Anneaux et corps

Tous les anneaux que nous considérerons sont *unitaires*, i.e. munis d'un élément unité 1_A pour la multiplication, et nous dirons *anneau* au lieu d'*anneau unitaire*.

1 Anneaux

Définition 1.1 Un anneau est un ensemble A muni de deux lois internes notées $+$ et $\times$, et de deux éléments notés 0 et 1, tels que :

(i) $(A, +, 0)$ est un groupe commutatif,

(ii) la loi $\times$ est associative et 1 est neutre pour cette loi,

(iii) la loi $\times$ est *distributive* à droite et à gauche pour $+$: $\forall (a, b, c) \in A^3$, $a \times (b + c) = a \times b + a \times c$ et $(b + c) \times a = b \times a + c \times a$.

Si l'on adopte le point de vue de la définition d'un groupe donnée dans le cours sur les groupes, un anneau est donc un quintuplet $(A, +, \times, 0, 1)$. De manière générale, on adopte avec les anneaux des conventions similaires à celles de la théorie des groupes : par exemple, on écrit ab ou $a.b$ au lieu de $a \times b$; on écrit simplement A au lieu de $(A, +, \times, 0, 1)$, etc.

Remarques 1.2 (1) Le symétrique d'un élément $a \in A$ est appelé son *opposé* et noté $-a$. Si a possède un inverse pour la loi $\times$, on l'appelle l'*inverse* et on le note a^{-1}.
(2) Dans un anneau A, on a toujours $a.0 = 0.a = 0$, pour tout $a \in A$. En effet, par distributivité on a $a.0 = a.(0+0) = a.0+a.0$ d'où $a.0 = 0$ en additionnant $-a.0$ de part et d'autre. (*Idem* pour $0.a = 0$.)
(3) On n'a pas précisé si 0 et 1 étaient distincts. En fait, si $0 = 1$ alors l'anneau A ne contient pas d'autre élément que 0. En effet, dans ce cas, pour tout $a \in A$ on a $a = a.1 = a.0 = 0$ donc $A = \{0\}$ (que l'on appelle l'*anneau nul*). Dit autrement, $A \neq \{0\} \Rightarrow 0_A \neq 1_A$.
(4) Prenez garde au fait qu'en général $(A, \times, 1)$ n'est pas un groupe, car les éléments n'ont pas tous des inverses (par exemple, si $A \neq \{0\}$, alors 0 n'a pas d'inverse). Attention aussi au fait qu'en général la loi $\times$ n'est pas commutative. Ces deux faits sont illustrés sur l'exemple de l'anneau $M_n(\mathbb{C})$ des matrices carrées de taille (n, n) à coeff. complexes.

Définition 1.3 L'ensemble des $a \in A$ qui possèdent un inverse pour la loi $\times$ est appelé le *groupe des éléments inversibles* de A et noté A^* ou $A^\times$.

Comme son nom l'indique, le groupe des inversibles $(A^*, \times, 1)$ est un groupe : la vérification est immédiate.

Définition 1.4 Un anneau A est dit *commutatif* si sa loi $\times$ est commutative.

Définition 1.5 Un *morphisme d'anneaux* entre deux anneaux A et B est une application $f : A \to B$ telle que

(i) f est un morphisme du groupe $(A, +)$ dans le groupe $(B, +)$,

(ii) $f(1) = 1$,

(iii) pour tout $(a, a') \in A^2$, on a $f(aa') = f(a)f(a')$.

On exprime parfois cette dernière propriété en disant que f est *multiplicative*.

Cela simplifie beaucoup la vie de noter par les mêmes lettres les lois d'anneaux différents, mais bien sûr, pour être le plus précis possible, il faudrait noter par exemple $+_A$, $+_B$, $\times_A$, $\times_B$.

Attention : *on ne dit pas* que f est un morphisme du groupe $(A, \times)$ dans le groupe $(B, \times)$, simplement car ceux-ci ne sont pas des groupes. En revanche, f induit un morphisme de groupes $f : A^* \to B^*$: cela provient simplement du fait que si $a \in A$ est inversible, il existe $a' \in A$ tel que $aa' = 1$, donc $f(a)f(a') = 1$ et $f(a)$ est inversible.

Définition 1.6 Soit $f : A \to B$ un morphisme d'anneaux. Le *noyau* de f est $\ker(f) := \{a \in A,\ f(a) = 0\}$ et l'*image* de f est $f(A)$.

Définition 1.7 Un sous-anneau d'un anneau A est un sous-ensemble $A_0 \subset A$ qui est un sous-groupe de $(A, +)$, contient 1 et est stable pour $\times$.

Par exemple $M_n(\mathbb{R})$ est un sous-anneau de $M_n(\mathbb{C})$.

