CaMUS **5**, 1 – 21

Semi-anneaux, semi-corps et leurs propriétés

Véronique Bazier-Matte et Mélissa Barbe Marcoux

Résumé Dans cet article, nous définissons les semi-anneaux et les semi-corps, qui s'apparentent aux anneaux et aux corps, mais dans lesquels les inverses additifs n'existent pas nécessairement, et nous étudions leurs propriétés. Par la suite, nous nous intéressons au concept d'idéaux de semi-anneaux. Finalement, nous nous penchons sur les algèbres de Boole et les treillis et nous observons leurs liens avec les semi-anneaux.

1 Introduction

Les semi-anneaux et les semi-corps sont des structures algébriques semblables aux anneaux et aux corps, mais sans inverse additif. Ils sont à la base de la géométrie tropicale. Un des exemples les plus simples de ce genre de structure est l'ensemble des nombres naturels muni de l'addition et la multiplication usuelles. Il n'est donc pas étonnant qu'il s'agisse du premier exemple de semi-anneau étudié historiquement. La définition des semi-anneaux a été introduite formellement par Vandiver en 1934 [Van39], mais Dedekind [Ded96] avait déjà étudié quelques exemples à la fin du XIX^e siècle. La théorie des semi-anneaux a commencé à se développer véritablement au début des années 50, alors que celle des semi-corps a commencé au début des années 60 [RV04].

L'étude des semi-anneaux permet de travailler sur des structures sans inverse additif. Ainsi, nous généralisons le concept d'idéal, développé initialement pour les anneaux, au cadre des semi-anneaux. Il est également possible d'établir des liens avec les treillis et algèbres de Boole, qui possèdent de nombreuses applications.

2 Définitions

Commençons par définir les semi-anneaux. Il existe plusieurs définitions différentes dans la littérature scientifique. Celle que nous avons choisi d'utiliser ici est celle de Kala et Korbelář [KK10], qui est plus générale que la plupart des autres définitions existantes.

Nous aimerions remercier chaleureusement MM. Ibrahim Assem, professeur à l'Université de Sherbrooke, et Juan Carlos Bustamante, chargé de cours, pour leur aide et leur supervision qui ont permis l'écriture de cet article durant notre cours d'initiation à la recherche.

Définition 2.1. Un *semi-anneau* est un triplet $(S,\ \oplus, \odot)$ où S est un ensemble non vide et $\oplus$, $\odot$ sont des opérations sur S appelées respectivement l'*addition* et la *multiplication*. L'addition est commutative et associative, tandis que la multiplication est associative. De plus, la multiplication se distribue à gauche et à droite sur l'addition, c'est-à-dire que, pour tous $a,\ b,\ c \in S$, on a $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ et $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

Pour alléger la lecture, notons un semi-anneau S plutôt que $(S,\ \oplus\ ,\ \odot)$.

Exemple 2.2.

a) $(\mathbb{N},\ +\ ,\ \cdot)$ où $+$ et $\cdot$ représentent respectivement l'addition et la multiplication usuelles des entiers est un semi-anneau. Par la suite, nous écrirons simplement $\mathbb{N}$.

b) L'ensemble des réels $\mathbb{R}$ muni des deux opérations suivantes est un semi-anneau : l'addition est $a \oplus b = \max(a,\ b)$, le plus grand des deux réels a et b, et la multiplication est $a \odot b = a + b$. En effet, $\max(a,\ \max(b,\ c)) = \max(a,\ b,\ c) = \max(\max(a,\ b)\ ,\ c)$, ce qui établit l'associativité de l'addition. Il est clair qu'elle est aussi commutative, et que la multiplication est associative.

Il reste à vérifier que les deux opérations sont compatibles. Soit $a,\ b,\ c \in \mathbb{R}$ et supposons sans perte de généralité que $b \leq c$. Donc, $a + b \leq a + c$. D'où

$$a \odot (b \oplus c) = a + \max(b,\ c) = a + c = \max(a + b,\ a + c) = (a \odot b) \oplus (a \odot c).$$

De la même façon, nous obtenons que $\max(a,\ b) + c = \max(a + c,\ b + c)$.

c) Soit X un ensemble non-vide et soit $\mathcal{P}(X)$ l'ensemble des parties de X. Alors, $(\mathcal{P}(X),\ \cup\ ,\ \cap)$ est un semi-anneau où $\cup$ et $\cap$ représentent respectivement l'union et l'intersection entre deux ensembles. En effet, $\cup$ est une opération associative et commutative sur $\mathcal{P}(X)$, tandis que $\cap$ est une opération associative sur $\mathcal{P}(X)$. Par ailleurs, soit $A,\ B,\ C \in \mathcal{P}(X)$. Comme

$$(B \cup C) \cap A = A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\,,$$

l'intersection $\cap$ se distribue sur l'union $\cup$.

De même, $\cup$ se distribue également sur $\cap$ et $\cap$ est une opération commutative sur $\mathcal{P}(X)$. Ainsi, nous aurions pu définir l'addition sur $\mathcal{P}(X)$ comme étant plutôt $\cap$ et la multiplication comme étant plutôt $\cup$ et nous aurions obtenu aussi un semi-anneau.

Les propriétés de ces opérations amènent au concept d'algèbre de Boole, étudié à la section 5. Remarquons donc au passage que $(\mathcal{P}(X), \cup, \cap)$ constitue un exemple d'algèbre de Boole.

Remarque 2.3. Certains auteurs tels que Assem et Dupont [AD13], Bistarelli et Gaducci [BG06], Fenga, Jun, Zhaoc [FJZ08] définissent les semi-anneaux en exigeant en outre que $(S,\ \oplus)$ soit un monoïde commutatif avec l'élément neutre 0, que $(S,\ \odot)$ soit un monoïde avec l'élément neutre 1 et que $0 \odot a = a \odot 0$ pour tout $a \in S$.

3 Préliminaires

Définissons à présent plusieurs propriétés que peuvent posséder les semi-anneaux et observons les liens entre ces propriétés.

Définition 3.1. Soit S un semi-anneau.

a) Le semi-anneau S est *idempotent additivement* (ou simplement *idempotent*) si $a \oplus a = a$ pour tout $a \in S$.

b) Par ailleurs, S est *absorbant* si $a \oplus (a \odot b) = a = a \oplus (b \odot a)$ pour tous $a, b \in S$. L'opération $\oplus$ est alors dite *absorbante* sur $\odot$.

c) Finalement, S est *commutatif* si $a \odot b = b \odot a$ pour tous $a, b \in S$.

Exemple 3.2.

a) $\mathbb{N}$ est un semi-anneau commutatif, mais il n'est ni idempotent, ni absorbant.

b) $(\mathbb{R},\ \max,\ +)$ est un semi-anneau idempotent, commutatif mais non absorbant. En effet, $\max(a,\ a) = a$ et $\max(a,\ b) = \max(b,\ a)$. De plus, si $b > 0$, alors $\max(a,\ a + b) \neq a$. Toutefois, $(\mathbb{R}_-,\ \max,\ +)$ est un semi-anneau absorbant.

c) $(\mathcal{P}(X),\ \cup,\ \cap)$ est un semi-anneau idempotent, absorbant et commutatif.

Les propriétés suivantes se retrouvent dans les travaux de Rudeanu et Vaida [RV04].

Définition 3.3. Soit S un semi-anneau.

a) Un élément $g \in S$ est appelé un *plus grand élément* si $a \oplus g = g$ pour tout $a \in S$.

b) Un élément $e \in S$ est appelé une *identité multiplicative* si $a \odot e = a = e \odot a$ pour tout $a \in S$.

c) Un élément $p \in S$ est appelé un *plus petit élément* si $a \oplus p = a$ pour tout $a \in S$.

d) Un élément $z \in S$ est appelé un *zéro* si $a \odot z = z = z \odot a$ pour tout $a \in S$.

Lemme 3.4. *S'il existe dans un semi-anneau un plus grand élément (ou une identité multiplicative, ou un plus petit élément, ou un zéro), alors celui-ci est unique.*

Démonstration. Soit g_1 et g_2 deux plus grands éléments dans le même semi-anneau. Par définition, $g_1 = g_1 \oplus g_2 = g_2$ car l'addition est commutative. L'unicité des plus petits éléments se vérifie de la même façon. De même, soit e_1 et e_2 deux identités multiplicatives. Par définition, $e_1 = e_1 \odot e_2 = e_2$. La démonstration de l'unicité des zéros est identique. □

Exemple 3.5.

a) Dans $\mathbb{N}$, 1 est l'identité multiplicative et 0 est le plus petit élément et le zéro. Toutefois, ce semi-anneau ne possède pas de plus grand élément.

Considérons à présent $(\mathbb{N} \cup \{\infty\},\ +,\ \cdot)$ où convenons que $a + \infty = \infty$ et $a \cdot \infty = \infty = \infty \cdot a$. Avec cette définition, il s'agit d'un semi-anneau avec le plus grand élément $g = \infty$.

Finalement, considérons $(\{a \in \mathbb{N} \mid a > 1\},\ +,\ \cdot)$. Il est facile de vérifier que ce triplet satisfait aux axiomes de définition d'un semi-anneau. Il s'agit d'un semi-anneau sans plus grand élément, ni identité multiplicative, ni plus petit élément, ni zéro.

b) $(\mathbb{R},\ \max,\ +)$ est un semi-anneau avec l'identité multiplicative $e = 0$, mais sans plus grand élément, ni zéro, ni plus petit élément.

