Algèbres et anneaux de Boole

Marc SAGE

6 février 2018

Table des matières

[1] terminolgie de Bourbaki

1 Algèbres de Boole

Une *algèbre de Boole* ou *algèbre booléenne* est un ensemble ordonné A vérifiant les trois propriétés suivantes :

1. toute partie **finie** de A a un infimum et un supremum[2] ;
2. $\wedge := \inf$ et $\vee := \sup$ sont distributifs l'un sur l'autre ;
3. il y a deux éléments 0 et 1 de A et une application $\left\{\begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & \overline{a} \end{array}\right.$ vérifiant $\left\{\begin{array}{l} a \wedge \overline{a} = 0 \\ a \vee \overline{a} = 1 \end{array}\right.$ pour tout $a \in A$.

Questions.

1. *Montrer que $\mathfrak{P}(E)$ est une algèbre de Boole pour tout ensemble E.*
   Donner un autre exemple d'algèbre de Boole.

On fixe pour la suite une algèbre de Boole A.

2. *Montrer que le couple $(0, 1)$ est unique et le caractériser 0 et 1 à l'aide de l'ordre sur A.*
3. *Montrer que l'application $a \mapsto \overline{a}$ est unique et involutive. Que valent $\overline{0}$ et $\overline{1}$?*
4. *Montrer les lois de De Morgan*

$$\begin{array}{rcl} \overline{a \wedge b} & = & \overline{a} \vee \overline{b} \\ \overline{a \vee b} & = & \overline{a} \wedge \overline{b} \end{array}$$

Pouvait-on se passer de la distributivité de $\vee$ sur $\wedge$ pour obtenir ces dernières ?

5. *En déduire une autre structure d'algèbre de Boole sur A.*

On suppose dorénavant l'algèbre A de cardinal fini.

6. *On note (μ_i) les éléments minimaux de $A \backslash \{0\}$. Montrer que tout élément de A s'écrit comme un supremum (éventuellement nul) de μ_i.*
7. *Montrer que A est isomorphe à un $\mathfrak{P}(E)$.*
8. *Quelle(s) hypothèse(s) raisonnable(s) rajouter pour que le résultat reste valable sans la finitude de A ?*

Solution proposée.

1. On considère la structure suivante : $\begin{array}{cccccc} \leq & \wedge & \vee & 0 & 1 & \overline{a} \\ \subset & \cap & \cup & \emptyset & E & {}^{c}A \end{array}$. Les vérifications sont aisées et laissées au lecteur.

   Un autre exemple est l'ensemble des diviseurs positifs d'un entier $n \geq 1$ quadratfrei[3] pour la structure $\begin{array}{cccccc} \leq & \wedge & \vee & 0 & 1 & \overline{a} \\ \mid & \text{pgcd} & \text{ppcm} & 1 & n & \frac{n}{a} \end{array}$.
2. Puisque $1 = a \vee \overline{a} \geq a$ pour tout $a \in A$, on a $1 = \max A$, ce qui montre l'unicité de 1 et de même $0 = \min A$ est unique.
3. Soit $a \in A$ et $\widetilde{a}$ satisfaisant les propriétés de $\overline{a}$. On peut écrire

$$\widetilde{a} = \widetilde{a} \wedge 1 = \widetilde{a} \wedge (a \vee \overline{a}) = \underbrace{(\widetilde{a} \wedge a)}_{=0} \vee (\widetilde{a} \wedge \overline{a}) = \widetilde{a} \wedge \overline{a}.$$

L'expression $\widetilde{a} = \widetilde{a} \wedge \overline{a}$ est symétrique en $\overline{a}$ et $\widetilde{a}$, donc vaut également $\overline{a}$, d'où $\widetilde{a} = \overline{a}$.

Puisque a satisfait les propriétés de $\overline{\overline{a}}$ pour tout $a \in A$, l'unicité sus-montrée conclut à l'involutivité de $a \mapsto \overline{a}$.

