	(1/5/2/6/34/78)	(15/26/3/7/4/8)	(1/5/26/34/7/8)	
9	8	(15/26/3/7/4/8)	(1/5/2/6/34/7/8)		
10	9	(1/5/26/3/7/4/8)	(1/5/2/6/34/7/8)		
11	10	(1/2/3/4/5/6/7/8)			
12	8	(1/5/2/6/34/78)	(15/26/3/7/4/8)	(1/5/26/34/7/8)	(15/2/6/3/4/78)
13	6	(15/26/3/7/4/8)	(234/1/6/78/5)	(15/2/6/3/4/78)	
14	13	(234/1/6/78/5)	(15/2/6/3/7/4/8)		
15	14	(234/1/6/7/8/5)	(15/2/6/3/7/4/8)		
16	13	(15/26/3/7/4/8)	(1/5/24/6/3/78)	(15/2/6/3/4/78)	
17	16	(15/26/3/7/4/8)	(1/5/24/6/3/78)	(15/2/6/3/4/78)	(1/5/246/3/7/8)
18	13	(15/26/3/7/4/8)	(234/1/6/78/5)	(15/2/6/3/4/78)	(1/5/2346/7/8)
19	6	(15/26/3/7/4/8)	(234/1/6/78/5)	(15/2/6/34/7/8)	
20	19	(15/26/3/7/4/8)	(1/5/234/6/7/8)	(15/2/6/34/7/8)	
21	20	(15/26/3/7/4/8)	(1/5/234/6/7/8)	(15/2/6/34/7/8)	(1/5/236/7/4/8)
22	19	(15/26/3/7/4/8)	(234/1/6/78/5)	(15/2/6/34/7/8)	(1/5/246/3/78)
23	6	(15/2/6/34/78)	(15/26/3/7/4/8)	(234/1/6/78/5)	(1/5/246/3/78)
24	23	(15/2/6/34/78)	(15/26/3/7/4/8)	(234/1/6/78/5)	(1/5/246/3/7/8)
25	6	(15/2/6/34/78)	(15/26/3/7/4/8)	(234/1/6/78/5)	(1/5/2346/7/8)
26	5	(234/1/678/5)	(15/26/3/7/4/8)	(15/2/6/34/7/8)	
27	26	(234/1/678/5)	(15/2/6/3/7/4/8)		
28	26	(15/26/3/7/4/8)	(15/2/6/34/7/8)	(234/1/67/8/5)	
29	28	(15/26/3/7/4/8)	(15/2/6/34/7/8)	(234/1/67/8/5)	(1/5/2467/3/8)
30	28	(15/26/3/7/4/8)	(15/2/6/34/7/8)	(234/1/67/8/5)	(1/5/246/37/8)
31	26	(234/1/678/5)	(15/26/3/7/4/8)	(15/2/6/34/7/8)	(24678/3/1/5)
32	26	(234/1/678/5)	(15/26/3/7/4/8)	(15/2/6/34/7/8)	(236/478/1/5)
33	26	(234/1/678/5)	(15/26/3/7/4/8)	(15/2/6/34/7/8)	(2468/37/1/5)
34	5	(234/1/678/5)	(15/2/6/34/78)	(15/26/3/7/4/8)	(23467/8/1/5)

35	34	(234/1/678/5)	(15/2/6/34/78)	(15/26/3/7/4/8)	(1/5/2467/3/8)
36	34	(234/1/678/5)	(15/2/6/34/78)	(15/26/3/7/4/8)	(1/5/236/47/8)
37	5	(234/1/678/5)	(15/2/6/34/78)	(15/26/3/7/4/8)	(2368/47/1/5)
38	5	(234/1/678/5)	(15/2/6/34/78)	(15/26/3/7/4/8)	(478/236/1/5)
39	4	(234/1/678/5)	(15/2/6/34/78)	(15/2/6/37/48)	
40	39	(15/2/6/34/78)	(15/2/6/37/48)	(234/1/6/78/5)	
41	40	(15/2/6/37/48)	(1/2/34/5/6/78)		
42	41	(1/5/2/6/37/48)	(1/5/2/6/34/78)		
43	40	(15/2/6/34/78)	(15/2/6/37/48)	(234/1/6/78/5)	(1/5/6/237/48)
44	39	(234/1/678/5)	(15/2/6/34/78)	(15/2/6/37/48)	(2367/48/1/5)
45	39	(234/1/678/5)	(15/2/6/34/78)	(15/2/6/37/48)	(248/367/1/5)
46	4	(15/26/37/48)	(15/2/6/34/78)	(234/1/6/78/5)	
47	46	(15/26/37/48)	(1/5/2/6/34/78)		
48	46	(15/26/37/48)	(15/2/6/34/78)	(234/1/6/78/5)	(1/5/2367/48)
49	4	(15/26/37/48)	(234/1/678/5)	(15/2/6/34/78)	(1/5/2367/48)
50	3	(15/26/37/48)	(234/1/678/5)	(1/5/26/3478)	
51	50	(234/1/678/5)	(1/5/26/37/48)		
52	2	(15/26/37/48)	(34/12/78/56)		
53	52	(15/26/37/48)	(34/12/78/56)	(15/26/34/78)	
54	53	(15/26/37/48)	(34/12/78/56)	(15/26/34/78)	(12/56/37/48)
55	52	(15/26/37/48)	(34/12/78/56)	(1/5/2/6/3478)	
56	55	(34/12/78/56)	(1/5/2/6/3478)	(1/5/26/37/48)	
57	56	(1/5/2/6/3478)	(1/5/26/37/48)	(34/1/2/78/56)	
58	57	(1/5/2/6/3478)	(1/5/26/37/48)	(34/1/2/78/56)	(3/4/1/256/7/8)
59	56	(34/12/78/56)	(1/5/2/6/3478)	(1/5/26/37/48)	(3/4/1256/7/8)
60	55	(15/26/37/48)	(34/12/78/56)	(1/5/2/6/3478)	(1256/3/7/4/8)
A		(1/2/5/6/3478)	(1256/3/4/7/8)		

BIBLIOGRAPHIE

- [1] A. DAIGNEAULT, *Théorie des modèles en logique mathématique*, Uni. de Montréal (1963).
- [2] S. KOCHEN and E. SPECKER, *Logical structures arising in Quantum Theory*, Proc. Model Theory Symp., Berkeley (1963).
- [3] S. KOCHEN and E. SPECKER, *The calculus of partial propositional functions*, Proc. of the 1964 internat. Congress for Logic, Methodology and Philosophy of Science.
- [4] S. KOCHEN and E. SPECKER, *The problem of hidden variables in Quantum Mechanics*, Journal of Mathematics and Mechanics, 17, No. 1 (July 1967).
- [5] G. W. MACKEY, *The mathematical foundations of quantum mechanics* (Benjamin, New York 1963).
- [6] R. SIKORSKI, *Boolean Algebras*, Ergebnisse der Mathematik und ihrer Grenzgebiete (N.F.) H. 25 (1960).

Reçu le 17 avril 1969