En considérant $(\mathbb{R}_+^*,\ \max,\ +)$, nous obtenons un semi-anneau sans identité multiplicative.

Étudions plutôt $(\mathbb{R} \cup \{-\infty\},\ \max,\ +)$ tel que $-\infty \leq a$ et $-\infty + a = -\infty$ pour tout $a \in \mathbb{R} \cup \{-\infty\}$. L'élément $-\infty$ est le zéro et le plus petit élément de ce semi-anneau, car $a + -\infty = -\infty$ et $\max(a,\ -\infty) = a$ pour tout a.

De même, soit, $(\mathbb{R} \cup \{\infty\},\ \max,\ +)$. Il s'agit d'un semi-anneau avec le plus grand élément $g = \infty$ puisque $\max(a,\ \infty) = \infty$ pour tout a.

c) $(\mathcal{P}(X),\ \cup,\ \cap)$ contient un plus grand élément X, qui est aussi l'identité multiplicative. Il contient également un plus petit élément et un zéro, $\varnothing$.

Contrairement à ce que peuvent laisser croire les derniers exemples, le zéro et le plus petit élément d'un semi-anneau ne sont pas nécessairement égaux. Dans l'exemple suivant, le semi-anneau possède un plus petit élément qui n'est pas un zéro.

Exemple 3.6. Notons $S = [0,\ \infty] \times [0,\ \infty]$. Soit $(S,\ \min,\ \odot)$ où

$$\begin{array}{rccc} \min : & S \times S & \longrightarrow & S \\ & ((x_1,\ y_1),\ (x_2,\ y_2)) & \longmapsto & (\min(x_1,\ x_2),\ \min(y_1,\ y_2)) \end{array}$$

et

$$\begin{array}{rccc} \odot : & S \times S & \longrightarrow & S \\ & ((x_1,\ y_1),\ (x_2,\ y_2)) & \longmapsto & (x_1,\ y_2)\,. \end{array}$$

Il est clair que min est associatif et commutatif et que $\odot$ est associative. Vérifions la distributivité.

$$\begin{aligned} (x_1,\ y_1) \odot \min((x_2,\ y_2),\ (x_3,\ y_3)) &= (x_1,\ y_1) \odot (\min(x_2,\ x_3),\ \min(y_2,\ y_3)) \\ &= (x_1,\ \min(y_2,\ y_3)) \\ &= (\min(x_1,\ x_1),\ \min(y_2,\ y_3)) \\ &= \min((x_1,\ y_2),\ (x_1,\ y_3))\,. \end{aligned}$$

D'où

$$(x_1,\, y_1) \odot \min\left((x_2,\, y_2)\,,\ (x_3,\, y_3)\right) \\ = \min\left((x_1,\, y_1) \odot (x_2,\, y_2)\,,\ (x_1,\, y_1) \odot (x_3,\, y_3)\right).$$

De même,

$$\min\left((x_1,\, y_1)\,,\ (x_2,\, y_2)\right) \odot (x_3,\, y_3) \\ = \min\left((x_1,\, y_1) \odot (x_3,\, y_3)\,,\ (x_2,\, y_2) \odot (x_3,\, y_3)\right).$$

Ainsi, $(S,\ \min\,,\ \odot)$ est un semi-anneau. Il possède $(\infty,\, \infty)$ comme plus petit élément, car $\min\left((x,\, y)\,,\ (\infty,\, \infty)\right) = (x,\, y)$. Cependant, $(x,\, y) \odot (\infty,\, \infty) \neq (\infty,\, \infty)$ si $y \neq \infty$.

Remarquons que ce semi-anneau ne possède pas de zéro.

Au même titre que les anneaux, les semi-anneaux peuvent posséder des éléments inversibles, définis ci-dessous. Cette définition sert d'ailleurs de base à la définition des semi-corps, voir [VC09].

Définition 3.7. Soit S un semi-anneau possédant une identité multiplicative notée e.

a) Un élément $a \in S$ est *inversible* s'il existe $b \in S$ tel que $a \odot b = e = b \odot a$. L'élément b est appelé l'*inverse* de a et est noté a^{-1}.

b) Un *semi-corps* T est un semi-anneau $(T,\ \oplus\,,\ \odot)$ dans lequel chaque élément différent du zéro s'il existe est inversible.

Remarque 3.8. Si l'inverse d'un élément existe, alors il est unique. En effet, supposons qu'il existe deux inverses de a notés b et c. Alors, $b = b \odot a \odot c = c$.

Exemple 3.9.

a) Le seul élément inversible de $\mathbb{N}$ est 1, d'inverse 1.

b) Dans $(\mathbb{R},\ \max\,,\ +)$, chaque élément x est inversible d'inverse $-x$, ce qui fait de ce semi-anneau un semi-corps.

c) Mis à part X, aucun élément de $\mathcal{P}(X)$ n'est inversible. L'inverse de X est donc X.

Il est également possible de définir une relation d'ordre sur les semi-anneaux. Donnons donc d'abord une définition des ensembles partiellement ordonnés à partir de laquelle nous construirons celle des semi-anneaux partiellement ordonnés, voir [KS85].

Définition 3.10. Soit E un ensemble. Une relation $\leq$ sur E est appelée une relation d'*ordre partiel* si elle est réflexive, antisymétrique et transitive. L'ensemble E muni de l'ordre partiel $\leq$ est alors dit *partiellement ordonné* par cette relation.

Définition 3.11. Un semi-anneau S est dit *partiellement ordonné* si l'ensemble S est partiellement ordonné sous une relation $\leq$ et si pour tous $a,\ b,\ c \in S$, les deux conditions suivantes sont vérifiées :

a) si $a \leq b$, alors $a \oplus c \leq b \oplus c$;

b) si $a \leq b$, alors $a \odot c \leq b \odot c$ et $c \odot a \leq c \odot b$.

Remarque 3.12. En vertu de cette définition des semi-anneaux partiellement ordonnés, la relation $\leq$ est compatible avec les opérations $\oplus$ et $\odot$.

Exemple 3.13.

a) $\mathbb{N}$ et $(\mathbb{R} \cup \{-\infty\},\ \max,\ +)$ sont des semi-anneaux partiellement ordonnés par l'ordre usuel.

b) $(\mathcal{P}(X),\ \cup,\ \cap)$ est également un semi-anneau ordonné par l'inclusion $\subseteq$.

Les définitions ci-dessous sont données par [AD13].

Définition 3.14. Soit S un semi-anneau.

a) Si S possède un plus petit élément p, alors S est *non-négatif* si $a \oplus b = p$ implique $a = p = b$ pour tous a, $b \in S$.

b) Si S est commutatif et possède un zéro z, alors S est *intègre* si $a \odot b = z$ implique $a = z$ ou $b = z$ pour tous a, $b \in S$.

Exemple 3.15.

a) Contrairement à $(\mathbb{Z},\ +,\ \cdot)$, $\mathbb{N}$, $(\mathbb{R} \cup \{-\infty\},\ \max,\ +)$ et $(\mathcal{P}(X),\ \cup,\ \cap)$ sont des semi-anneaux non-négatifs.

b) En outre, $\mathbb{N}$ et $(\mathbb{R} \cup \{-\infty\},\ \max,\ +)$ sont des semi-anneaux intègres alors que $(\mathcal{P}(X),\ \cup,\ \cap)$ n'est pas intègre.

Définition 3.16. Soit S un semi-anneau. Un élément $a \in S$ est *régulier* si l'égalité $a \oplus b = a \oplus c$ implique $b = c$ pour tout b, $c \in S$. Si tous les éléments de S sont réguliers, alors le semi-anneau est *régulier*.

Exemple 3.17. Le semi-anneau $\mathbb{N}$ est régulier, alors que ce n'est pas le cas pour les semi-anneaux $(\mathbb{R} \cup \{-\infty\},\ \max,\ +)$ et $(\mathcal{P}(X),\ \cup,\ \cap)$.

Les propositions suivantes relient les différentes propriétés des semi-anneaux. En particulier, la proposition ci-dessous (énoncée par [RV04], [BG06]) énumère quelques propriétés des semi-anneaux absorbants tandis que la suivante explicite une condition pour obtenir un semi-anneau absorbant.

Proposition 3.18. *Soit S un semi-anneau absorbant.*

a) Si S possède une identité multiplicative e, alors e est également le plus grand élément de S et S est idempotent.

b) Le semi-anneau S possède un plus petit élément si et seulement s'il possède un zéro. En outre, ces éléments sont égaux.

Démonstration.

a) Soit $e \in S$ l'identité multiplicative de S. Comme S est absorbant, $a = a \oplus (a \odot b)$ pour tous $a,\ b \in S$. En particulier, nous obtenons $e = e \oplus (e \odot b)$, d'où $e = e \oplus b$ pour tout b, ce qui fait de e un plus grand élément.

   En utilisant encore la propriété d'absorption, $a = a \oplus (e \odot a) = a \oplus a$ pour tout a. Ainsi, S est idempotent.

b) Soit $p \in S$ le plus petit élément de S. Comme S est absorbant, $p \oplus (p \odot a) = p = p \oplus (a \odot p)$, ce qui implique $p \odot a = p = a \odot p$.

