Devoir Sur Table N°11 Bis

Structures Algébriques

31 Janvier 2019

Idéaux et blocs d'un anneau.

Dans tout le problème, A désigne un anneau non commutatif.

— On dit qu'une partie non vide I de A est un *idéal* de A si :
Pour tous x, y de I, pour tout a de A, l'élément $a(x-y)$ est dans I.

— On dit qu'une partie non vide B de A est un *bloc* de A si :
Pour tous x, y, z de B, pour tout a de A, l'élément $a(x-y)+z$ est dans B.

I. Généralités sur les idéaux

1. Vérifier que $\{0\}$ et A sont deux idéaux de A (idéaux *triviaux*).
Montrer qu'un idéal I de A est un sous-groupe de $(A,+)$. Préciser les idéaux de $\mathbb{Z}$.

2. Soit I un idéal de A. Montrer que $\forall\,(a,x)\in A\times I,\ ax\in I$.
Montrer que si I contient un élément inversible de A, alors $I=A$. Décrire les idéaux d'un corps.

3. Soient I et J deux idéaux de A. On pose $I+J=\{x+y,\ x\in I,\ y\in J\}$.
Montrer que $I\cap J$ et $I+J$ sont des idéaux de A.

4. Soit I un idéal de A. On note $\sqrt{I}=\{x\in A,\ \exists n\in\mathbb{N}^*,\ x^n\in I\}$.

   (a) Montrer que $\sqrt{I}$ est un idéal de A qui contient I. Préciser $\sqrt{A}$ et interpréter $\sqrt{\{0\}}$.

   (b) Pour tous idéaux I, J de A, montrer que $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$ et $\sqrt{\sqrt{I}}=\sqrt{I}$.

   (c) Quels sont les idéaux de $\mathbb{Z}$ tels que $\sqrt{I}=I$? Simplifier $\sqrt{360\mathbb{Z}}$.

II. Généralités sur les blocs

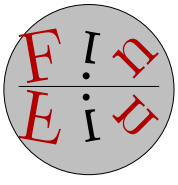
1. Montrer que tout idéal est un bloc. Vérifier que tout singleton est un bloc.
   Montrer qu'un bloc est un idéal si et seulement s'il contient 0.
2. Soit B un bloc de A, et soit t un élément de A.
   Montrer que l'ensemble noté $B+t$ et égal à $\{b+t,\ b\in B\}$ est un bloc de A.
3. Montrer qu'une partie B de A est un bloc si et seulement s'il existe un élément t de A et un idéal I de A tels que $B=I+t$ (voir notations précédentes.)
   Vérifier alors qu'à B fixé l'idéal I est unique, et que $B=I+t\Leftrightarrow t\in B$.
   On dit que l'idéal I est la *direction* du bloc B. Vérifier que $I+t=I+t'\Leftrightarrow t'-t\in I$.
   Quels sont les blocs de l'anneau $\mathbb{Z}$?
4. Montrer que si B et C sont des blocs il en est de même de $B+C$.
   A quelle condition peut-on dire que $B\cap C$ est un bloc ?
   Montrer sur un exemple qu'on ne peut pas généraliser aux blocs le résultat de $(I4a)$.
5. Soient $f:A\to A'$ un morphisme d'anneaux commutatifs.
   Soit B' un bloc de A'. Montrer que si $B=\overset{-1}{f}(B')$ est non vide, c'est un bloc de A.
   Montrer que pour tout b de $\operatorname{Im} f$, l'ensemble $\{x\in A,\ f(x)=b\}$ est un bloc de A.

III. Relation d'équivalence associée à un idéal

Soit I un idéal de A. On définit une relation sur A par : $a\,\mathcal{R}\,b\Leftrightarrow b-a\in I$.

Soit $\mathcal{B}_I$ l'ensemble des blocs de A de direction I, c'est-à-dire des $I_t=t+I$, avec t dans A.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur A.
2. Prouver que les classes d'équivalence de A pour $\mathcal{R}$ sont les I_t, avec t dans A.
3. Montrer que l'ensemble $\mathcal{B}_I$ est muni d'une structure d'anneau commutatif quand on le munit des opérations suivantes (dont on justifiera qu'elles ont un sens) : $\forall\,(t,u)\in A^2,\ I_t+I_u=I_{t+u}$ et $I_tI_u=I_{tu}$.
4. Montrer que $\mathcal{B}_I$ est un corps si et seulement I est inclus dans exactement deux idéaux de A (I et lui-même).



