Anneaux

Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159, France
dany-jack.mercier@univ-ag.fr

23 octobre 2002

1 Définitions

Définition 1 *Un* ***anneau*** $(A\ +\ \ )$ *est la donnée d'un ensemble* A *et de deux lois internes* $+$ *et* $\ $ *telles que* $(A\ +)$ *soit un groupe commutatif et que la loi* $\ $ *soit associative et distributive par rapport à l'addition* $+$*. En général, on impose à* A *d'être* ***unitaire****, i.e. de posséder un élément neutre pour la multiplication. Cet élément est noté* 1_A*, et s'appelle* ***l'élément unité*** *(ou plus simplement "****l'unité****") de* A*. On retient : CANS-AD. On dit que l'anneau est* ***commutatif*** *si la loi* $\ $ *est commutative.*

La structure d'anneau est très utilisée en algèbre puisque correspond à la donnée d'un ensemble et de deux lois internes possédant de bonnes propriétés. L'ensemble $\mathbb{Z}$ des entiers relatifs, l'ensemble $\mathbb{Q}$ des nombres rationnels et celui $\mathbb{R}$ des nombres réels sont des anneaux. En fait tout élément de $\mathbb{R}$ possède un inverse multiplicatif, ce qui constitue une qualité supplémentaire et nous mène à la définition :

Définition 2 *Un* ***corps*** $(K\ +\ \ )$ *est la donnée d'un ensemble* K *et de deux lois internes* $+$ *et* $\ $ *telles que* $(K\ +)$ *soit un groupe commutatif, que* $(K^*\ \ )$ *soit un groupe, et que la loi* $\ $ *soit distributive par rapport à l'addition* $+$*. On retient : CANS-ANS-D.*

2 Anneaux quotients, Idéaux

Soit A un anneau. Cherchons les relations d'équivalence $\mathcal{R}$ sur A compatibles avec la structure d'anneau, i.e. vérifiant les deux conditions :

$$\begin{array}{lllll} (C1) & x\ y\ x\ \ y & A & x\mathcal{R}y \text{ et } x\,\mathcal{R}y & (x+x\,)\,\mathcal{R}\,(y+y\,) \\ (C2) & x\ y\ x\ \ y & A & x\mathcal{R}y \text{ et } x\,\mathcal{R}y & xx\,\mathcal{R}yy \end{array}$$

Ces conditions équivalent à l'affirmation "il est possible de définir une structure d'anneau sur l'ensemble quotient $A\ \mathcal{R}$ en choisissant les opérations naturelles $x+y\ =\ \overline{x+y}$ et

[0] [cann0007] v1.00 http://perso.wanadoo.fr/megamaths

$x\ y\ =\ \overline{xy}$". En effet, les résultats de telles opérations sont bien définis si, et seulement si, ils ne dépendent pas du choix des représentants x et y des classes x et y, ce qui est la traduction des conditions $(C2)$ et $(C2)$.
On a vu, lors de l'étude des groupes, qu'une relation du groupe commutatif $(A\ +)$ est compatible avec la loi $+$ (i.e. vérifie $(C1)$) si, et seulement si, c'est une relation suivant un sous-groupe H. Autrement dit, la condition $(C1)$ équivaut à l'existence d'un sous-groupe H tel que

$$x\mathcal{R}y \quad x-y \quad H \quad x \quad y+H$$

Vérifions-le rapidement : si $\mathcal{R}$ vérifie $(C1)$ alors $x\mathcal{R}y$ équivaut à $(x-y)\,\mathcal{R}0$ soit encore à $x-y \quad 0$ où 0 représente la classe de l'élément neutre 0 de A. Il est facile de vérifier que 0 est un sous-groupe de A. Notons-le H. Ainsi $x\mathcal{R}y$ équivaut à $x-y \quad H$. Réciproquement toute relation d'équivalence définie par $x-y \quad H$ est compatible avec la loi $+$ puisque pour tous $x\ y\ z \quad A$, $x-y \quad H$ entraîne $(x+z)-(y+z) \quad H$.