   À présent, supposons que z est un zéro. L'absorption de S implique aussi $a = a \oplus (a \odot z)$, c'est-à-dire $a = a \oplus z$ pour tout a.

□

Proposition 3.19. *Un semi-anneau qui possède un plus grand élément qui est l'identité multiplicative est absorbant.*

Démonstration. Montrons que $a \oplus (a \odot b) = a = a \oplus (b \odot a)$ pour tous $a,\ b \in S$. Soit g le plus grand élément et l'identité multiplicative de S. Nous avons

$$a \oplus (a \odot b) = (a \odot g) \oplus (a \odot b) = a \odot (g \oplus b) = a \odot g = a.$$

De la même façon, nous obtenons que $a \oplus (b \odot a) = a$. □

Exemple 3.20. Soit $S = \{0,\ 1,\ 2\}$ avec les opérations $x \oplus y = \min(x + y,\ 2)$ et $x \odot y = \min(xy,\ 2)$ pour tous $x,\ y \in S$. Il est clair que $\oplus$ est associatif et commutatif, de même que $\odot$ est associatif. Montrons que $\odot$ se distribue sur $\oplus$. Pour tous $x,\ y,\ z \in S$, nous avons

$$\begin{aligned} x \odot (y \oplus z) &= \min(x \cdot \min(y + z,\ 2),\ 2) \\ &= \min(x(y + z),\ 2x,\ 2) \\ &= \min(xy + xz,\ 2) \\ &= \min(xy + xz,\ xy + 2,\ xz + 2,\ 2) \\ &= \min(\min(xy + 2) + \min(xz + 2),\ 2) \\ &= (x \odot y) \oplus (x \odot z). \end{aligned}$$

Il en va de même pour la distributivité à droite. Ainsi, S est un semi-anneau. De plus, $x \oplus 2 = \min(x + 2,\ 2) = 2$ implique que 2 est le plus grand élément de S et $1 \odot x = \min(1 \cdot x,\ 2) = \min(x,\ 2) = x$ que 1 est sont identité multiplicative.

Remarquons que $1 \oplus (1 \odot 1) = 2 \neq 1$, donc S n'est pas absorbant.

La proposition suivante établit un lien entre les éléments réguliers et inversibles dans les semi-anneaux [AD13].

Proposition 3.21. *Soit S un semi-anneau et $e \in S$ l'identité multiplicative. Si e est régulier, alors tous les éléments inversibles de S le sont également.*

Démonstration. Soit a, b, $c \in S$ tels que a est inversible et $a \oplus b = a \oplus c$. Comme $a \odot a^{-1} = e$, en multipliant à droite chaque côté par a^{-1} et en distribuant, nous obtenons $e \oplus (a^{-1} \odot b) = e \oplus (a^{-1} \odot c)$. On sait que e est régulier, donc $a^{-1} \odot b = a^{-1} \odot c$ et ainsi $b = c$, ce qui fait de a un élément régulier. □

Le lemme ci-dessous concerne les semi-corps et servira à étudier l'ordre d'un semi-corps, voir [VC09].

Lemme 3.22. *Soit T un semi-corps et a, b et $c \in T$. Si $a \oplus b \oplus c = a$, alors $a \oplus b = a$.*

Démonstration. Soit T un semi-corps et a, b et $c \in T$ tels que $a \oplus b \oplus c = a$. En multipliant à droite chaque côté de l'égalité par $a^{-1} \odot b \odot a^{-1}$ et en additionnant $c \odot a^{-1}$, nous obtenons

$$(b \odot a^{-1}) \oplus (b \odot a^{-1} \odot b \odot a^{-1}) \oplus (c \odot a^{-1} \odot b \odot a^{-1}) \oplus (c \odot a^{-1}) = (b \odot a^{-1}) \oplus (c \odot a^{-1}).$$

En vertu de la propriété de distributivité, il est possible de réécrire cette égalité :

$$(b \odot a^{-1} \oplus c \odot a^{-1}) \odot (1 \oplus b \odot a^{-1}) = b \odot a^{-1} \oplus c \odot a^{-1}.$$

Il suffit donc de multiplier à gauche par $(b \odot a^{-1} \oplus c \odot a^{-1})^{-1}$ et à droite par a pour obtenir

$$a \oplus b = a.$$ □

Les prochaines propositions concernent les semi-anneaux partiellement ordonnés. Dans la première proposition, une propriété des semi-anneaux partiellement ordonnés est montrée, tandis que la deuxième fournit des conditions suffisantes pour obtenir un semi-anneau partiellement ordonné.

Proposition 3.23. *Si un semi-anneau est partiellement ordonné et possède un plus petit élément, alors il est non-négatif.*

Démonstration. Soit S un semi-anneau partiellement ordonné, p son plus petit élément et $a,\ b \in S$ tel que $a \oplus b = p$. D'une part, nous savons que $p \leq a \leq a \oplus b$ et d'autre part, nous savons que $p \leq b \leq a \oplus b$. Comme $a \oplus b = p$, il est possible de déduire que $p \leq a \leq p$ et $p \leq b \leq p$. Ainsi, S est non négatif. □

Proposition 3.24.

a) Tout semi-anneau idempotent est partiellement ordonné.

b) Tout semi-anneau régulier et non négatif est partiellement ordonné.

c) Tout semi-corps est partiellement ordonné.

Démonstration.

a) Supposons que S est un semi-anneau idempotent et définissons la relation $\leq$ sur S par $a \leq b$ si et seulement si $a \oplus b = b$.

Montrons que $\leq$ est un ordre partiel sur S. En vertu de l'idempotence $a \oplus a = a$ implique que $a \leq a$ pour tout $a \in S$. Aussi, $a \leq b$ et $b \leq a$ donnent $a \oplus b = b$ et $b \oplus a = a$, d'où $a = b$. Enfin, $a \leq b$ et $b \leq c$ entraînent $a \oplus b = b$ et $b \oplus c = c$, d'où $a \oplus c = a \oplus b \oplus c = b \oplus c = c$ et alors $a \leq c$.

Il faut aussi montrer que cet ordre partiel est compatible avec les opérations de S. D'une part, $a \leq b$ implique $a \oplus b = b$ et il en découle, en vertu de l'idempotence, que $b \oplus c = a \oplus b \oplus c = a \oplus c \oplus b \oplus c$ et donc, $a \oplus c \leq b \oplus c$. D'autre part, $a \odot c \oplus b \odot c = b \odot c$ et $c \odot a \oplus c \odot b = c \odot b$, d'où $a \odot c \leq b \odot c$ et $c \odot a \leq c \odot b$.

b) Supposons que S est non-négatif et définissons la relation $\leq$ par $a \leq b$ si et seulement s'il existe $c \in S$ tel que $a \oplus c = b$.

Montrons que $\leq$ est une relation d'ordre. Puisque S est non-négatif, il possède un plus petit élément p. Nous savons que $a \oplus p = a$ donc $a \leq a$ pour tout $a \in S$. Montrons à présent l'antisymétrie de la relation. Soit $a,\ b \in S$ tels que $a \leq b$ et $b \leq a$. Ceci implique qu'il existe $c,\ d \in S$ tels que $a \oplus c = b$ et $b \oplus d = a$. En substituant b dans la deuxième égalité, nous obtenons $a \oplus c \oplus d = a$, d'où il est possible de déduire que $c \oplus d = p$ en vertu de la régularité de S. Ainsi, $c = p = d$ car S est non-négatif, ce qui prouve $a = b$ et donc la relation est antisymétrique. Par ailleurs, soit $a,\ b,\ c \in S$ tels que $a \leq b$ et $b \leq c$. Ainsi, il existe $x,\ y \in S$ tels que $a \oplus x = b$ et $b \oplus y = c$. Or, $a \oplus (x \oplus y) = (a \oplus x) \oplus y = b \oplus y = c$. Donc, nous avons $a \leq c$.

Il faut également prouver que cet ordre fait de S un semi-anneau partiellement ordonné. Prenons $a,\ b,\ c \in S$ tels que $a \leq b \leq c$. Donc, il existe $d \in S$ tel que $a \oplus d = b$. Puisque $a \oplus c \oplus d = b \oplus c$ et $c \odot a \oplus c \odot d = c \odot (a \oplus d) = c \odot b$, nous en déduisons que $a \oplus c \leq b \oplus c$ et $c \odot a \leq c \odot b$. Il en est de même pour la multiplication par c à droite.

c) Soit T un semi-anneau dont l'identité multiplicative est notée e. Définissons la relation $\leq$ ainsi : $a \leq b$ si et seulement si $a = b$ ou s'il existe $c \in T$ tel que $a \oplus c = b$.

Trivialement, cette relation est réflexive. Afin de montrer l'antisymétrie, prenons a et $b \in T$ tels que $a \leq b$ et $b \leq a$ et supposons qu'il existe c et $d \in T$ tels que $a \oplus c = b$ et $b \oplus d = a$. Nous savons que $a \oplus c \oplus d = b \oplus d = a$, d'où nous déduisons, en vertu du lemme 3.22, que $a \oplus c = a$, ce qui donne $b = a$. Prenons à présent a, b et $c \in T$ tels que $a \leq b \leq c$ pour prouver la transitivité. Alors, il existe $x \in T$ tel que $a \oplus x = b$ ou $a = b$ et il existe $y \in T$ tel que $b \oplus y = c$ ou $b = c$. Si $a = b$ ou $b = c$, la transitivité est triviale. Sinon, $a \oplus x \oplus y = b \oplus y = c$ d'où il également possible de conclure $a \leq c$.