I. Généralités sur les idéaux

1. Il est vraiment évident que $\{0\}$ et A sont deux idéaux de A...

   Soit I un idéal de A. Tout d'abord I est non vide, et si dans la définition on pose $a = 1$, on trouve : $\forall\,(x,y) \in I,\ x - y \in I$, ce qui prouve que I est un sous-groupe de $(A,+)$.

   Tout idéal de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$ donc un $n\mathbb{Z}$, avec n dans $\mathbb{N}$.
   Réciproquement, soit n dans $\mathbb{N}$. Soient a dans $\mathbb{Z}$ et x, y dans $n\mathbb{Z}$.
   L'entier n divise x et y donc il divise $a(x-y)$.
   Ainsi $a(x-y)$ est encore dans $n\mathbb{Z}$, ce qui prouve que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

   Conclusion : les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour tout n de $\mathbb{N}$.

2. Dans la définition de l'idéal I, on pose $y = 0$ (possible car tout idéal est un sous-groupe de $(A,+)$.)
   On trouve effectivement : $\forall\,(a,x) \in A \times I,\ ax \in I$.

   Soit I un idéal de A contenant un élément inversible a de A.
   Tout y de A peut s'écrire $y = ax$ avec $x = a^{-1}y$.
   Puisque a est dans I, il est en donc de même de x. Ainsi $A \subset I$, donc $I = A$.

   Soit I un idéal d'un corps K. Il est possible que I soit réduit à $\{0\}$.
   Sinon, I contient un élément non nul donc inversible de K. Il en résulte alors $I = K$.
   Conclusion : les deux seuls idéaux d'un corps sont ses idéaux triviaux.

3. Les ensembles $I \cap J$ et $I + J$ contiennent 0 donc sont non vides.

   Soit a dans A et soient x, y dans $I \cap J$. I et J sont des idéaux donc $a(x-y)$ est dans I et dans J, donc dans $I \cap J$. Ainsi $I \cap J$ est un idéal de A.

   Soit a dans A et soient x et y deux éléments de $I + J$.
   Il existe x', y' dans I et x'', y'' dans J tels que $x = x' + x''$ et $y = y' + y''$.
   On écrit $a(x-y) = a(x'-y') + a(x''-y'')$. Mais $a(x'-y') \in I$ et $a(x''-y'') \in J$.
   Ainsi $a(x-y)$ est dans $I + J$. Conclusion : $I + J$ est un idéal de A.

4. (a) Tout d'abord $\sqrt{I}$ contient I (si $x \in I$ alors $x^n \in I$ avec $n = 1$...).

   Soient x, y dans $\sqrt{I}$. Il existe $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$ tels que $x^m \in I$ et $y^n \in I$.

   A étant commutatif : $(a(x-y))^p = a^p \sum_{k=0}^{p} (-1)^k \binom{p}{k} x^{p-k} y^k$ pour tout $p \geqslant 1$.

   Pour montrer que $(a(x-y))^p \in I$, il suffit de le vérifier pour les $x^{p-k}y^k$ $(0 \leqslant k \leqslant p.)$
   Pour cela, on choisit $p = m + n - 1$. Si $k \geqslant n$ alors $y^k = y^n y^{k-n} \in I$ car $y^n \in I$.
   Si $k \leqslant n-1$, alors $p - k \geqslant m$ donc x^{p-k} est dans I.
   Dans tous les cas $x^{p-k}y^k \in I$, donc $(a(x-y))^p \in I$, ce qui prouve que $a(x-y) \in \sqrt{I}$.

   Tout cela fait que $\sqrt{I}$ est un idéal de A contenant I.

   Puisque $\sqrt{A}$ contient A, on a évidemment $\sqrt{A} = A$.

   Enfin $\sqrt{I} = \{x \in A,\ \exists\, n \geqslant 1,\ x^n = 0\}$.
   $\sqrt{I}$ est donc formé des élément nilpotents de A (0 compris.)

