Anneaux et corps

1 Anneaux

Définition : (A)
Soit A [1] un ensemble muni de deux lois de compositions internes notées "+" et " · " . On dit que (A,+, ·) est un anneau si :
(i) (A,+) est un groupe **abélien**
(ii) La loi " · " est associative
(iii) La loi " · " est distributive par rapport à la loi +
On peut résumer (iii) par : $\forall x, y, z \in$ A, on a :

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

Si la loi " · " admet un élément neutre, on dit que (A,+, ·) est un anneau unitaire[2].
Si la loi " · " est commutative, on dit que (A,+, ·) est un anneau commutatif.
Un élément de A est dit inversible s'il l'est pour la loi " · "

Exemples : $(\mathbb{Z}, +, \cdot)$,$(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$,$(\mathbb{C}, +, \cdot)$
$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$,$(\mathcal{M}_n(\mathbb{R}),+,\cdot)$

Remarques :

1. L'élément neutre de la loi " + " sera souvent noté 0, celui de la loi " · " sera souvent noté 1 ou *e* (et appelé élément unité ou unité).
2. Un élément de A est bien sûr toujours inversible pour la loi " + " car (A,+) est un groupe.
3. En général, on impose à (A,+,·) d'être unitaire.
4. On utilisera un abus de notation bien répandu : on notera l'anneau (A,+,·) par : A.
5. Si 1=0 (ie si l'élément neutre de la loi "+" est le même que celui de la loi " · " , alors A=0 (anneau trivial). Les deux anneaux dits "anneau trivial" sont : 0 et A. Dans certains livres, 0 n'est pas considéré comme un anneau[3].
6. Lorsqu'un élément $x \in$ A est inversible (pour la loi " · " bien sûr), son inverse est unique.
7. Les éléments neutres 0 (pour la loi "+") et 1 (pour la loi " · ") sont uniques.

Définition : ( )
On appelle corps[4] un anneau unitaire dans lequel tout élément non nul est inversible

Exemples : $(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{C},+,\cdot)$ $(\mathbb{Z}/p\mathbb{Z},+,\cdot)$ [où *p* premier] sont des corps. $(\mathbb{Z},+,\cdot)$ n'est pas un corps car seuls 1 et -1 sont inversibles (par la loi ·)/ $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ n'est pas un corps car il existe des matrices non inversibles.

Définition : (´)
Un élément *a* de A est dit diviseur de zéro à droite (respectivement à gauche) si $a \neq 0$ et s'il existe $b \neq 0$ tel que $a \cdot b = 0$ (resp $b \cdot a = 0$)

Définition : (`)
Un anneau A est dit intègre[5] s'il est sans diviseur de zéro, autrement dit :

$$a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Remarques :
1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ intègres
2) $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car 2 et 3 sont des diviseurs de zéro : $2 \cdot 3 = 0$ et $3 \cdot 2 = 0$ dans $\mathbb{Z}/6\mathbb{Z}$
3) Si *p* est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est intègre (mettre la preuve)
4) $M_n(\mathbb{R})$ est un anneau unitaire non intègre.

Proposition : *A* corps $\Rightarrow$ *A* anneau intègre

Définition : (´ ´)
Un élément $a \in$ A est dit nilpotent s'il existe un entier naturel non nul *n* tel que $a^n = 0$. L'indice de nilpotence de *a* (ou l'ordre[6] de *a*) est le plus petit entier naturel non nul *n* tel que $a^n = 0$.

Définition : (S -)
Un sous-ensemble B de A est dit un sous anneau si (B,+,·) est un anneau.

Remarques :
-La définition de sous-anneau est beaucoup moins utilisé que la notion de sous-groupe.
-On peut aussi définir un sous-anneau par :

Définition équivalente :
Un sous-ensemble B de A est appelé sous anneau de A si :
(i)(B,+) est un sous-groupe de (A,+)
(ii)Pour tout $x, y \in$ B, on a $x \cdot y \in$ B

remarque : si $n \neq \pm 1$, alors $n\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ (car ne contient pas *e*).