Montrons en outre que la relation $\leq$ est compatible avec l'addition et la multiplication. Soit a et $b \in T$ tels que $a \leq b$. Si $a = b$, alors $a \oplus c = b \oplus c$,

$a \odot c = b \odot c$ et $c \odot a = c \odot b$, de sorte que $a \oplus c \leq b \oplus c$, $a \odot c \leq b \odot c$ et $c \odot a \leq c \odot b$. Sinon, il existe $d \in T$ tel que $a \oplus d = b$. Comme $a \oplus d \oplus c = b \oplus c$, alors $a \oplus c \leq b \oplus c$. De plus $(c \odot a) \oplus (c \odot d) = c \odot (a \oplus d) = c \odot b$ de sorte que $c \odot a \leq c \odot b$. De même, $a \odot c \leq b \odot c$.

□

4 Homomorphismes

Il est aussi intéressant de regarder les applications entre semi-anneaux. Plus particulièrement, considérons les semi-anneaux qui possèdent un zéro et un plus petit élément tels que décrits dans la définition 3.3. Les notations et la plupart des résultats proviennent des travaux de Allen [All69].

Définition 4.1. Soient deux semi-anneaux S et S'. Une application $f : S \longrightarrow S'$ est un *homomorphisme* si $f(a \oplus b) = f(a) \oplus' f(b)$ et $f(a \odot b) = f(a) \odot' f(b)$ pour tous a, $b \in S$.

Un homomorphisme $f : S \longrightarrow S'$ est un *isomorphisme* s'il existe un homomorphisme $g : S' \longrightarrow S$ tel que $g \circ f = \mathrm{id}_S$ et $f \circ g = \mathrm{id}_{S'}$. S et S' sont alors dits *isomorphes* et notés $S \cong S'$.

Naturellement, le *noyau* d'un homomorphisme est noté $\mathrm{Ker} f = \{x \in S \mid f(x) = 0_{S'}\}$.

Remarque 4.2. Soit 0_S et $0_{S'}$ les zéros des semi-anneaux S et S'. Alors, $f(0_S) = 0_{S'}$. En effet, pour tout $x \in S$ nous savons que $f(x) = f(x \oplus 0_S) = f(x) \oplus' f(0_S)$, d'où $f(0_S) = 0_{S'}$.

Lemme 4.3. *Un homomorphisme de semi-anneaux $f : S \longrightarrow S'$ est un isomorphisme si et seulement si f est bijectif.*

Démonstration. Comme un isomorphisme admet une application inverse, alors f est bijectif.

Réciproquement, supposons que $f : S \longrightarrow S'$ est un homomorphisme bijectif. Alors, il existe une application inverse de f, notée g.

Nous avons alors

$$\begin{aligned} g(a \oplus' b) &= g(f(g(a)) \oplus' f(g(b))) \\ &= g(f(g(a) \oplus g(b))) \\ &= g(a) \oplus g(b). \end{aligned}$$

De même, $g(a \odot' b) = g(a) \odot g(b)$. Comme g est un homomorphisme, f est un isomorphisme. □

Il devient pertinent de chercher un équivalent au théorème d'isomorphisme pour les anneaux. Il faudra d'abord définir la notion d'idéal et l'adaptée aux semi-anneaux.

Définition 4.4. Soit S un semi-anneau et I un ensemble tel que $I \subseteq S$. Alors, I est un *idéal* de S si :

a) pour tous $a, b \in I$, nous avons $a \oplus b \in I$.

b) pour tous $a \in I$ et $x \in S$, nous avons $a \odot x \in I$ et $x \odot a \in I$.

Écrivons alors $I \lhd S$.

Exemple 4.5.

a) Soit un semi-anneau commutatif S. Alors, $Sx = \{a \odot x \mid a \in S\}$ pour un $x \in S$. Nous prétendons que $Sx \lhd S$. En effet, soit $a, b \in Sx$. Alors, $a = a' \odot x$ et $b = b' \odot x$ avec $a', b' \in S$. Ainsi, $a \oplus b = a' \odot x \oplus b' \odot x = (a' \oplus b') \odot x \in Sx$. De plus, soit $y \in S$. Alors, $y \odot a = y \odot (a' \odot x) = (y \odot a') \odot x \in Sx$ et $a \odot y = (a' \odot x) \odot y = (a' \odot y) \odot x \in Sx$.

b) Soit le semi-anneau $(\mathbb{N}, +, \cdot)$. Posons $I = \mathbb{N}\backslash\{1\}$. Alors, I est un idéal de $\mathbb{N}$. En effet, soit $x, y \in I$ et $a \in \mathbb{N}$. Alors, $x + y \in I$, car $1 = 1 + 0 = 0 + 1$, mais $x \neq 1$ et $y \neq 1$. De plus, $a \cdot x \neq 1$, car $x \neq 1$, d'où le résultat. Toutefois, observons que $0 + I = I$ et $1 + I = \mathbb{N}\backslash\{0, 2\}$ et donc $(0 + I) \cap (1 + I) = \mathbb{N}\backslash\{0, 1, 2\} \neq \varnothing$.

c) Soit $f : S \longrightarrow S'$ un homomorphisme. Montrons que $\mathrm{Ker} f$ est un idéal de S. Soit $x, y \in \mathrm{Ker} f$ et $a \in S$. Alors, $f(x \oplus y) = f(x) \oplus' f(y) = 0_{S'}$ et donc, $x \oplus y \in \mathrm{Ker} f$. De plus, $f(a \odot x) = f(a) \odot' f(x) = 0_{S'} = f(x) \odot' f(a) = f(x \odot a)$ et ainsi, $a \odot x, x \odot a \in \mathrm{Ker} f$.

Comme dans le cas des anneaux, il est possible de faire un lien entre semi-corps et idéaux, voir [AL09].

Théorème 4.6. *Soit T un semi-anneau commutatif avec une identité multiplicative. Alors, T est un semi-corps si et seulement si ses seuls idéaux sont $\{0\}$ et T.*

Démonstration. Supposons que T est un semi-corps. Soit $I \lhd T$ tel que $I \neq \{0\}$. Prenons $x \in I$, $x \neq 0$. Alors, $x \in T$ est inversible. De ce fait, $x \odot x' = x' \odot x = e \in I$. Comme l'identité multiplicative est dans l'idéal, nous obtenons $I = T$.

Réciproquement, supposons que les seuls idéaux de T sont $\{0\}$ et T. Soit $x \in T$ tel que $x \neq 0$. Cherchons x' tel que $x \odot x' = e = x' \odot x$. Soit $Tx = \{t \odot x \mid t \in T\}$ l'idéal engendré par x. Comme $x \in Tx$, $Tx \neq \{0\}$ et ainsi, $Tx = T$ ce qui implique que $e \in Tx$. Il existe donc un $x' \in T$ tel que $x \odot x' = e = x' \odot x$. □

Avec cette définition d'idéal, l'exemple 4.5 b) permet de constater que la congruence modulo un idéal n'est pas une équivalence puisque $\{x + I\}_{x \in S}$ n'est pas nécessairement une partition de S. Nous avons donc besoin d'une définition d'idéal plus restrictive.

Définition 4.7. Soit S un semi-anneau et I un ensemble tel que $I \lhd S$. I est un *Q-idéal* s'il existe un ensemble $Q \subseteq S$ tel que $\{q \oplus I\}_{q \in Q}$ est une partition de S.

Exemple 4.8. Soit le semi-anneau $(\mathbb{N},\ +\ ,\ \cdot)$. Alors, $\langle m \rangle = \{n \cdot m \mid n \in \mathbb{N}\}$ est un idéal de $\mathbb{N}$. En effet, soit $x,\ y \in \langle m \rangle$ et $a \in \mathbb{N}$. Alors, $x + y = x'm + y'm = (x'+y')m \in \langle m \rangle$ pour $x',\ y' \in \mathbb{N}$ et $ax = a(x'm) = (ax')m = (x'm)a = xa \in \langle m \rangle$. Si $m = 0$, alors $\langle m \rangle = \{0\}$ et posons $Q = \mathbb{N}$. Ainsi, $\{q + 0\} = \{q\}$ et c'est une partition de $\mathbb{N}$. Sinon, posons $Q = \{0,\ 1,\ \ldots,\ m-1\}$. Alors, $\{q_1 + n \cdot m\} \cap \{q_2 + n' \cdot m\} = \varnothing$ et il s'agit aussi d'une partition de $\mathbb{N}$.

Commençons par illustrer le lien entre le semi-anneau S et l'ensemble Q lorsqu'il existe un Q-idéal.

Lemme 4.9. *Soit I un Q-idéal dans le semi-anneau S. Alors, si $x \in S$, il existe un unique $q \in Q$ tel que $x \oplus I \subseteq q \oplus I$.*

Démonstration. Soit une partition $\{q \oplus I\}_{q \in Q}$, de sorte que pour tout $x \in S$, il existe un unique $q \in Q$ tel que $x \in q \oplus I$. Ainsi, il existe un $i_1 \in I$ tel que $x = q \oplus i_1$.