Supposons maintenant que $\mathcal{R}$ soit compatible avec la loi $+$, autrement dit que $\mathcal{R}$ soit une relation suivant un sous-groupe H. La condition $(C2)$ équivaut aux deux conditions

$(C2d)$ $x\ y\ a \quad A \quad x\mathcal{R}y \quad xa\mathcal{R}ya$ (compatibilité à droite avec la loi $\times$),
$(C2g)$ $x\ y\ a \quad A \quad x\mathcal{R}y \quad ax\mathcal{R}ay$ (compatibilité à gauche avec la loi $\times$),

ou encore à

$$\begin{array}{lllllll} (C2d) & x\ y\ a & A & x-y & H & (x-y)\,a & H \\ (C2g) & x\ y\ a & A & x-y & H & a\,(x-y) & H \end{array}$$

Cela s'écrit aussi

$$\begin{array}{llllll} (C2d) & x & H & a & A & xa \quad H \\ (C2g) & x & H & a & A & ax \quad H \end{array}$$

et nous invite à poser :

Définition 3 *Un* ***idéal à gauche (resp. à droite)*** *est un sous-groupe additif I de l'anneau A tel que*

$$\begin{array}{llllll} i & I & a & A & ai & I \\ (resp. & i & I & a & A & ia \quad I) \end{array}$$

Un idéal bilatère *(ou plus simplement un* ***idéal****) de A est un idéal à gauche et à droite de A.*

Théorème 1 *Les relations d'équivalence compatibles avec la structure d'anneau de $(A\ +\ )$ sont les relations suivants des idéaux bilatères I. Elles sont définies par*

$$x\mathcal{R}y \quad x-y \quad I$$

L'ensemble quotient $A\ \mathcal{R}$, noté commodément $A\ I$, est alors structuré en anneau pour les lois quotients $x+y\ =\ \overline{x+y}$ et $x\ y\ =\ \overline{xy}$.

Preuve : immédiate à partir du moment où les lois quotients sont bien définies. ■

3 Idéal engendré par une partie

Supposons l'anneau A commutatif de sorte que tous les idéaux de A sont bilatères. On vérifie que :

Proposition 1 *L'intersection d'idéaux de A est encore un idéal.*

Si $\mathcal{A}$ est une partie de A, l'intersection de tous les idéaux contenant $\mathcal{A}$ est un idéal, et c'est le plus petit idéal (au sens de l'inclusion) contenant $\mathcal{A}$. On le note $< \mathcal{A} >$ et on l'appelle **l'idéal engendré par la partie $\mathcal{A}$**. Ainsi

$$< \mathcal{A} >= \bigcap_{I \text{ idéal et} \mathcal{A} \subset I} I$$

L'idéal engendré par un élément $a \quad A$ est noté (a), aA ou Aa. Si I et J sont deux idéaux de A, l'idéal engendré par $I \quad J$ (resp. par la partie de A formée de tous les produits ij où i et j décrivent respectivement I et J) est noté $I + J$ (resp. IJ). La proposition suivante éclaire le choix de ces notations :

Théorème 2 *Soient I, J deux idéaux de A, et $a \quad A$.*
1) $(a) = \quad ax \quad x \quad A$
2) $I + J = \quad i + j \quad A \quad i \quad I$ *et* $j \quad J$
3) $IJ = \left\{ \sum_{k=1}^{n} i_k j_k \quad A \quad n \quad \mathbb{N}, i_k \quad I \text{ et } j_k \quad J \right\}$

Théorème 3 *L'idéal engendré par une partie quelconque $\mathcal{A}$ de A est*

$$< \mathcal{A} >= \left\{ x \quad A \quad n \quad \mathbb{N} \quad x_i \quad \mathcal{A} \quad a_i \quad A \; x = \sum_{i=1}^{n} a_i x_i \right\}$$