Montrons que $\left(\overline{0}, \overline{1}\right) = (1, 0)$. D'après l'involutivité de $a \mapsto \overline{a}$, il suffit de montrer $\overline{0} = 1$. D'après son unicité, il s'agit de montrer $\left\{\begin{array}{l} 0 \wedge 1 = 0 \\ 0 \vee 1 = 1 \end{array}\right.$, ce qu'il est aisé de voir en écrivant $\left\{\begin{array}{l} 0 \wedge 1 \leq 0 = \min A \\ 0 \vee 1 \geq 1 = \max A \end{array}\right.$.

[2] un tel ordre est appelé *treillis*
[3] *i. e.* ne possédant aucun diviseur qui est un carré

4. Soient a et b dans A. Posons $c := a \wedge b$ et $c' := \overline{a} \vee \overline{b}$. D'après l'unicité de $\overline{c}$, montrer $\overline{c} = c'$ revient à montrer $\begin{cases} c \wedge c' = 0 \\ c \vee c' = 1 \end{cases}$. Avanti :

$$\begin{aligned} \text{d'une part, } c \wedge c' &= a \wedge b \wedge \left(\overline{a} \vee \overline{b}\right) = \underbrace{\left(a \wedge b \wedge \overline{a}\right)}_{\leq a \wedge \overline{a} = 0} \vee \underbrace{\left(a \wedge b \wedge \overline{b}\right)}_{\leq b \wedge \overline{b} = 0} \leq 0 \vee 0 = 0, \\ \text{d'autre part, } c \vee c' &= (a \wedge b) \vee \overline{a} \vee \overline{b} = \underbrace{\left(a \vee \overline{a} \vee \overline{b}\right)}_{\geq a \vee \overline{a} = 1} \wedge \underbrace{\left(b \vee \overline{a} \vee \overline{b}\right)}_{\geq b \vee \overline{b} = 1} \geq 1 \wedge 1 = 1, \text{ CQFD.} \end{aligned}$$

Pour avoir l'autre loi, on applique $\bar{\cdot}$ et on invoque son involutivité :

$$\overline{a \vee b} = \overline{\overline{\overline{a}} \vee \overline{\overline{b}}} = \overline{\overline{\overline{a} \wedge \overline{b}}} = \overline{a} \wedge \overline{b}, \text{ CQFD.}$$

Par ailleurs, les lois de De Morgan permettent via le procédé ci-dessus de tranformer la distributivité de $\wedge$ sur $\vee$ en celle de $\vee$ sur $\wedge$ et réciproquement : les deux sont donc nécesaires.

5. Il suffit de renverser l'ordre : cela échange les rôles de $\wedge$ et $\vee$ ainsi que de 0 et 1, l'application $a \mapsto \overline{a}$ restant la même.

6. Pensons un instant A comme un $\mathfrak{P}(E)$: les éléments minimaux de $\mathfrak{P}(E) \setminus \{\emptyset\}$ sont alors les singletons, ce qui devrait éclaircir la proposition à montrer (on reconstruit les éléments de A à partir des briques élémentaires μ_i).

Montrons déjà que 1 est un supremum de μ_i. Dans l'écriture

$$1 = \bigwedge \left(\mu_i \vee \overline{\mu_i}\right),$$

chaque terme du développement (à l'exception de $\bigwedge \overline{\mu_i}$) est de la forme $\mu_i \wedge a$, donc est plus petit que μ_i, donc ou bien nul ou bien valant μ_i. En élaguant les éventuels 0, en rajoutant $\bigvee \mu_i$ pour se débarasser du $\bigwedge \overline{\mu_i} = \overline{\bigvee \mu_i}$ puis en rajoutant les éventuels μ_i manquant, on voit que 1 est le supremum de *tous*[4] les μ_i.