2 Idéaux

Définition : (I ´)
Soit I C A. On dit que I est un idéal à gauche (respectivement idéal à droite) de l'anneau (A, +,·) si (i) (I,+) est un sous-groupe de (A,+)
(ii) $x \in$ I,$y \in$ A $\Rightarrow xy \in$ I
(ie $\forall (x, y) \in$ I$\times$ A, $x.y \in$ I

[1] sources : Gourdon, Waggemann, Pajitnov, Danny-Jack Mercier, Dixmier. Tapé par Gwendal Haudebourg. Mis à jour le 31/07/2007

[2] Pajitnov considère que tous les anneaux sont unitaires

[3] Nous supposerons que 0 est un anneau dans ce cours (en suivant le cours de M.Pajitnov)

[4] Il existe une définition équivalente de corps :
Soit K un ensemble muni de deux lois de compositions internes "+" et " · ".(K,+,·) est un corps si :
(i) (K,+) est un groupe abélien
(ii) (K^*," · ") est un groupe
(iii) La loi · est distributive par rapport à la loi "+" Si la loi "·" est commutative, on parle de corps commutatifs.

[5] On excluera l'anneau 0, en le considérant comme non-intègre. Une définition pour éviter ce cas est donné ds le cours de Pajitnov : Un anneau A est dit intègre si $1 \neq 0$ et s'il est sans diviseur de zéro.

[6] On privilégera cette terminaison

Un anneau bilatère (ou tout simplement un idéal[7]) de A est un idéal à gauche et à droite de A, ie :

$$\forall (x,a) \in \mathrm{I} \times \mathrm{A},\ xa \in \mathrm{I} \text{ et } ax \in \mathrm{I}$$

Remarques :
-Un idéal est un sous-anneau de A
-La notion d'idéal est en quelque sorte l'analogue pour les anneaux de la notion de sous-groupe distingué.
-Si A est commutatif, alors pour tout $x \in$ A, l'ensemble $x\mathrm{A} := \{xa,\ a \in \mathrm{A}\}$ (que l'on note aussi (x)) est un idéal de A.
-Si A est unitaire et si $1 \in$ I où I est un idéal de A, la propriété (ii) entraîne que I=A (car, pour tout $a \in$ A, $x.1 = x \in$ I)
-Si un idéal I de A possède un élément inversible x de A, alors I=A :
-0 et A sont des idéaux de A

Proposition :
Une intersection d'idéaux de A est un idéal de A. Une somme finie d'idéaux de A est un idéal de A.

Définition (A)
Soit (A,+," · ") un anneau. Un idéal I de A est dit principal s'il existe $x \in$ A tel que I=(x). On note alors I=(x).
L'anneau A est dit principal s'il est commutatif, unitaire, intègre, et si tous les idéaux de A sont principaux.

Remarque : Il suffit de l'existence d'un $x \in$ A tel que I=xA (ie un x tel que I=(x)) pour que I soit principal.

Proposition : Les anneaux $\mathbb{Z}$ et $\mathbb{R}[x]$ sont principaux.

Définition : (I ´ ´)
Soient $(x_1, x_2, ..., x_n)$ n éléments de A. Le plus petit idéal contenant les éléments $x_1, x_2, ..., x_n$ est appelé idéal engendré par $(x_1, x_2, ..., x_n)$, et noté : $(x_1, x_2, ..., x_n)$ On a :
$(x_1, x_2, ..., x_n) := \{x_1 \cdot y_1 + x_2 \cdot y_2 + ... + x_n \cdot y_n)$,
$y_i \in A, \forall i = 1...n\}$

Proposition : A est un corps si et seulement si tous les idéaux de A sont triviaux.