4 Homomorphismes d'anneaux

Définition 4 ***Un morphisme d'anneaux*** *de A vers A est une application $f : A \quad A$ entre deux anneaux telle que :*
1) $x \; y \quad A \quad f(x + y) = f(x) + f(y)$
2) $x \; y \quad A \quad f(xy) = f(x) \; f(y)$
3) $f(1_A) = 1_{A'}$

Contre-exemple : f peut vérifier 1) et 2) sans transformer l'unité de A en celle de A . Considérons une partie non vide F d'un ensemble E, et notons Δ la différence symétrique de deux ensembles. $(\mathcal{P}(E) \; \Delta \quad)$ est un anneau unitaire et l'application

$$\begin{array}{rccc} f : & \mathcal{P}(E) & - & \mathcal{P}(E) \\ & X & - & X \quad F \end{array}$$

vérifie 1) et 2). Cependant $f(E) = E \quad F = E$ montre que f n'est pas un endomorphisme d'anneaux. Dans ce cas, on dit que f est une "**représentation**".

Proposition 2 *Si* $f : A \quad A$ *est un homomorphisme d'anneaux,*
1) $f(0) = 0$
2) $x \quad A \quad f(-x) = -f(x)$
3) Si $x \quad A$ *est inversible, alors* $f(x)$ *l'est aussi et* $f(x)^{-1} = f\left(x^{-1}\right)$.

Théorème 4 ***Décomposition canonique d'un morphisme.***
Si $f : A \quad A$ *est un homomorphisme d'anneaux entre deux anneaux non nécessairement commutatifs, alors*
1) $\operatorname{Ker} f$ *est un idéal bilatère,*
2) $\operatorname{Im} f$ *est un sous-anneau de* A
3) Il existe un unique isomorphisme d'anneaux g *de* $A \quad \operatorname{Ker} f$ *sur* $\operatorname{Im} f$ *qui rende le diagramme suivant commutatif :*

$$\begin{array}{ccc} A & \overset{f}{} & A \\ \pi & & i \\ A \quad \operatorname{Ker} f & \overset{g}{} & \operatorname{Im} f \end{array}$$

i.e. tel que $f = i \circ g \circ \pi$. *Dans ce diagramme,* π *désigne la projection canonique de* A *sur* $A \quad \operatorname{Ker} f$ *et* i *l'injection canonique de* $\operatorname{Im} f$ *dans* A .

Preuve : 1) La partie $\operatorname{Ker} f$ est un sous-groupe additif de A comme noyau d'un morphisme de groupes (en effet $\operatorname{Ker} f$ n'est pas vide puisque contient l'élément neutre 0 de l'addition, et $a \quad b \quad \operatorname{Ker} f$ entraîne $f(a-b) = f(a) - f(b) = 0$ d'où $a - b \quad \operatorname{Ker} f$). De plus pour tout $a \quad A$ et tout $x \quad \operatorname{Ker} f$, $f(ax) = f(a) f(x) = f(a) 0 = 0$ montre que $ax \quad \operatorname{Ker} f$. Le noyau $\operatorname{Ker} f$ est bien un idéal à gauche. On montrerait de même que $\operatorname{Ker} f$ est un idéal à droite.

2) $\operatorname{Im} f$ est un sous-groupe additif de A comme image d'un morphisme de groupes ($\operatorname{Im} f$ n'est pas vide et $f(a) \quad f(b) \quad \operatorname{Im} f$ entraînent $f(a) - f(b) = f(a-b) \quad \operatorname{Im} f$), et la multiplication est interne dans $\operatorname{Im} f$ car si $f(a)$ et $f(b)$ appartiennent à $\operatorname{Im} f$, alors $f(a) f(b) = f(ab)$ aussi. Le lecteur notera bien que la partie $\operatorname{Im} f$ n'est pas un idéal de A dès que f n'est pas surjective. En effet si $\operatorname{Im} f$ est un idéal alors $1_{A'} = f\left(1_A\right) \quad \operatorname{Im} f$ entraîne $\operatorname{Im} f = A$.