Ensuite, supposons que $y \in x \oplus I$. Alors, il existe un $i_2 \in I$ tel que $y = x \oplus i_2$. Mais alors $y = (q \oplus i_1) \oplus i_2 = q \oplus (i_1 \oplus i_2)$, ce qui implique que $y \in q \oplus I$. □

Remarque 4.10. Il s'ensuit que $q_1 \oplus I = q_2 \oplus I$ si et seulement si $q_1 = q_2$.

Définition 4.11. Soit $\{q \oplus I\}_{q \in Q}$ une partition d'un semi-anneau S, I un idéal de S et $q_1,\ q_2 \in Q$. Notons q_3 et q_4 respectivement les uniques éléments de Q tels que $(q_1 \oplus q_2) \oplus I \subseteq q_3 \oplus I$ et $(q_1 \odot q_2) \oplus I \subseteq q_4 \oplus I$. Définissons alors les opérations $+$ et $\cdot$ sur les éléments de la partition de la manière suivante :

a) $(q_1 \oplus I) + (q_2 \oplus I) = q_3 \oplus I$

b) $(q_1 \oplus I) \cdot (q_2 \oplus I) = q_4 \oplus I$.

Notation 4.12. Notons $\{q \oplus I\}_{q \in Q} = S/_Q I$ afin de simplifier l'écriture.

Théorème 4.13. *Soit I un Q-idéal du semi-anneau S. Alors, $(S/_Q I,\ +\ ,\ \cdot)$ est un semi-anneau ayant un zéro et un plus petit élément.*

Démonstration. D'abord, vérifions la commutativité de l'addition. Soit $q_1,\ q_2 \in Q$. Nous savons que :

$$(q_1 \oplus I) + (q_2 \oplus I) = (q_3 \oplus I)$$

où q_3 est l'unique élément de Q tel que $(q_1 \oplus q_2) \oplus I \subseteq q_3 \oplus I$. Or, $(q_2 \oplus q_1) \oplus I \subseteq q_3 \oplus I$ et donc

$$(q_1 \oplus I) + (q_2 \oplus I) = (q_3 \oplus I) = (q_2 \oplus I) + (q_1 \oplus I)\,.$$

Ensuite, vérifions l'associativité de l'addition et de la multiplication. Soit q_1, q_2, $q_3 \in Q$. Nous avons

$$((q_1 \oplus I) + (q_2 \oplus I)) + (q_3 \oplus I) = (q_4 \oplus I) + (q_3 \oplus I)\,,$$

où q_4 est tel que $(q_1 \oplus q_2) \oplus I \subseteq q_4 \oplus I$. Comme il existe aussi q_5 tel que $(q_4 \oplus q_3) \oplus I \subseteq q_5 \oplus I$ et alors $(q_1 \oplus q_2 \oplus q_3) \oplus I \subseteq q_5 \oplus I$,

$$((q_1 \oplus I) + (q_2 \oplus I)) + (q_3 \oplus I) = q_5 \oplus I.$$

De plus,

$$(q_1 \oplus I) + ((q_2 \oplus I) + (q_3 \oplus I)) = (q_1 \oplus I) + (q_6 \oplus I)\,,$$

où q_6 est tel que $(q_2 \oplus q_3) \oplus I \subseteq q_6 \oplus I$. Donc, il existe q_7 tel que $(q_1 \oplus q_6) \oplus I \subseteq q_7 \oplus I$ et alors $(q_1 \oplus q_2 \oplus q_3) \oplus I \subseteq q_7 \oplus I$. En vertu du lemme 4.9 et de la remarque 4.10, nous savons que $q_5 = q_7$ et ainsi,

$$((q_1 \oplus I) + (q_2 \oplus I)) + (q_3 \oplus I) = (q_1 \oplus I) + ((q_2 \oplus I) + (q_3 \oplus I))\,.$$

L'associativité de la multiplication est prouvée de manière similaire.

Il faut aussi vérifier la distributivité.

$$(q_1 \oplus I) \cdot ((q_2 \oplus I) + (q_3 \oplus I)) = (q_1 \oplus I) \cdot (q_4 \oplus I)\,,$$

où q_4 est tel que $(q_2 \oplus q_3) \oplus I \subseteq q_4 \oplus I$. Comme il existe aussi q_5 tel que $(q_1 \odot q_4) \oplus I \subseteq q_5 \oplus I$ et $(q_1 \odot q_2 \oplus q_1 \odot q_3) \oplus I \subseteq q_5 \oplus I$,

$$(q_1 \oplus I) \cdot ((q_2 \oplus I) + (q_3 \oplus I)) = (q_5 \oplus I)$$

et ainsi,

$$(q_5 \oplus I) = ((q_1 \oplus I) \cdot (q_2 \oplus I)) + ((q_1 \oplus I) \cdot (q_3 \oplus I))\,,$$

d'où le résultat. Avec un raisonnement semblable, nous prouvons la distributivité à droite.

Il reste à prouver l'existence d'un zéro et d'un plus petit élément. Construisons la fonction ϕ définie comme suit. Pour $x \in S$ soit $q \in Q$ l'unique élément tel que $x \oplus I \subseteq q \oplus I$. Posons alors $\phi(x) = q \oplus I$. C'est un homomorphisme. Soit $0 \in S$ et $\phi(0) = q^* \oplus I$. Montrons que $q^* \oplus I$ est le zéro et le plus petit élément. Nous savons que $x \odot 0 = 0$ avec $\phi(x) = q \oplus I$. Donc

$$(q \oplus I) \cdot (q^* \oplus I) = \phi(x) \cdot \phi(0) = \phi(x \odot 0) = \phi(0) = q^* \oplus I.$$

De même, nous obtenons que $(q^* \oplus I) \cdot (q \oplus I) = q^* \oplus I$. De manière similaire, nous savons que $x \oplus 0 = x$, ce qui implique que

$$q \oplus I = \phi(x) = \phi(x \oplus 0) = \phi(x) + \phi(0) = (q \oplus I) + (q^* \oplus I),$$

d'où le résultat. □

Lemme 4.14. *Soit S un semi-anneau et $I \lhd S$. Si I est un Q-idéal et un Q'-idéal, alors $S/_Q I \cong S/_{Q'} I$.*

Démonstration. Soit $q \in Q \subseteq S$ et $q' \in Q'$ l'unique élément tel que $q \oplus I \subseteq q' \oplus I$. Construisons la fonction

$$\begin{array}{rccc} f: & S/_Q I & \longrightarrow & S/_{Q'} I \\ & q \oplus I & \longmapsto & q' \oplus I \end{array}$$

Nous voulons prouver qu'il s'agit d'un isomorphisme. Tout d'abord, montrons que f est un homomorphisme. Soit q_1, $q_2 \in Q$. Alors, il existe un unique $q_3 \in Q$ tel que $(q_1 \oplus q_2) \oplus I \subseteq q_3 \oplus I$. Soit q_1', q_2', $q_3' \in Q'$ tel que $f(q_1 \oplus I) = q_1' \oplus I$, $f(q_2 \oplus I) = q_2' \oplus I$ et $f(q_3 \oplus I) = q_3' \oplus I$. Ainsi, nous avons $(q_1 \oplus q_2) \oplus I \subseteq q_3' \oplus I$ et donc, $q_1' \oplus q_2' \oplus I \subseteq q_3' \oplus I$, ce qui implique

$$\begin{aligned} f\left((q_1 \oplus I) + (q_2 \oplus I)\right) &= f\left(q_3 \oplus I\right) \\ &= q_3' \oplus I \\ &= (q_1' \oplus I) + (q_2' \oplus I) \\ &= f\left(q_1 \oplus I\right) + f\left(q_2 \oplus I\right). \end{aligned}$$

Il en va de même pour la multiplication.

Il reste donc à montrer que f est bijective. Soit q_1, $q_2 \in Q$ et q_1', $q_2' \in Q'$ tels que $q_1' \oplus I = f(q_1 \oplus I) = f(q_2 \oplus I) = q_2' \oplus I$. Alors, $q_1' = q_2'$ et en vertu de la remarque 4.10, nous savons que $q_1 = q_2$, donc f est injective.

Prouvons à présent que f est aussi surjective. Soit $q' \in Q'$. Comme $S/_{Q'} I$ est une partition de S, il existe $x \in S$ tel que $x \in q' \oplus I$. Alors, il existe $i_1 \in I$ tel que $x \oplus i_1 = q'$, mais il existe aussi $q \in Q$ tel que $x \in q \oplus I$, ce qui implique qu'il existe $i_2 \in I$ tel que $x \oplus i_2 = q$. Il en découle que $x \oplus i_2 \oplus i_1 \oplus I = q \oplus I \subseteq q' \oplus I$. Par conséquent, f est un homomorphisme bijectif et donc un isomorphisme. □

Lemme 4.15. *Soit S et S' deux semi-anneaux, I un Q-idéal dans S et un homomorphisme $f : S \longrightarrow S'$.*

a) Soit $p : S \longrightarrow S/_Q I : x \mapsto q \oplus I$ où q est l'unique élément tel que $x \oplus I \subseteq q \oplus I$. Alors, p est un homomorphisme appelé la projection canonique.

