Université Pierre et Marie Curie
Master de Sciences et Technologies
Mention *Mathématiques et Applications*
Spécialité *Education et Formation*, Section CAPES, M1
Année 2011 - 2012

ANNEAUX ET CORPS (résumé)

1. Anneaux

1.1. Définition d'un anneau (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). Remarques concernant la terminologie et les notations (les opérations sont appelées *addition* et *multiplication* et notées $+$ et $\times$, respectivement ; l'inverse d'un élément a d'un anneau A pour l'opération $+$ est appelé *opposé* de a et noté $-a$. Si un élément a de A possède un inverse pour l'opération $\times$, on l'appelle *inverse* de a et on le note a^{-1}).

Un élément a d'un anneau A tel que a possède un inverse pour l'opération $\times$ est dit *inversible*. Tous les éléments inversibles d'un anneau A forment un groupe par rapport à l'opération $\times$. Ce groupe est noté A^*.

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

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

(i) f soit un morphisme du groupe $(A, +)$ dans le groupe $(B, +)$,
(ii) $f(1_A) = 1_B$,
(iii) pour des éléments quelconques a_1 et a_2 de A, on ait $f(a_1a_2) = f(a_1)f(a_2)$.

Si $f : A \to B$ est un morphisme d'anneaux, alors f induit un morphisme de groupes A^* et B^*.

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

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

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 de f n'est pas un sous-anneau de A, car $f(1_A) = 1_B \neq 0_B$.

2. Anneaux commutatifs

Dans la suite, tous les anneaux sont supposés commutatifs.

Dans un anneau A (sous-entendu maintenant commutatif), un *diviseur de zéro* est un élément $a \neq 0$ tel qu'il existe un élément $a' \neq 0$ satisfaisant $aa' = 0$. Un anneau est dit *intègre* s'il est non nul et ne possède pas de diviseur de zéro.

Un idéal d'un anneau (commutatif) A 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 élément a de A et pour tout élément i de I, on a $ai \in I$.

L'intersection d'une famille d'idéaux d'un anneau (commutatif) A est un idéal de A.

Soit A un anneau (commutatif), et soient $x_1, \ldots, x_n$ des éléments de A. L'*idéal engendré par* $x_1, \ldots, x_n$ est l'intersection de tous les idéaux contenant $x_1, \ldots, x_n$. On le note $(x_1, \ldots, x_n)$.

Proposition. *Soit A un anneau (commutatif), et soit $x_1, \ldots, x_n$ des éléments de A. Alors, l'idéal engendré par $x_1, \ldots, x_n$ coïncide avec l'ensemble des éléments de A de la forme*

$$a_1x_1 + \ldots + a_nx_n,$$

où $a_1, \ldots, a_n$ sont des éléments quelconques de A.

Un idéal I d'un anneau A est dit *principal* s'il peut être engendré par un seul élément. Un anneau est dit *principal* s'il est intègre et tous ses idéaux sont principaux.

Pour tout morphisme d'anneaux (commutatifs) $f : A \to B$, le noyau de f est un idéal de A.

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

Proposition *Les idéaux de l'anneau $\mathbb{Z}$ sont les sous-ensembles de $\mathbb{Z}$ de la forme $n\mathbb{Z}$, où n est un entier positif ou nul.*

Proposition *Soit $I = n\mathbb{Z}$ un idéal de $\mathbb{Z}$, où n est un nombre entier positif ou nul. Les conditions suivantes sont équivalentes :*

(i) *l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre,*
(ii) *n est nul ou est un nombre premier.*

3. Corps

Tous les corps considérés dans ce cours seront commutatifs. Un anneau (commutatif) K est appelé un *corps* si tout élément non nul de K est inversible.

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

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

En effet, soit $f : K \to L$ un morphisme de corps. Le noyau de f est un idéal distinct de K, car $\ker(f)$ ne contient pas 1_K. 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.

Pour tout corps K, nous allons définir la caractéristique de K. Soit K un corps. On note qu'il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to K$. Ce morphisme est défini par $f(m) = m \times 1_K$ pour tout nombre entier m. Le noyau $\ker(f)$ est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un certain nombre entier $n \geq 0$. D'après le théorème ci-dessus, il existe un morphisme injectif $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to K$. Ceci montre que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-anneau d'un corps, donc $\mathbb{Z}/n\mathbb{Z}$ est intègre. D'après une proposition ci-dessus, on obtient que n doit être nul ou égal à un nombre premier.

On appelle *caractéristique* d'un corps K le nombre entier $n \geq 0$ 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 $\mathrm{car}(K)$.

Exemples.

(1) Les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique 0.
(2) Soit $p \in \mathbb{N}$ 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.

Soit K un corps. Un *sous-corps* de K est un sous-anneau $k \subset K$ tel que k soit un corps. L'intersection d'une famille quelconque de sous-corps de K est un sous-corps de K. L'intersection k_0 de tous les sous-corps de K est appelé le *sous-corps premier* de K. C'est le plus petit sous-corps de K. Si $\mathrm{car}(K) = 0$, le sous-corps premier k_0 est isomorphe à $\mathbb{Q}$. Si $\mathrm{car}(K) = p > 0$, le sous-corps premier k_0 est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.