Il est maintenant aisé de conclure. Ensemblistement, toute partie est réunion de ses singletons. Traduisons dans A : un élément $a \in A$ s'écrit

$$a = a \wedge 1 = a \wedge \left(\bigvee \mu_i\right) = \bigvee \left(a \wedge \mu_i\right).$$

Or, l'élément $a \wedge \mu_i$ est plus petit que μ_i, donc ou bien est nul ou bien vaut μ_i et réciproquement tout $\mu_i \leq a$ s'écrit $\mu_i = a \wedge \mu_i$. Finalement, on peut écrire

$$a = \bigvee_{\mu_i \leq a} \mu_i.$$

7. Notons E l'ensemble des μ_i. Vu ce qui précède, on regarde les applications

$$\left\{ \begin{array}{ccc} A & \longrightarrow & \mathfrak{P}(E) \\ a & \overset{f}{\longmapsto} & \{\mu_i\}_{\mu_i \leq a} \\ \bigvee \mu_j & \overset{g}{\longleftarrow} & \{\mu_j\} \end{array} \right. .$$

Pour montrer qu'elles sont réciproques l'une de l'autre, il y a deux choses à regarder.

Pour $a \in A$, l'égalité prouvée ci-dessus nous donne

$$g(f(a)) = \bigvee_{\mu_i \leq a} \mu_i = \bigvee \left(a \wedge \mu_i\right) = a.$$

Par ailleurs, on a vu que les μ_i plus petit qu'un $a \in A$ donné sont les μ_i non nuls tels que $\mu_i \wedge a = \mu_i$. Pour $a = \bigvee \mu_j$, sachant $\mu_i \wedge \mu_j = \delta_i^j \mu_i$, on trouve les μ_j qui apparaissent dans a, ce qui montre que $f\left(g\left(\{\mu_j\}\right)\right) = \{\mu_j\}$.

Il reste à montrer que cette bijection préserve la structure d'algèbre booléenne.

Si $a \leq b$, les $\mu_i \leq a$ seront automatiquement $\leq b$, donc il y aura plus de $\mu_i \leq b$ que de $\mu_i \leq a$, d'où l'inclusion $f(a) \subset f(b)$. Réciproquement, la croissance de $P \mapsto \sup P$ est claire.

[4] Vue l'interprétation ensembliste, cela est rassurant.

Les μ_i minorant $a \wedge b$ étant ceux minorant a et b, on a $f(a \wedge b) = f(a) \cap f(b)$. Autrement dit, f est un morphisme du magma $(A, \wedge)$ vers le magma $(P(E), \cap)$. Comme ce morphisme est bijectif, sa réciproque g l'est, d'où $g(X \cap Y) = g(X) \wedge g(Y)$ pour tout $X, Y \subset E$. Même histoire pour $\vee$ et $\cup$.

Les couples $(0, 1)$ et $(\emptyset, E)$ sont échangés par la bijection. Enfin, pour $a \in A$ fixé, tout μ_i s'écrit

$$\mu_i = \mu_i \wedge 1 = \mu_i \wedge (a \vee \overline{a}) = (\mu_i \wedge a) \vee (\mu_i \wedge \overline{a}),$$

donc minore a ou $\overline{a}$ (sinon la conjonction ci-dessus serait nulle), mais ne peut minorer les deux à la fois (sinon il minorerait $a \wedge \overline{a} = 0$ et serait nul). Ceci montre que les $\mu_i \leq \overline{a}$ sont les $\mu_i \not\leq \overline{a}$, d'où $f(\overline{a}) = {}^c f(a)$. L'égalité $g({}^c X) = \overline{g(X)}$ s'en déduit sans peine.