(b) Il est clair que l'inclusion $I \cap J \subset I$ implique $\sqrt{I \cap J} \subset \sqrt{I}$.
De même $\sqrt{I \cap J} \subset \sqrt{J}$ donc $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.
Soit x dans $\sqrt{I} \cap \sqrt{J}$. Il existe m et n dans $\mathbb{N}^*$ tels que $x^m \in I$ et $x^n \in J$.
Avec $p = \max(m, n)$ on a alors $x^p \in I \cap J$, ce qui prouve que x est dans $\sqrt{I \cap J}$.
Conclusion : on a l'égalité $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

On sait déjà que $\sqrt{\sqrt{I}}$ contient $\sqrt{I}$.
Soit x un élément de $\sqrt{\sqrt{I}}$. Il existe n dans $\mathbb{N}^*$ tel que $y = x^n$ soit dans $\sqrt{I}$.
Mais alors il existe m dans $\mathbb{N}^*$ tel que y^m soit dans I, avec $y^m = x^{mn}$.
On en déduit que x est un élément de $\sqrt{I}$. Ainsi $\sqrt{\sqrt{I}} = \sqrt{I}$.

(c) On sait que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec n dans $\mathbb{N}$.
Donnons-nous n dans $\mathbb{Z}$. L'appartenance de x à $n\mathbb{Z}$ signifie que n divise x.
Dire que $\sqrt{I} = I$, c'est dire qu'on a l'inclusion $\sqrt{I} \subset I$.
C'est donc dire que dès que n divise une puissance d'un entier x, alors n divise x.
Cela est si $n = 0$ et $n = 1$, ce qui donne déja les deux idéaux triviaux $0\mathbb{Z} = \{0\}$ et $1\mathbb{Z} = \mathbb{Z}$.
Pour tout $n \geqslant 2$, cela n'est vrai que si n est un produit d'entiers premiers distincts.
Conclusion : les idéaux I de $\mathbb{Z}$ tels que $\sqrt{I} = I$ sont $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$ et les $n\mathbb{Z}$ où l'entier n est un produit d'entiers premiers distincts.

On a $360 = 2^3 3^2 5$, qui est divisble par $2 \cdot 3 \cdot 5 = 30$, et on sait que $30\mathbb{Z} = \sqrt{30\mathbb{Z}}$.
Puisque 30 divise 360, on a $360\mathbb{Z} \subset 30\mathbb{Z}$ donc $30\mathbb{Z} = \sqrt{30\mathbb{Z}} \subset \sqrt{360\mathbb{Z}}$.
Réciproquement, si x est dans $\sqrt{360\mathbb{Z}}$, alors il existe $m \geqslant 1$ tel que $360 \mid x^n$.
Il en découle que $2, 3, 5$ divisent x^n donc divisent x, donc que 30 divise x.
Conclusion : on a l'égalité $\sqrt{360\mathbb{Z}} = 30\mathbb{Z}$.

II. Généralités sur les blocs

1. Soit I un idéal de A. Soit a un élément de A et x, y, z dans I.
Puisque I est un idéal, le produit $a(x - y)$ est un élément de I.
Enfin, I étant aussi un sous-groupe de $(A, +)$ l'élément $a(x - y) + z$ est encore dans I.
Conclusion : I est un bloc de A.

Un singleton $B = \{b\}$ de A est évidemment un bloc (si on revient à la définition, la seule possibilité pour l'élément $a(x - y) + z$ est b.)

Si un bloc B de A contient 0 alors c'est un idéal (dans la définition d'un bloc, poser $z = 0$, et on retrouve la définition d'un idéal.)
Réciproquement, si un bloc est un idéal, il est un sous-groupe de $(A, +)$ donc contient 0.
Conclusion : un bloc de A en est un idéal si et seulement s'il contient 0.

2. Tout d'abord, $B_t = B + t$ est non vide. Soient x, y, z dans $B + t$ et a un élément de A.
Il existe x', y', z' dans B tels que $x = x' + t$, $y = y' + t$ et $z = z' + t$.
Dans ces conditions, $a(x - y) + z = b + t$, avec $b = a(x' - y') + z'$.
Puisque B est un bloc, l'élément $b = a(x' - y') + z'$ est encore dans B.
Ainsi $a(x - y) + z = b + t$ est dans $B + t$, ce qui prouve que $B + t$ est un bloc de A.

3. Si I est un idéal, alors c'est un bloc, et $B = I + t$ est un bloc pour tout t de I.

   Réciproquement, soit B un bloc de A. Si on veut écrire $B = I + t$ où I un idéal et t un élément de A, alors t est nécessairement dans B (car I contient 0.)