*b) Soit $j : \mathrm{Im} f \longrightarrow S' : x \mapsto x$. Alors, cette application est un homomorphisme appelé l'*inclusion.

Démonstration.

a) Soit x, $y \in S$ et q, q_1, $q_2 \in Q$ tels que $p(x \oplus y) = q \oplus I$, $p(x) = q_1 \oplus I$, $p(y) = q_2 \oplus I$. Alors, nous avons $(x \oplus y) \oplus I \subseteq q \oplus I$ et donc $p(x \oplus y) = q \oplus I = (q_1 \oplus I) + (q_2 \oplus I) = p(x) + p(y)$. De la même manière, avec $q \in Q$ tel que $p(x \odot y) = q \oplus I$, nous savons que $p(x \odot y) = p(x) \cdot p(y)$. Ainsi, la projection est un homomorphisme.

b) Soit x', $y' \in \mathrm{Im}f$. Alors, il existe x, $y \in S$ tels que $x' = f(x)$ et $y' = f(y)$. Ainsi, nous avons que $j(x' \oplus' y') = j(f(x) \oplus' f(y)) = j(f(x \oplus y)) = f(x \oplus y) = f(x) \oplus' f(y) = j(x') \oplus' j(y')$ et de la même manière $j(x' \odot' y') = j(x') \odot' j(y')$. Ainsi, l'inclusion est un homomorphisme.

□

Lemme 4.16. *Soit* $\mathrm{Im}f$ *l'image d'un homomorphisme de semi-anneaux* $f : S \longrightarrow S'$. *Alors,* $\mathrm{Im}f$ *est un semi-anneau pour les mêmes opérations que celles définies dans* S'.

Démonstration. Prouvons d'abord la commutativité de l'addition. Soit $f(x)$, $f(y) \in \mathrm{Im}f$. Alors, nous savons que $f(x) \oplus' f(y) = f(x \oplus y) = f(y \oplus x) = f(y) \oplus' f(x)$. De la même manière, nous obtenons l'associativité de l'addition et de la multiplication ainsi que la distributivité à gauche et à droite. Il y a aussi un zéro, car $f(x) \oplus' f(0) = f(x \oplus 0) = f(x)$ et un plus petit élément, car $f(x) \odot' f(0) = f(x \odot 0) = f(0)$. □

Définition 4.17. Soit $f : S \longrightarrow S'$ un homomorphisme de semi-anneaux. La fonction f est dite *maximale* si pour tout élément a de l'image de f, il existe un élément c_a de sa préimage $f^{-1}(a) = \{x \mid f(x) = a\}$ tel que $x \oplus \mathrm{Ker}f \subseteq c_a \oplus \mathrm{Ker}f$ pour tout $x \in f^{-1}(a)$.

Remarque 4.18. Dans les travaux de Allen [All69], la définition d'un homomorphisme maximal requiert la surjectivité de l'application. Nous avons généralisé les résultats qui suivent pour qu'ils s'appliquent à tous les homomorphismes de semi-anneaux. De plus, remarquons que l'élément c_a n'est pas nécessairement unique.

Exemple 4.19.

a) Soit $S = (\mathbb{N},\ \max,\ \min)$. Montrons qu'il s'agit d'un semi-anneau. D'abord, max est commutatif et les deux opérations sont associatives, car pour tous $a, b, c \in \mathbb{N}$, nous avons $\max(a,\ \max(b, c)) = \max(a, b, c) = \max(\max(a, b), c)$ et $\min(a,\ \min(b,\ c)) = \min(a,\ b,\ c) = \min(\min(a,\ b),\ c)$. Ensuite, il est facile de vérifier que la distributivité est respectée en étudiant chacun des cas possibles : $a \leq b \leq c$, $a \leq c \leq b$, $b \leq a \leq c$, $b \leq c \leq a$, $c \leq a \leq b$ et $c \leq b \leq a$. Enfin, c'est un semi-anneau avec un zéro et un plus petit élément. En effet $\min(a,\ 0) = 0 = \min(0,\ a)$ et $\max(a,\ 0) = a$ pour tout $a \in \mathbb{N}$. Il s'ensuit que c'est un semi-anneau bien ordonné, c'est-à-dire que toute partie non vide possède un plus petit élément.

   De façon similaire, nous obtenons que $S' = (\{0,\ 1\},\ \max,\ \min)$ est un semi-anneau. Soit l'application $f : \mathbb{N} \to \{0,\ 1\}$ telle que

$$f = \begin{cases} 0 & \text{si } x \leq 5 \\ 1 & \text{si } x > 5 \end{cases}$$

où $x \in \mathbb{N}$. Prouvons que f est un homomorphisme. Soit x, $y \in \mathbb{N}$. Alors, $f(\max(x, y)) = \max(f(x), f(y))$ et $f(\min(x, y)) = \min(f(x), f(y))$.

Vérifions si f est maximal. Prenons $y \in f^{-1}(1)$, donc $f(y) = 1$ ce qui implique $y > 5$. Nous avons ainsi $\max_{k \in \mathrm{Ker} f}(y, k) = y$ et alors, il n'existe pas de $c \in f^{-1}(1)$ tel que $\max_{k \in \mathrm{Ker} f}(y, k) \subseteq \max_{k \in \mathrm{Ker} f}(c, k)$ pour tout $y \in f^{-1}(1)$. Il en découle que f n'est pas maximal.

b) Soit le semi-anneau $(\mathbb{N}, +, \cdot)$ et $\langle m \rangle = \{n \cdot m \mid n \in \mathbb{N}\}$ un Q-idéal de $\mathbb{N}$. Soit $m > 0$ et $\mathbb{N}/\langle m \rangle = \{a + \langle m \rangle \mid a \in \mathbb{N}\}$ un semi-anneau en vertu du théorème 4.13. Nous savons aussi que $x \in \mathbb{N}$ s'écrit de manière unique tel que $x = qm + r$ où q, $r \in \mathbb{N}$ et $0 \leq r < m$. Alors, posons

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N}/\langle m \rangle \\ & x & \longmapsto & r + \langle m \rangle \end{array}$$

où r est tel que défini plus haut. Nous prétendons que c'est un homomorphisme maximal.

Commençons par montrer qu'il s'agit bien d'un homomorphisme. Pour l'addition, on nous avons que

$$f(x + y) = f((qm + r) + (q'm + r')) = f((q + q')m + (r + r'))$$

ce qui donne deux cas possibles. Si $r + r' < m$, alors $f(x+y) = r + r' + \langle m \rangle = f(x) + f(y)$. Sinon, nous avons que $m \leq r + r' < 2m$ et ainsi, il existe $0 \leq r'' < m$ tel que $r + r' = m + r''$. Alors, $f(x + y) = f((q + q' + 1) + r'') = r'' + \langle m \rangle = f(x) + f(y)$. Pour la multiplication, il suffit de suivre un raisonnement similaire.

Il reste à montrer que f est maximal. Mais $\mathrm{Im} f = \mathbb{N}/\langle m \rangle$, donc f est surjective et $\mathrm{Ker} f = \langle m \rangle$. Soit un élément $a + \langle m \rangle \in \mathbb{N}/\langle m \rangle$ tel que $f(a) = a + \langle m \rangle$. Prenons un élément de la préimage de $a + \langle m \rangle$, disons y. Mais cela implique que $f(y) = f(qm + a) = a + \langle m \rangle$. Il en découle que

$$y + \mathrm{Ker} f = qm + a + \langle m \rangle = a + \langle m \rangle = a + \mathrm{Ker} f$$

et, par conséquent, $y + \mathrm{Ker} f \subseteq a + \mathrm{Ker} f$. Ainsi, f est maximal.

Lemme 4.20. *Soit $f : S \longrightarrow S'$ un homomorphisme maximal de semi-anneaux. Alors,* $\mathrm{Ker} f$ *est un Q-idéal avec $Q = \{c_a\}_{a \in \mathrm{Im} f}$*

Démonstration. Nous savons que $\mathrm{Ker} f$ est un idéal de S. Il reste donc à montrer que $\{c_a \oplus \mathrm{Ker} f\}_{c_a \in Q}$ donne une partition de S.

Supposons que c_a, $c_b \in Q$ distincts, c'est-à-dire que $a \neq b$. Si $(c_a \oplus \mathrm{Ker} f) \cap (c_b \oplus \mathrm{Ker} f) \neq \varnothing$, alors il existe k, $k' \in \mathrm{Ker} f$ tel que $c_a \oplus k = c_b \oplus k'$.

Or, $a = f(c_a) \oplus' f(k) = f(c_a \oplus k) = f(c_b \oplus k') = f(c_b) \oplus' f(k') = b$, ce qui contredit l'hypothèse de départ. Donc, il s'agit bien une partition et $\mathrm{Ker} f$ est un Q-idéal. □

Lemme 4.21. *Soit $f : S \longrightarrow S'$ un homomorphisme maximal de semi-anneaux et $Q = \{c_a\}_{a \in \mathrm{Im}f}$. Si c_a, c_b, $c_d \in Q$, alors nous avons que :*

a) Si $c_a \oplus c_b \oplus \mathrm{Ker}f \subseteq c_d \oplus \mathrm{Ker}f$, alors $a \oplus' b = d$.

b) Si $c_a \odot c_b \oplus \mathrm{Ker}f \subseteq c_d \oplus \mathrm{Ker}f$, alors $a \odot' b = d$.