8. Reprenons tout ce qui précède et voyons où cela achoppe. Sans hypothèse de finitude, les suprema ne sont plus assurés d'existence et les propriétés de distributivité s'écroulent. Il est donc raisonnable de rajouter une hypothèse d'*achèvement* de l'ordre (toute partie admet un infimum et un supremum) ainsi qu'une hypothèse de distributivité généralisée :

$$\bigwedge_{i \in I} (a_i \vee b_i) = \bigvee_{f \in \{0,1\}^I} \left(a_{f(i)} \wedge b_{f(i)}\right) \text{ pour tous } a_i, b_i \text{ dans } A.$$

Nous laissons le lecteur vérifier que la preuve ci-dessus reste encore valide sous ces hypothèses – lesquelles, notera-t-il, sont nécessaires car vraies pour A un $\mathfrak{P}(E)$.

Remarque. Dans le cas général, une algèbre de Boole est isomorphe à l'algèbre des parties ouvertes et fermées d'un compact *totalement discontinu* (th Stone). Si de plus l'algèbre est complète, on peut supposer le compact *extrèmement discontinu* (les ouverst sont stables par adhérence, les fermés sont stable par intérieur)

Un espace topologique est *complètement déconnecté* si les seules parties connexes sont l'ensemble vide et les singletons.

La dualité de Stone montre l'équivalence entre la catégorie des algèbres de Boole et la catégorie (duale) des espaces topologiques compactes, Hausdorff et totalement discontinu (ces espaces sont appelés *espace de Stone*).

A un espace de Stone S on associe l'ensemble $\operatorname{Clop} S$ des ouverts-fermés (qui est une algèbre de Boole pour les opérations ensemblistes). A un morphisme $\varphi : S \longrightarrow T$, on associe $\operatorname{Clop} \varphi : \begin{array}{ccc} \operatorname{Clop} T & \longrightarrow & \operatorname{Clop} S \\ U & \longmapsto & \varphi^{-1}(U) \end{array}$

A une algèbre de Boole B on associe l'ensemble $\operatorname{Ult} B$ des ultrafiltres de B. On munit $\operatorname{Ult} B$ de la topologie engendrée par la famille $O_b := \{\mathfrak{p} \in \operatorname{Ult} B \ ; \ b \in \mathfrak{p}\}$ losque b décrit B. A un morphisme d'algèbre de Boole $f : A \longrightarrow B$ on associe $\operatorname{Ult} f : \begin{array}{ccc} \operatorname{Ult} B & \longrightarrow & \operatorname{Ult} B \\ \mathfrak{p} & \longmapsto & f^{-1}(\mathfrak{p}) \end{array}$

Enfin (pour toute les algèbres de Boole) on a un isomorphisme naturel $\mu_b : \left\{ \begin{array}{ccc} B & \longmapsto & \operatorname{Clop} \operatorname{Ult} B \\ b & \longrightarrow & O_b \end{array} \right.$ (voir plus haut).

On a aussi (pour les espaces de Stone) $\nu_S : \left\{ \begin{array}{ccc} S & \longrightarrow & \operatorname{Ult} \operatorname{Clop} S \\ s & \longmapsto & \{O \in \operatorname{Clop} S \ ; \ x \in O\} \end{array} \right.$

2 Anneaux et algèbres booléen

Un anneau **booléen**[5] est un anneau dans lequel tout élément est idempotent.

Une algèbre **de Boole**[6] ou algèbre **booléenne** est un treillis[7] A distributif[8] borné (on peut parler de $0 := \min A$ et de $1 := \max A$) complémenté (il y a une invoultion $\left\{ \begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & \overline{a} \end{array} \right.$ vérifiant $\left\{ \begin{array}{l} a \wedge \overline{a} = 0 \\ a \vee \overline{a} = 1 \end{array} \right.$ pour tout $a \in A$). On peut montrer que toute algèbre de Boole *finie* est isomorphe à l'algèbre $\mathfrak{P}(E)$ des parties d'un ensemble (fini).

On notera $\mathbb{F}_2$ le corps à deux éléments $\{0, 1\}$ muni de la somme $1 + 1 = 0$.

Le but de l'exercice est d'établir une correspondance entre anneaux et algèbres booléens.