   Donnons-nous un élément quelconque t de B.
   L'égalité $B = I + t$ définit $I = B - t = \{b - t,\ b \in B\}$. Puisque B est un bloc, $I = B - t$ en est un. D'autre part il contient 0 (choisir $b = t$) : c'est donc un idéal de A.

   Si on s'était donné t' plutôt que t dans B, on aurait obtenu l'idéal $I' = B - t'$.
   Mais si $x' = b - t'$ est dans I' (ici $b \in B$) alors $x' = (b + t - t') - t$ est dans $B - t = I$ (car $b + t - t'$ est dans B par définition d'un bloc.) Ainsi $I' \subset I$, puis $I' = I$ par symétrie.

   Conclusion :

   — B est un bloc de $A \Leftrightarrow$ il existe un idéal I de A et un élément t dans A tels que $B = I + t$.

   — L'idéal est unique à B fixé : $I = B - t = \{b - t,\ b \in B\}$, où t est quelconque dans B.

   — Les éléments t de A tels que $B = I + t$ sont exactement les éléments de B.

   Si $I + t = I + t'$ alors $I + t' - t = I$, donc $t' - t = 0 + t' - t$ est dans I. Réciproquement, si $t' - t$ est dans I, alors pour tout x de I, l'élément $x + t' = (x + t' - t) + t'$ est dans $I + t'$ donc $I + t \subset I + t'$ (par symétrie $I + t = I + t'$.)

   Puisqu'on sait que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec n dans $\mathbb{N}$, ce qui précède montre que les blocs de $\mathbb{Z}$ sont les $n\mathbb{Z} + r$ avec n dans $\mathbb{N}$ et r dans $\mathbb{Z}$.

   Avec $n = 0$, on trouve les singletons de $\mathbb{Z}$. Avec $n = 1$, on a toujours $n\mathbb{Z} + r = \mathbb{Z}$.

   Pour tout $n \geqslant 2$, on a $n\mathbb{Z} + r = \{nq + r,\ (q, r) \in \mathbb{Z}^2\}$. Dans cette écriture, on peut d'ailleurs limiter les valeurs de r à l'intervalle $\{0, \dots, r - 1\}$.

4. Soient B et C deux blocs de A. Soient t dans B et u dans C.
   On sait qu'il existe deux idéaux I et J tels que $B = I + t$ et $C = J + u$.
   On obtient alors $B + C = \{b + c,\ b \in B,\ c \in B\} = (I + t) + (J + u) = (I + J) + (t + u)$.
   On sait que $I + J$ est un idéal. Il en résulte que $B + C$ est un bloc.

   Remarquons que si B et C sont disjoints, alors $B \cap C$ n'est pas un bloc. Supposons au contraire qu'il existe un élément t, commun à B et à C.
   On sait alors qu'il existe deux idéaux I et J de A tels que $B = I + t$ et $C = J + t$.
   Alors : $x \in B \cap C \Leftrightarrow \begin{cases} x \in B \\ x \in C \end{cases} \Leftrightarrow \begin{cases} x - t \in I \\ x - t \in J \end{cases} \Leftrightarrow x - t \in I \cap J \Leftrightarrow x \in (I \cap J) + t.$
   Autrement dit, $B \cap C = (I \cap J) + t$, qui est un bloc car $I \cap J$ est un idéal.
   Conclusion : l'ensemble $B \cap C$ est un bloc de A si et seulement si $B \cap C$ est non vide.

   Considérons $B = 3\mathbb{Z} + 1 = \{3q + 1,\ q \in \mathbb{Z}\}$, qui est bien un bloc de l'anneau $\mathbb{Z}$.
   Les éléments de $B = 3\mathbb{Z} + 1$ sont évidemment dans $\sqrt{B}$. Ceux de $3\mathbb{Z}$ n'y sont pas (toute puissance d'un multiple de 3 est encore un multiple de 3.)
   Enfin les éléments de $3\mathbb{Z} + 2$ sont dans $\sqrt{B}$ (si $x = 3q + 2$ alors $x^2 = 3q' + 1$.)
   Ainsi $\sqrt{B} = (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$, qui n'est pas un bloc du fait qu'il contient 1 et que $\sqrt{B} - 1 = (3\mathbb{Z}) \cup (3\mathbb{Z} + 1)$ n'est pas un idéal de $\mathbb{Z}$.