Démonstration. Soit $c_a \oplus c_b \oplus \mathrm{Ker}f \subseteq c_d \oplus \mathrm{Ker}f$. Alors, nous avons que $c_a \oplus c_b \in c_d \oplus \mathrm{Ker}f$ et donc, il existe $k \in \mathrm{Ker}f$ tel que $c_a \oplus c_b = c_d \oplus k$. Ainsi, $a \oplus' b = f(c_a) \oplus' f(c_b) = f(c_a \oplus c_b) = f(c_d \oplus k) = f(c_d) \oplus' f(k) = d$.

De même, nous obtenons que $a \odot' b = d$. □

Théorème 4.22. *Soit $f : S \longrightarrow S'$ un homomorphisme maximal de semi-anneaux, $p : S \longrightarrow S/_Q\mathrm{Ker}f$ la projection canonique et $j : \mathrm{Im}f \longrightarrow S'$ l'inclusion. Alors, il existe un unique homomorphisme $f' : S/_Q\mathrm{Ker}f \longrightarrow \mathrm{Im}f$ tel que $f = j \circ f' \circ p$. En outre, f' est un isomorphisme.*

Démonstration. Pour l'unicité, nous supposons que f' existe telle que définie plus haut, ce qui donne $f'(c_a \oplus \mathrm{Ker}f) = f'(p(c_a)) = j(f'(p(c_a))) = f(c_a) = a$. Il faut prouver que cette dernière formule définit f' sans ambiguïté. Soit $x \oplus \mathrm{Ker}f = y \oplus \mathrm{Ker}f$. Il existe alors un $k \in \mathrm{Ker}f$ tel que $x = y \oplus k$ et $f(x) = f(y \oplus k) = f(y) \oplus' f(k) = f(y)$. Il est possible d'en déduire que $f'(x \oplus \mathrm{Ker}f) = f(x) = f(y \oplus k) = f'(y \oplus k \oplus \mathrm{Ker}f) = f'(y \oplus \mathrm{Ker}f)$, d'où l'existence.

Il reste à montrer qu'il s'agit d'un isomorphisme. Montrons d'abord que f' est bijective. Comme f est maximal, $f'(c_a \oplus \mathrm{Ker}f) = f'(c_b \oplus \mathrm{Ker}f)$ implique que $a = b$, d'où l'injectivité. De plus, soit $a \in \mathrm{Im}f$. Alors, $f'(c_a \oplus \mathrm{Ker}f) = a$ et $c_a \oplus \mathrm{Ker}f \in S/_Q\mathrm{Ker}f$. Enfin, c_a existe en vertu de la maximalité de f. Donc, f' est surjective et par le fait même bijective. Il reste à montrer que f' est un homomorphisme. D'abord pour l'addition, $f'((c_a \oplus \mathrm{Ker}f) + (c_b \oplus \mathrm{Ker}f)) = f'(c_d \oplus \mathrm{Ker}f) = d$ avec $c_a \oplus c_b \oplus \mathrm{Ker}f \subseteq c_d \oplus \mathrm{Ker}f$. En vertu du lemme précédent, nous savons que $d = a \oplus' b = f'(c_a \oplus \mathrm{Ker}f) \oplus' f'(c_b \oplus \mathrm{Ker}f)$. Il suffit de procéder de la même manière pour la multiplication. □

Observons maintenant les quotients d'un semi-corps T.

Lemme 4.23. *Soit T un semi-corps. Alors, ses quotients sont, à isomorphisme près, $\{0\}$ et T.*

Démonstration. Selon le théorème 4.6, les seuls idéaux d'un semi-corps T sont $\{0\}$ et T. Soit $\{0\} \lhd T$. Alors, $\{0\}$ est un Q-idéal avec $Q = T$. Le quotient $T/_T\{0\}$ est égal, par définition, à $\{t \oplus \{0\}\}_{t \in T} = \{\{t\}\}_{t \in T} \cong T$. Soit $T \lhd T$. Alors, $Q = \{0\}$ pour que T soit un Q-idéal et son quotient est de la forme $T/_{\{0\}}T$. Mais alors, $T/_{\{0\}}T = \{0 \oplus T\} = \{T\} \cong \{0\}$. □

5 Algèbres de Boole et treillis

Tel que mentionné dans l'exemple 2.2, un semi-anneau peut également être une algèbre de Boole. Définissons donc cette structure selon [BML08] et intéressons-nous aux similitudes avec les semi-anneaux.

Définition 5.1. Une *algèbre de Boole* est un ensemble B muni de deux opérations binaires $\vee$ et $\wedge$ qui sont idempotentes, commutatives, associatives, absorbantes entre elles ($a \vee (a \wedge b) = a$ et $a \wedge (a \vee b) = a$) et mutuellement distributives. De plus, il existe O et $I \in B$ tels que $O \vee a = a$, $O \wedge a = O$, $I \vee a = I$ et $I \wedge a$. Enfin, l'ensemble possède une opération unaire $a \mapsto a'$ telle que $a \vee a' = I$ et $a \wedge a' = O$.

Déterminons les propriétés nécessaires aux semi-anneaux pour avoir une algèbre de Boole.

Théorème 5.2. *Soit un triplet $(S, \oplus, \odot)$. Alors, S est une algèbre de Boole si et seulement si $(S, \oplus, \odot)$ et $(S, \odot, \oplus)$ sont des semi-corps idempotents, absorbants, commutatifs, avec un plus petit élément qui est le zéro ainsi qu'un plus grand élément qui est l'identité multiplicative.*

Démonstration. Soit S une algèbre de Boole. En vertu de sa définition, l'opération $\oplus$ est commutative et associative, alors que $\odot$ est associative. De plus, nous savons que $\odot$ se distribue sur $\oplus$. Par conséquent, $(S, \oplus, \odot)$ est un semi-anneau. De manière analogue, il s'ensuit que $(S, \odot, \oplus)$ est aussi un semi-anneau.

En vertu de la définition 5.1 et des propriétés des semi-anneaux dans la section 3, nous savons que $(S, \oplus, \odot)$ est un semi-anneau idempotent, absorbant, commutatif, possédant un plus grand élément qui est l'identité multiplicative I de même qu'un plus petit élément qui est le zéro O. De plus, a' est l'inverse de a pour tout $a \in S$, donc S est un semi-corps. Il en va de même pour $(S, \odot, \oplus)$.

Réciproquement, soit $(S, \oplus, \odot)$ et $(S, \odot, \oplus)$ deux semi-corps idempotents, absorbants, commutatifs, avec un plus petit élément et zéro et un plus grand élément et identité multiplicative. Alors, les deux opérations sont idempotentes, commutatives, associatives, absorbantes entre elles et mutuellement distributives. De plus, il existe un plus petit élément qui est un zéro et un plus grand élément qui est une identité multiplicative et il existe un inverse, donc une opération unaire. Ainsi, nous avons vérifié tous les axiomes de la définition 5.1 et S est une algèbre de Boole. □

Exemple 5.3. Soit $n \in \mathbb{N}$ tel que $n \neq k^2$ pour tout $k \in \mathbb{N}$. Considérons $B = \{m \mid m|n\}$. Prenons comme opérations le plus grand commun diviseur (pgcd) et le plus petit commun multiple (ppcm). Nous prétendons qu'il s'agit d'une algèbre de Boole. Montrons que B vérifie bien tous les axiomes.

Par définition, le pgcd et le ppcm sont idempotents. Il est aussi clair que les deux opérations sont commutatives. Prouvons qu'elles sont également associatives, c'est-à-dire pour tous a, b, $c \in B$, nous avons ,

$$\text{pgcd}(a,\ \text{pgcd}(b,\ c)) = \text{pgcd}(\text{pgcd}(a,\ b),\ c)$$

et

$$\text{ppcm}(a,\ \text{ppcm}(b,\ c)) = \text{ppcm}(\text{ppcm}(a,\ b),\ c).$$

En effet, posons $e = \text{pgcd}(a,\ \text{pgcd}(b,\ c))$ et $f = \text{pgcd}(\text{pgcd}(a,\ b),\ c)$. Il s'ensuit que $e \mid a$ et $e \mid \text{pgcd}(b,\ c)$, ce qui implique que $e \mid a$, $e \mid b$ et $e \mid c$. Ainsi,

$e \mid \text{pgcd}(a,\, b)$ et $e \mid c$, d'où $e \mid f$. De la même façon, il est possible de montrer que $f \mid e$, donc $e = f$. L'associativité du ppcm se prouve de manière similaire.

L'absorption est vérifiée, car $\text{pgcd}(a,\ \text{ppcm}(a,\, b)) = \text{pgcd}(a,\, ka) = a$ pour un $k \in B$ tel que $\text{ppcm}(a,\, b) = ka$. Nous avons $\text{ppcm}(a,\ \text{pgcd}(a,\, b)) = a$ de la même manière.