[5] Bourbaki écrit « booléien »

[6] *cf.* feuille sur les relation binaires pour un exercice consacré

[7] ordre où toute partie finie a un infimum et un supremum (Bourbaki parle d'ordre **réticulé**)

[8] les lois binaires $\wedge := \inf$ et $\vee := \sup$ sont distributives l'une sur l'autre

1. *Donner des exemples simples d'anneaux booléen. Montrer que $(\mathfrak{P}(E), \Delta, \cap)$ est un anneau booléen pour tout ensemble E.*
2. *Soit A une algèbre de Boole. Trouver une somme Δ telle que $(A, \Delta, \wedge)$ soit un anneau booléen.*

On fixe pour la suite un anneau booléen A.

3. *Montrer que A de caractéristique 2 et commutatif.*
4. *Montrer que la relation $a \leq b \overset{\text{déf.}}{\iff} a = ab$ définit un ordre sur A.*
5. *Mettre une structure d'algèbre de Boole sur A ordonné par $\leq$.*
6. *Vérifier que la correspondance entre algèbres et anneaux booléen sus-exhibée est bijective entre les $\mathfrak{P}(E)$ pour E ensemble quelconque*[9].
7. *En déduire que les anneaux booléen finis sont les $\mathbb{F}_2^E$.*
8. *Contre-exemple si infini ?*

Solution proposée.

1. La notation rappelée nous guide : $\mathbb{F}_2$ est bien commutatif et ses éléments sont idempotents. Ces deux propriétés passant au produit (en d'autres termes : le produit d'anneaux booléen étant un anneau booléen), on en déduit que $\mathbb{F}_2^E$ est un anneau booléen pour tout ensemble E.

   Rappelons incidemment que $P(E)$ et $\mathbb{F}_2^E$ sont en bijection via les fonctions caractéristiques et que les propriétés $\begin{cases} \chi_{A\Delta B} = \chi_A + \chi_B \\ \chi_{A\cap B} = \chi_A \cap \chi_B \end{cases}$ permettent de transporter la structure d'anneau de $\mathbb{F}_2^E$ vers $P(E)$. La commutativité et l'idempotence passant à l'isomorphisme, la structure d'anneau booléen passe aussi à l'isomorphisme, ce qui conclut.
2. Pensons notre algèbre de Boole comme un $P(E)$: l'addition Δ vérifie alors $a\Delta b = (a \cap {}^c b) \cup ({}^c a \cap b)$, ce qui se réécrit en utilisant uniquement les lois de l'algèbre de Boole

$$\begin{aligned} a\Delta b &= \left(a \wedge \overline{b}\right) \vee \left(\overline{a} \wedge b\right) \\ &= (a \vee b) \wedge \left(\overline{a} \vee \overline{b}\right). \end{aligned}$$

   Revenons dans notre algèbre de Boole. On sait déjà que $\wedge$ est commutative et idempotente[10]. L'égalité ci-dessus définit une loi Δ : il reste à montrer qu'elle munit A d'une structure de groupe abélien et que $\wedge$ est distributif sur Δ. Ces propriétés sont déjà connues pour les algèbres $P(E)$. Par ailleurs, elles équivalent à la conjonction d'énoncés (une infinité) ayant chacun un nombre fini de variables libres : trois pour l'associativité et la distributivité, deux pour la commutativité, une pour le neutre et le symétrique pour Δ. Il suffit donc de montrer ces propriétés pour une algèbre de Boole (quelconque) engendrée par trois éléments ; or, une telle algèbre est finie, donc isomorphe à de $P(E)$ d'après le rappel, algèbre où toutes les propriétés voulues sont vraies. ? ? ? ? ?
3. $2 = 2^2 = 4 = 2 + 2$. Alors $ab + ba = (a + b)^2 + a + b = 2(a + b) = 0$.
4. (réf car idem, antisym car comm, enfin $a = ab$ et $b = bc => a = ab = a(bc) = (ab)c = ac$),
5. si $x \leq a, b$ alors$ax = x$ et $bx = x$, d'où $abx = ax = x$ et $x \leq ab$; réciproeimqn, on a bien $ab \leq a, b$, donc $ab = \inf\{a, b\}$.