L'image d'un morphisme d'anneaux $f : A \to B$ est un sous-anneau de B. En revanche, si $B \neq \{0\}$, le noyau n'est jamais un sous-anneau, car $f(1) = 1 \neq 0$.

2 Anneaux commutatifs

Dans la suite, tous les anneaux sont supposés commutatifs. Ceci simplifie un certain nombre de choses, et est conforme au programme du Capes qui demande de mettre l'accent sur ces anneaux, car les exemples principaux que nous regarderons sont commutatifs ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $k[X]$...). Les anneaux de matrices sont *essentiellement* les seuls anneaux non commutatifs du programme.

Définition 2.1 Dans un anneau A (sous-entendu maintenant commutatif), un *diviseur de zéro* est un élément $a \neq 0$ tel qu'il existe $a' \neq 0$ satisfaisant $aa' = 0$.

Les anneaux les plus sympathiques sont ceux qui ne possèdent pas de diviseur de zéro.

Définition 2.2 Un anneau est dit *intègre* s'il est non nul et ne possède pas de diviseur de zéro. Un anneau est appelé un *corps* si tout élément non nul est inversible.

Définition 2.3 Un *idéal* d'un un anneau A (commutatif) est un sous-ensemble $I \subset A$ tel que

(i) I est un sous-groupe de $(A, +)$,

(ii) I est stable par multiplication par des éléments de A : pour tout $a \in A$ et pour tout $i \in I$, on a $ai \in I$.

Exercice 2.4 (1) Montrez que le noyau d'un morphisme est un idéal. (2) Montrez que si a est un élément fixé de A, l'ensemble

$$\{x \in A, \exists y \in A, x = ay\} ,$$

est un idéal de A (ensemble des « multiples » de A). On le note (a).

L'idéal (a) de l'exercice ci-dessus est un exemple d'une notion plus générale, qui est celle idéal engendré par une partie. Pour simplifier, nous considérons uniquement des parties finies :

Proposition 2.5 *Soit A un anneau.*

(1) *L'intersection d'une famille d'idéaux de A est un idéal de A.*

(2) *Soient $x_1, \ldots, x_n$ des éléments de A. Alors, il existe un plus petit idéal de A contenant $x_1, \ldots, x_n$. C'est l'intersection des idéaux de A contenant $x_1, \ldots, x_n$. C'est aussi l'ensemble des éléments de la forme $a_1x_1 + \cdots + a_nx_n$ avec $a_1, \ldots, a_n$ éléments quelconques de A. On le note $(x_1, \ldots, x_n)$ et on l'appelle l'*idéal engendré par $x_1, \ldots, x_n$.

Compte tenu de sa description dans la proposition, on peut dire que l'idéal engendré par $x_1, \ldots, x_n$ est l'ensemble des « combinaisons linéaires de $x_1, \ldots, x_n$ à coefficients dans A ».

Définition 2.6 Un idéal I de A est dit *principal* s'il est engendré par un seul élément a, i.e. $I = (a)$. Un anneau est dit *principal* s'il est intègre et tous ses idéaux sont principaux.

Revenons à un morphisme d'anneaux (commutatifs) $f : A \to B$: on a dit que le noyau n'est jamais un sous-anneau si $B \neq \{0\}$. Nous allons voir que la situation pour les noyaux et les images est très sembable à ce que nous avons vu pour les groupes : *l'analogue d'un sous-groupe est un sous-anneau, et l'analogue d'un sous-groupe distingué est un idéal.* Ainsi : tout sous-anneau est l'image d'un morphisme d'anneaux et réciproquement ; tout idéal est le noyau d'un morphisme et réciproquement.

Dans la dernière phrase, la seule affirmation qui est difficile à démontrer est l'existence du quotient d'un anneau par un idéal :

Théorème 2.7 *Soit A un anneau et I un idéal. Alors il existe sur l'ensemble quotient A/I une unique structure d'anneau telle que la projection $\pi : A \to A/I$ soit un morphisme d'anneaux (surjectif). De plus, on a la propriété suivante : pour tout morphisme d'anneaux $f : A \to B$ tel que $I \subset \ker(f)$, il existe un unique morphisme $\widetilde{f} : A/I \to B$ tel que $f = \widetilde{f} \circ \pi$. De plus $\ker(\widetilde{f})$ est l'image de $\ker(f)$ dans A/I.*

C'est l'analogue du théorème d'existence du quotient d'un groupe G par un sous-groupe distingué H. La démonstration est analogue, et pour alléger, nous ne la donnerons pas ici.

Terminons cette partie par l'exemple des quotients de l'anneau $\mathbb{Z}$.