3 Anneaux quotients

Comme pour les groupes, on peut définir la notion de quotient sur les anneaux. Etant donné une relation d'équivalence R sur A, on cherche à faire de A/R un anneau en le munissant des loi :
(i)$\overline{x+y} = \overline{x} + \overline{y}$
(ii)$\overline{x \cdot y} = \overline{x} \cdot \overline{y}$
Si ces lois sont bien définies (c'est à dire que ne dépendent pas des représentants choisis de $\overline{x}$ et $\overline{y}$, on dit que R est compatible avec la structure d'anneau. On montre que les relations d'équivalences compatibles avec la structure d'anneau sont de la forme $x\mathcal{R}y \Leftrightarrow x - y \in$ I, où I est un idéal de A. Si tel est le cas, A/$\mathcal{R}$ est un anneau (muni des loi définies plus haut) appelé anneau quotient et noté A/I.

[7] on privilégera cette terminaison

4 Morphismes d'anneaux

Définition : (M ')
Soient A et B deux anneaux. On appelle morphisme d'anneau (ou homomorphisme d'anneaux) de A dans B toute application f : A→ B tq :
(i) $f(x+y) = f(x) + f(y),\ \forall x, y \in \mathrm{A}$
(ii)[8] $f(x \cdot y) = f(x) \cdot f(y),\ \forall x, y \in \mathrm{A}$

Définitions : ( )
Un morphisme d'anneau f est dit monomorphisme si f est injectif
Un morphisme d'anneau f est dit épimorphisme si f est surjectif
Un morphisme d'anneau f est dit isomorphisme si f est bijectif
Deux anneaux (A, +," · ") et (B,+," · ") sont dits isomorphes s'il existe un isomorphisme f : A→ B
Soit f un morphisme d'anneaux. Alors $Ker\,f$ est appelé noyau de f, $Im\,f$ est appelé image de f, où :
$Ker\,f = \{x \in \mathrm{A},\ f(x) = 0\} = f^{-1}(\{0\})$
$Im\,f = \{y \in \mathrm{B},\ \exists x \in \mathrm{A} \text{ tq } f(x) = y\} = \{f(x),\ x \in \mathrm{A}\}$

remarques :
Soit f : A→ B un morphisme d'anneaux. Alors $Im\,f$ est un sous-anneau de B ; $Ker\,f$ est un idéal de A, donc un sous-anneau de A

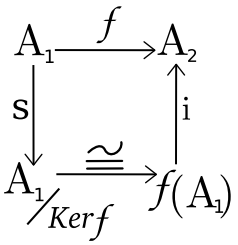
exemple :
P : $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
$x \to [x]$ est un morphisme d'anneaux, avec les lois définies plus haut

Proposition :
Soient A et B deux anneaux, f : A→ B un morphisme d'anneau. Alors :
Si I est un idéal de A, et si f est surjectif, alors f(A) est un idéal de A.
Si I' est un idéal de A', f^{-1}(I') est un idéal de A.
L'image (et l'image réciproque) par f (respectivement par f^{-1}) d'un sous-anneau (donc d'un anneau) est un sous-anneau (donc un anneau).
f(A) est isomorphe à l'anneau quotient A/$Ker\,f$

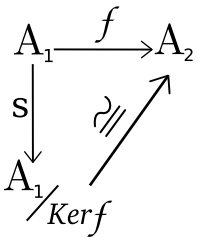
Remarque : La dernière assertion de la proposition est importante. C'est souvent le moyen le plus rapide pour montrer qu'un anneau est isomorphe à un anneau quotient.

Proposition : (')
Soit f : A→ B un morphisme d'anneaux, I ⊆ A un idéal tel que I ⊆ $Ker\,f$. Alors, il existe un unique morphisme d'anneaux g : A/I→ B tel que le diagramme suivant soit commutatif :

[8] Et pas : f hom. de groupe pour la loi . car (A, .) pas forcément un groupe ! De plus, faire attention à la loi . employée : pas forcément la même dans A et dans B.