Montrons que le pgcd est distribué sur le ppcm et vice versa. Nous savons que le pgcd est distributif sur lui-même. Ainsi, nous avons que

$$\begin{aligned}\text{pgcd}(a,\, c)\,\text{pgcd}(b,\, c)\,\text{pgcd}(a,\, b) &= \text{pgcd}(aab,\, abb,\, aac,\, abc,\, acc,\, bbc,\, bcc)\\ &= \text{pgcd}(a,\, b,\, c)\,\text{pgcd}(ab,\, ac,\, bc)\\ &= \text{pgcd}(a,\, b,\, c)\frac{abc}{\text{ppcm}(a,\, b,\, c)},\end{aligned}$$

d'où

$$\frac{abc}{\text{pgcd}(a,\, b)\,\text{ppcm}(a,\, b,\, c)} = \frac{\text{pgcd}(a,\, c)\,\text{pgcd}(b,\, c)}{\text{pgcd}(a,\, b,\, c)}.$$

Ainsi,

$$\frac{\text{ppcm}(a,\, b)c}{\text{ppcm}(\text{ppcm}(a,\, b),\, c)} = \frac{\text{pgcd}(a,\, c)\,\text{pgcd}(b,\, c)}{\text{pgcd}(\text{pgcd}(a,\, c),\ \text{pgcd}(b,\, c))},$$

ce qui donne

$$\text{pgcd}(\text{ppcm}(a,\, b),\, c) = \text{ppcm}(\text{pgcd}(a,\, c),\ \text{pgcd}(b,\, c)).$$

De même, le ppcm se distribue sur le pgcd.

Il reste à trouver O et I de même que l'opération unaire. Remarquons que pour tout $a \in B$, nous avons que $\text{pgcd}(a,\, n) = a$ et $\text{ppcm}(a,\, n) = n$, donc $I = n$. Aussi, $\text{pgcd}(a,\, 1) = 1$ et $\text{ppcm}(a,\, 1) = a$ d'où $O = 1$. Enfin, posons a' tel que $aa' = n$. Alors, $\text{pgcd}(a,\, a') = n$ et $\text{ppcm}(a,\, a') = 1$.

Étudions à présent une structure semblable aux algèbres de Boole, mais possédant moins d'axiomes de définition. Plus précisément, cette structure ne possède pas d'éléments O et I, ni d'opération unaire tels que décrits à la définition 5.1 et ses opérations binaires ne sont pas nécessairement mutuellement distributives.

Définition 5.4. Un *treillis* est un ensemble L possédant deux opérations $\vee$ et $\wedge$ qui sont idempotentes, commutatives, associatives et absorbantes. Si de plus les deux opérations sont mutuellement distributives, L est appelé un *treillis distributif*.

Exemple 5.5. Soit G un groupe quelconque et Σ l'ensemble de tous les sous-groupes de G. Posons pour tous $H,\, K \in \Sigma$ les opérations $H \wedge K = H \cap K$ et $H \vee K = \langle H,\, K\rangle$ où $\langle H,\, K\rangle$ est le plus petit sous-groupe contenant H et K. Montrons qu'il s'agit d'un treillis.

Les opérations $\vee$ et $\wedge$ sont trivialement idempotentes et commutatives. Il reste à montrer qu'elles sont associatives et absorbantes. Or, $\wedge = \cap$ est associative et pour tous $H,\, K,\, M \in \Sigma$, nous savons que $\langle H,\, \langle K,\, M\rangle\rangle = \langle H,\, K,\, M\rangle =$

$\langle\langle H,\, K\rangle,\, M\rangle$. En outre, nous trouvons que $H \cap \langle H,\, K\rangle = H = \langle H,\, H \cap K\rangle$, et ainsi, Σ est un treillis. Toutefois, il n'est généralement pas distributif.

Par exemple, soit $G = \mathbb{Z} \oplus \mathbb{Z}$. Alors, Σ contient les sous-groupes $(1,\, 1)\,\mathbb{Z}$, $(0,\, 1)\,\mathbb{Z}$, $(1,\, 0)\,\mathbb{Z}$ et $(0,\, 0)\,\mathbb{Z}$. Ainsi, nous avons

$$\begin{aligned}(1,\, 1)\,\mathbb{Z} \cap \langle (0,\, 1)\,\mathbb{Z},\ (1,\, 0)\,\mathbb{Z}\rangle &= (1,\, 1)\,\mathbb{Z} \cap \mathbb{Z} \oplus \mathbb{Z} \\ &= (1,\, 1)\,\mathbb{Z}.\end{aligned}$$

Par contre, nous savons que

$$\begin{aligned}\langle (1,\, 1)\,\mathbb{Z} \cap (0,\, 1)\,\mathbb{Z},\ (1,\, 1)\,\mathbb{Z} \cap (1,\, 0)\,\mathbb{Z}\rangle &= \langle (0,\, 0)\,\mathbb{Z},\ (0,\, 0)\,\mathbb{Z}\rangle \\ &= (0,\, 0)\,\mathbb{Z}.\end{aligned}$$

Puisqu'il n'y a pas égalité, la distributivité n'est pas respectée.

Comme pour les algèbres de Boole, cherchons des conditions nécessaires et suffisantes sur un semi-anneau pour qu'il soit aussi un treillis distributif.

Théorème 5.6. *Soit un triplet $(S,\ \oplus\,,\, \odot)$. Alors, S est un treillis distributif si et seulement si $(S,\ \oplus\,,\, \odot)$ et $(S,\ \odot\,,\, \oplus)$ sont tous deux des semi-anneaux idempotents, commutatifs et absorbants.*

Démonstration. Soit S un treillis distributif avec les opérations $\oplus$ et $\odot$. Comme nous savons que $\oplus$ est commutative et associative, que $\odot$ est associative et que les deux opérations sont mutuellement distributives, nous en déduisons que $(S,\ \oplus\,,\, \odot)$ est un semi-anneau.

En vertu de la définition 5.4 et des propriétés des semi-anneaux dans la section 3, S est un semi-anneau idempotent, commutatif et absorbant. De plus, le triplet $(S,\ \odot\,,\, \oplus)$ est aussi un semi-anneau idempotent, commutatif et absorbant.

Réciproquement, soit $(S,\ \oplus\,,\, \odot)$ et $(S,\ \odot\,,\, \oplus)$ deux semi-anneaux idempotents, commutatifs et absorbants. Alors, les deux opérations sont idempotentes, commutatives, associatives, absorbantes et mutuellement distributives. Ainsi, tous les axiomes de la définition 5.4 sont vérifiés, donc S est un treillis distributif. □

Exemple 5.7. Considérons le semi-anneau $(\mathbb{N},\ \max\,,\, \min)$. Prouvons qu'il s'agit aussi d'un treillis. Il est clair que min et max sont idempotentes, commutatives et associatives. Il reste donc à montrer que ces opérations sont aussi absorbantes.

Or, $\max(a,\ \min(a,\, b)) = a$ et $\min(a,\ \max(a,\, b)) = a$ pour tous $a,\, b \in \mathbb{N}$, donc l'absorption est vérifiée. Par conséquent $(\mathbb{N},\ \max\,,\, \min)$ est un treillis.

Il est aussi possible de montrer que c'est un treillis distributif, tel que dans l'exemple 4.19.

Références

[AD13] Ibrahim Assem et Grégoire Dupont : Friezes over semirings and tropicalizations. 2013.

[AL09] Ibrahim Assem et Pierre Yves Leduc : *Cours d'algèbre : groupes, anneaux, modules et corps*. Presses inter Polytechnique, 2009.

[All69] Paul J. Allen : A fundamental theorem of homomorphisms for semirings. *Proceedings of the American Mathematical Society*, 21(2):412–416, 1969.

[BG06] Stefano Bistarelli et Fabio Gadducci : Enhancing constraints manipulation in semiring-based formalisms. *In Proceedings of the 2006 Conference on ECAI 2006 : 17th European Conference on Artificial Intelligence August 29 – September 1, 2006, Riva Del Garda, Italy*, pages 63–67. IOS Press, 2006.

[BML08] Garrett Birkhoff et Saunders Mac Lane : *A Survey of Modern Algebra*. A K Peters, 4e édition, 2008.

[Ded96] Richard Dedekind : *Theory of algebraic integers*. Cambridge University Press, New York, 1996.

[FJZ08] Feng Feng, Young B. Jun et Xianzhong Zhao : Soft semirings. *Computers and Mathematics with Applications*, 56(10):2621–2628, 2008.

[KK10] Vítězslav Kala et Miroslav Korbelář : Congruence-simple subsemirings of Q. *Semigroup Forum*, 81(2):286–296, 2010.

[KS85] Werner Kuich et Arto Salomaa : *Semirings, automata and languages*, volume 5 de *Monographs on Theoretical Computer Science*. Springer-Verlag New York, Inc., 1985.

[RV04] Sergiu Rudeanu et Dragoş Vaida : Semirings in operations research and computer science : More algebra. *Fundam. Inf.*, 61(1):61–85, janvier 2004.

[Van39] Harry Schultz Vandiver : On some simple types of semi-rings. *American Mathematical Monthly*, 46:22–26, 1939.

[VC09] E. M. Vechtomov et A. V. Cheraneva : Semifields and their properties. *Journal of Mathematical Sciences*, 163(6):625–661, 2009.

Véronique Bazier-Matte
Département de mathématiques, Université de Sherbrooke
Courriel: Veronique.Bazier-Matte@USherbrooke.ca

Mélissa Barbe Marcoux
Département de mathématiques, Université de Sherbrooke
Courriel: Melissa.Barbe-Marcoux@USherbrooke.ca