Proposition 2.8 *Les idéaux de l'anneau $\mathbb{Z}$ sont les parties de la forme $n\mathbb{Z}$, pour un entier $n \geqslant 0$.*

En effet, un idéal est en particulier un sous-groupe de $(\mathbb{Z}, +)$ donc de la forme $n\mathbb{Z}$. Comme un tel sous-groupe est clairement un idéal (c'est-à-dire stable par multiplication par des entiers relatifs quelconques $m \in \mathbb{Z}$), on obtient bien l'assertion de la proposition.

Proposition 2.9 *Soit $I = n\mathbb{Z}$ un idéal de $\mathbb{Z}$, avec $n \geqslant 0$ entier. Les conditions suivantes sont équivalentes :*

(i) *$\mathbb{Z}/n\mathbb{Z}$ est intègre,*

(ii) *n est nul ou c'est un nombre premier.*

En effet, si $n = 0$ on a $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$ qui est intègre. Si $n = 1$ on a $\mathbb{Z}/n\mathbb{Z} = \{0\}$ qui n'est pas intègre. Si n est un nombre premier p, $\mathbb{Z}/n\mathbb{Z}$ est intègre car $ab \equiv 0\ (p)$ implique d'après le lemme de Gauss que $a \equiv 0\ (p)$ ou $b \equiv 0\ (p)$. Enfin si $n \geqslant 2$ n'est pas premier, il possède au moins deux facteurs premiers p, q éventuellement égaux, de sorte que $pq \equiv 0\ (n)$ alors que ni p ni q n'est nul modulo n.

3 Corps

Tous les corps considérés dans ce cours seront commutatifs. Rappelons la définition :

Définition 3.1 Un anneau (commutatif) K est appelé un *corps* si tout élément non nul de K est inversible.

Définition 3.2 Soient K et L des corps. Un *morphisme de corps* est simplement un morphisme d'anneaux $f : K \to L$. Lorsque $K = L$, on dit que f est un *endomorphisme*. Un endomorphisme bijectif est appelé un *automorphisme*.

Remarque 3.3 Un corps K ne possède que deux idéaux : $\{0\}$ et K. En effet, soit I un idéal. Si $I \neq \{0\}$, il possède un élément $x \neq 0$, et comme cet élément est inversible, tout élément $y \in K$ s'écrit $y = yx^{-1}x \in I$. Donc $I = K$.

Proposition 3.4 *Tout morphisme de corps $f : K \to L$ est injectif.*

En effet, le noyau de f est un idéal distinct de K car il ne contient pas 1. Donc $\ker(f) = \{0\}$. Lorsqu'on a un morphisme (injectif) de corps $f : K \to L$, on dit aussi que L est une *extension* de K. Il est clair que f fait de L un K-espace vectoriel, avec la loi externe définie ainsi : si $\lambda \in K$ et $x \in L$, on pose $\lambda.x := f(\lambda)x$.

Nous allons définir la *caractéristique* d'un corps K. On note qu'il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to K$, qui est défini par $f(n) = n.1_K$. Le noyau $N = \ker(f)$ est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un certain entier $n \geqslant 0$. D'après le théorème d'existence et unicité du quotient (th. 2.7), il existe un unique morphisme *injectif* $\widetilde{f} : \mathbb{Z}/n\mathbb{Z} \hookrightarrow K$. Ceci montre que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-anneau d'un corps, donc il est intègre. D'après la proposition 2.9, on voit que n doit être nul ou égal à un nombre premier p.

Définition 3.5 On appelle *caractéristique* de K le nombre entier $n \geqslant 0$ générateur du noyau de l'unique morphisme $\mathbb{Z} \to K$. La caractéristique est égale à 0 ou à un nombre premier. On la note $\mathrm{car}(K)$.

Exemple 3.6 (1) Les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0.
(2) Soit p un nombre premier. Lorsqu'on regarde l'anneau $\mathbb{Z}/p\mathbb{Z}$ comme un corps, on le note le plus souvent $\mathbb{F}_p$. Ce corps est de caractéristique p.

Définition 3.7 Soit K un corps. Un *sous-corps* de K est un sous-anneau $k \subset K$ qui est un corps.

Proposition 3.8 *Soit K un corps. Alors, l'intersection d'une famille $\{k_i\}_{i \in I}$ de sous-corps de K est un sous-corps de K.*

La démonstration est routinière, elle se fait sur le modèle de la proposition qui affirme que dans un groupe G, l'intersection d'une famille de sous-groupes est un sous-groupe.

Proposition 3.9 *Soit K un corps. Alors l'intersection k_0 de tous les sous-corps de K est un sous-corps de K appelé le* sous-corps premier *de K. C'est le plus petit sous-corps de K. Si $\mathrm{car}(K) = 0$ on a $k_0 \simeq \mathbb{Q}$ et si $\mathrm{car}(K) = p > 0$ on a $k_0 \simeq \mathbb{Z}/p\mathbb{Z}$.*