De plus, si f est surjectif, g est un isomorphisme :



Définition : (I ´ -I ´)
Soit I ⊊ A un idéal. I est appelé premier si :

$$x.y \in \mathrm{I} \Rightarrow (x \in \mathrm{I} \text{ ou } y \in \mathrm{I})$$

I est appelé maximal s'il n'existe pas d'idéal J de A tel que I ⊊ J ⊊ A

Propositions :
1) Un idéal maximal est premier
2) I est premier ⟺ A/I est intègre
3) I est maximal ⟺ A/I est un corps

Proposition : $n\mathbb{Z}$ est un idéal premier ⇔ $n\mathbb{Z}$ est un idéal maximal ⇔ n est premier

Proposition : Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ (ie coincïdent avec les sous-groupes de $\mathbb{Z}$), et :

p ⟺ $\mathbb{Z}/p\mathbb{Z}$ ` ⟺ $\mathbb{Z}/p\mathbb{Z}$

5 Eléments irréductibles

Définition : (E ´ ´)
Un élément $x \neq 0$, $x \in A$ est appelé irréductible si x n'est pas inversible et si ($x = a.b \Rightarrow a$ inversible ou b inversible)

Remarques :
(1) les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers (rappel : les éléments sont dits inversibles, s'ils le sont pour la loi " · ")
(2) soient p_1, p_2 irréductibles. Alors $pgcd(p_1, p_2)$ ou $p_1 \sim p_2$

Proposition : soit $x \neq 0$. Alors x est irréductible ⇔ (x) est un idéal premier ⇔ (x) est un idéal maximal

Théorème (décomposition d'un élément) : soit $x \neq 0$. Alors soit x est inversible, soit il existe $(p_1, ..., p_k) \in A^k$ inversibles, $u \in A$ inversible, tels que $x = u.p_1...p_k$ (à permutation près)

6 Anneaux Euclidiens

Définition (Anneau euclidien) : soit A un anneau intègre. On dit que A est euclidien s'il existe une fonction N :
$A - \{0\} \longrightarrow \mathbb{N}$ telle que :
(1) $N(ab) \geqslant N(b)$, $\forall a, b \in A - \{0\}$
(2) $\forall a, b \in A$, $b \neq 0$, $\exists!(q, r) \in A$ tq. $a = bq + r$ ($r = 0$ ou $N(r) < N(b)$

La fonction N est appelée **norme euclidienne**

Exemples :

1. $\mathbb{Z}$ est euclidien, avec $N(x) = |x|$
2. $\mathbb{Z}[i] := \{m + in, (m, n) \in \mathbb{Z}^2\}$ est euclidien, avec $N(z = x + iy) = x^2 + y^2$. $\mathbb{Z}[i]$ est appelé anneau des nombres de Gauss.
3. $\mathbb{K}[x]$ est euclidien, avec $N(P) = deg(P)$

Théorème : A anneau euclidien ⇒ A principal

6.1 Anneau de Gauss

Rappel : $\mathbb{Z}[i] := \{m + in, (m, n) \in \mathbb{Z}^2\}$ est euclidien, avec $N(z = x + iy) = x^2 + y^2$. $\mathbb{Z}[i]$ est donc aussi principal.
Eléments inversibles : $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

Proposition 1 : soit $u \neq 0$, $u \in \mathbb{Z}[i]$. Alors
u inversible ⇔ $N(u) = 1$ ⇔ $u \in \{1, -1, i, -i\}$

Proposition 2 : $N(z)$ premier ⇒ z irréductible.

Proposition 3 : soit p un nombre premier. Alors :
(1) p n'est pas irréductible dans $\mathbb{Z}[i]$ ⇔ $\exists n, m \in \mathbb{Z}$ tq. $p = n^2 + m^2$
(2) si $p \equiv m \bmod 4$, alors p est irréductible dans $\mathbb{Z}$

Exemples :
$2 + i$ irréductible car $N(2 + i) = 5 \in \mathcal{P}$
$2 = (1 + i).(1 - i)$ n'est pas irréductible (car 2=produit de deux facteurs non inversibles dans $\mathbb{Z}[i]$)
$5 = 2^2 + 1^2$ et 5 premier donc pas irréductible
$2 = 1^2 + 2^2$ et 2 premier donc pas irréductible
$N(3) = 9$ pas premier, mais 3 irréductible (car réciproque Prop.2 est fausse)