   si $x \geq a, b$, alors $x \geq a, b, ab$, donc $x \geq a + b + ab$; récirpquemnt, $a(a + b + ab) = a + ab + ab = a$ (car car=2), donc $a + b + ab = \sup\{a, b\}$.

   on a $a(1 + a) = a + a = 0$ et $a + (1 + a) + a(1 + a) = 3a + 1 + a^2 = 1$.

   enfin, $a \wedge (b \vee c) = a(b + c + bc) = ab + ac + abc$ et $(a \wedge b) \vee (a \vee c) = ab + ac + abac$, idem ; de plus $a \vee (b \wedge c) = a + bc + abc$ et

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= (a + b + ab)(a + c + ac) \\ &= a + \underline{ac + ac} + \underbrace{ba} + bc + (bac) + \underbrace{ab} + (abc) + aabc \\ &= a + bc + abc \end{aligned}$$

[9] disons pour les parties E d'un même grand ensemble Ω pour pouvoir bien parler d'applications

[10] *i. e.* que tout élément est idempotent pour cette loi

6. partant de l'algèbre $P(A)$, le nouveau $\cap$ est $\wedge$ donc $\cap$, le nouveau Δ est

$$\left(a \wedge \overline{b}\right) \vee \left(\overline{a} \wedge b\right) = \left(a \cap \overline{b}\right) \cup \left(\overline{a} \wedge b\right) = a\Delta b, \text{ ok}$$

7. en parntat de l'annue $P(A)$:
   l'ordre est défini par $a \leq b$ ssi $a = ab = a \cap b$, ie ssi $a \subset b$, ok.
   Le $\wedge$ est le produit $\cap$.
   le $\vee$ ets $a + b + ab = A\Delta B\Delta (A \cap B) = A \cup B$ (: chque élt appartient à un nobre impair de partie, une ou trois)
   le 0 est le 0 de l'anneau, donc $\emptyset$
   le 1 est le 1 de l'anneau, donc E
   le $\overline{a}$ est est $1 + a = E\Delta a = {}^c a$.
8. $\mathbb{F}_2^{(E)}$ pose pb.

3 Anneaux booléiens[11], version idéaux

Pour apprécier l'utilisation des idéaux premiers et maximaux.

On rapeplel que la racind $\sqrt{I} = \{x,\ \exists n \geq 1,\ x^n \in I\}$ d'un idéal I vaut $\bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$

soit A booléien

1. *Mq si A intègre, il est nul ouvaut $\mathbb{F}_2$.En déduire que, tout idéal premier est maximal.*
2. *Mq un idéal strict I est intersction des idéaux premiers le contenant. En déduire que tout idéal irréductible est maximal*
3. *De ce qui préèce, déduire que A est isomorphe à un sous-anneau d'un anneau produit $\mathbb{F}_2^E$*
4. *Quid si A fini ?*

1. $a^2 = a \implies a = 1$ si $a \neq 0$. Alors A/p intègre no nul, donc F_2, donc corp, donc p max
2. On rappelle que $\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$. Puisque les puissances sont triviale, tout idéal vaut sa racine. Soit I irréd. Si premier, on a termliné. SInon, $\bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$ contient au plus un terme : si un esel I premeier, sinon $I = A$
3. on envoie A dans l produit des $A/m = F_2$. INj ? si a dans tous les m, a est dans tous les p, donc dans $\sqrt{0}$ d'où $a = a^2 = 0$.
4. si A fini, les m sont finis ; alors chinois dit que $\prod A/m \cong A/\cap m$ iso. Or $\cap m = \sqrt{0} = 0$, donc $A/\cap m \cong A$, CQFD.

[11] terminolgie de Bourbaki