5. Soient x, y, z trois éléments de B, qui est supposé non vide. Soit a dans A.
   Soit $t = a(x - y) + z$. On a $h(t) = h(a)(h(x) - h(y)) + h(z)$ car h est un morphisme d'anneaux.
   Mais $h(x), h(y), h(z)$ sont dans B', et $h(a)$ est dans A', donc $h(t)$ est dans B'.
   Ainsi t est dans B, ce qui prouve que B est un bloc de A.

   Si b est dans $\operatorname{Im} f$ alors $\{x \in A,\ f(x) = b\}$ est l'image réciproque non vide du singleton (donc du bloc) $\{b\}$: c'est donc un bloc de A.

III. Relation d'équivalence associée à un idéal

1. Pour tout x de A, $0 = x - x$ est élément de I, donc $\mathcal{R}$ est réflexive.
   L'ensemble I est stable pour le pssage à l'opposé. Il en résulte que si $x - y \in I$ (c'est-à-dire $x \mathcal{R} y$) alors $y - x \in I$ (c'est-à-dire $y \mathcal{R} x$.) Ainsi $\mathcal{R}$ est symétrique.
   Soient x, y, z dans A tels que $x \mathcal{R} y$ et $y \mathcal{R} z$, donc tels que $x - y$ et $y - z$ soient dans I.
   Alors $x-z = (x-y)+(y-z)$ est dans I car I est stable pour l'addition (sous-groupe de $(A, +)$.)
   Ainsi $x \mathcal{R} z$ ce qui prouve que $\mathcal{R}$ est transitive. Conclusion : $\mathcal{R}$ est une relation d'équivalence sur A.

2. Dire qu'une partie C de A est une classe d'équivalence pour la relation $\mathcal{R}$, c'est-dire qu'il existe t dans A tel que $C = \{x \in A,\ x \mathcal{R} t\}$.
   Mais $x \mathcal{R} t \Leftrightarrow \exists\, y \in I,\ x - t = y \Leftrightarrow \exists\, y \in I,\ x = t + y \Leftrightarrow x \in I_t = t + I$.
   Les classes d'équivalence de A pour $\mathcal{R}$ sont donc les I_t, avec t dans A.

3. Commençons par remarquer que les deux opérations $I_t I_u = I_{t+u}$ et $I_t I_u = I_{tu}$ ont un sens, c'est-à-dire que leurs résultats ne dépendent que des ensembles I_t et I_u, et pas des éléments t et u choisis pour les représenter.

   Pour cela donnnons nous $B = I_t$ et $C = I_u$ dans $\mathcal{B}_I$.
   On sait que $B = I_{t'} \Leftrightarrow t' - t \in I$ et que $C = I_{u'} \Leftrightarrow u' - u \in I$ (cf question II.3).
   On en déduit les égalités $\begin{cases} I_{t+u} = I_{t'+u'} \\ I_{tu} = I_{t'u'} \end{cases}$ car $\begin{cases} (t'+u') - (t+u) = (t'-t) + (u'-u) \in I \\ t'u' - tu = u'(t'-t) + t(u'-u) \in I \end{cases}$.
   Maintenant que les opérations sur $\mathcal{B}_I$ sont légitimées, on peut examiner leurs propriétés.
   Considérons l'application φ de A dans $\mathcal{B}_I$ définie par $\varphi(x) = I_x = I + x$.
   Cette application est par définition surjective.
   D'autre part, pour tous t, u de A, on a $\begin{cases} \varphi(t+u) = I_{t+u} = I_t + I_u = \varphi(t) + \varphi(u) \\ \varphi(tu) = I_{tu} = I_t I_u = \varphi(t)\varphi(u) \end{cases}$.
   Ainsi φ est un morphisme surjectif de $(A, +, \times)$ sur $(\mathcal{B}_I, +, \times)$.
   Il en résulte que φ "transporte" sur $\mathcal{B}_I$ les propriétés des lois de A, notamment :

   — Les lois $+$ et $\times$ de $\mathcal{B}_I$ sont commutatives et associatives.

   — Dans $\mathcal{B}_I$, la loi $\times$ est distributive par rapport à la loi $+$.

   — L'idéal $\varphi(0) = I_0 = I$ est le neutre de $\mathcal{B}_I$ pour la loi $+$.

   — Le bloc $\varphi(1) = I_1 = I + 1 = \{x + 1,\ x \in I\}$ est le neutre de $\mathcal{B}_I$ pour la loi $\times$.

   Conclusion : $\mathcal{B}_I$ est muni d'une structure d'anneau commutatif.