3) Si g existe, alors $g\left(x\right) = f(x)$ pour tout $x \quad A \quad \operatorname{Ker} f$, et donc g est unique. On vérifie ensuite que $g\left(x\right) = f(x)$ définit bien une application de $A \quad \operatorname{Ker} f$ sur $\operatorname{Im} f$. Pour le voir, on doit prouver que l'image $f(x)$ de x par f est indépendante du choix du représentant x de x. Cela provient de

$$x = x \qquad x - x \quad \operatorname{Ker} f \qquad f(x) = f\left(x\right)$$

g est bien un homomorphisme d'anneaux puisque $g\left(1_A\right) = f(1_A) = 1_{A'}$,

$$g\left(a+b\right) = g\left(\overline{a+b}\right) = f(a+b) = f(a) + f(b) = g\left(a\right) + g\left(b\right)$$

et

$$g\left(ab\right) = g\left(\overline{ab}\right) = f(ab) = f(a) f(b) = g\left(a\right) g\left(b\right) \quad \blacksquare$$

5 Caractéristique d'un anneau, d'un corps

Définition 5 *Soit A un anneau. S'il existe un entier n non nul tel que $n\,1_A = 0$, on pose $c = \mathrm{Inf}\ \ n \quad \mathbb{N}^*\ \ n\,1_A = 0$ et l'on dit que A est un* ***anneau de caractéristique*** *c. Dans le cas contraire, on dit que A est de caractéristique* 0.

En utilisant la notion d'ordre d'un élément d'un groupe $(A\ +)$, on obtient la définition équivalente :

Définition 6 *Soit A un anneau. Si 1_A est d'ordre additif fini, cet ordre est appelé la* ***caractéristique*** *de A. Dans le cas contraire, on dit que A est de caratéristique* 0.

On remarque que

$$n\,1_A = 0 \qquad c\ \ n$$

et quel'égalité $cx = (c\,1_A)\,x = 0$ est vraie pour tout $x \quad A$. On note aussi que $c = 1$.

Les anneaux $\mathbb{Z}\ \ \mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0 tandis que $\mathbb{Z}\ \ n\mathbb{Z}$ est de caractéristique n. L'anneau produit $\mathbb{Z}\ \ a\mathbb{Z}\times\ \mathbb{Z}\ \ b\mathbb{Z}$ est de caractéristique $\mathrm{ppcm}\,(a\ \ b)$ puisque

$$\begin{pmatrix}1 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix} \qquad \begin{pmatrix}\ & \ \end{pmatrix} = \begin{pmatrix}0 & 0\end{pmatrix} \qquad a \quad \text{et } b \qquad \mathrm{ppcm}\,(a\ \ b)$$

Si A est un anneau de caractéristique c et sans diviseur de zéro, alors

$$nx = 0 \qquad c\ n \text{ ou } x = 0$$

En effet,

$$nx = 0 \qquad (n\ 1)\,x = 0 \qquad (n\ 1 = 0 \text{ ou } x = 0) \qquad c\ n \text{ ou } x = 0$$

Voici encore une troisième définition possible de la caractéristique d'un anneau :

Définition 7 *Soit A un anneau. L'application*

$$\begin{array}{rccc} : & \mathbb{Z} & - & A \\ & n & - & n\,1_A \end{array}$$

est un morphisme d'anneaux, et l'unique entier $c \quad \mathbb{N}$ tel que $\mathrm{Ker} \quad = c\mathbb{Z}$ *s'appelle* ***la caractéristique*** *de A.*

Cette définition permet de montrer le

Théorème 5 *La caractéristique d'un anneau sans diviseurs de zéro est soit* 0, *soit un nombre premier. C'est le cas d'un anneau intègre ou d'un corps.*

Preuve : La décomposition canonique du morphisme montre que $\mathbb{Z}\ \ c\mathbb{Z}$ est isomorphe à un sous-anneau de A, donc sans diviseur de zéro. Il suffit alors de se rappeler que $\mathbb{Z}\ \ c\mathbb{Z}$ (avec $c = 1$) est intègre si et seulement si c est premier ou $c = 0$. ■