Anneaux - Décembre 2004

Définition 1. *On appelle* anneau *la donnée d'un groupe commutatif* $\langle A, +, 0\rangle$*, muni d'une seconde opération notée* $\cdot$ *et appelée multiplication vérifiant les propriétés suivantes :*

1. *la loi muliplicative est* interne et partout définie*, c'est-à-dire*

$$\forall a \in A \quad \forall b \in A \quad : \quad a \cdot b \in A,$$

2. *il existe un élément* neutre *pour la loi muliplicative, c'est-à-dire*

$$\exists c \in A \quad \forall a \in A \quad : \quad a \cdot c = c \cdot a = a.$$

   On note 1 *cet élément neutre pour la multiplication (car on peut montrer qu'il est unique, voir le lemme 3),*

3. *la loi muliplicative est* associative*, c'est-à-dire*

$$\forall a \in A \quad \forall b \in A \quad \forall c \in A \quad : \quad (a \cdot b) \cdot c = a \cdot (b \cdot c),$$

4. *la loi multiplicative est* distributive *sur la loi additive c'est-à-dire,*

$$\forall a \in A \quad \forall b \in A \quad \forall c \in A \quad :$$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad et \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Un tel anneau sera noté $\langle A, +, \cdot, 0, 1\rangle$. *Si de plus* $\langle A, +, \cdot, 0, 1\rangle$ *vérifie la propriété suivante :*

5 la loi $\cdot$ *est* commutative*, c'est-à-dire*

$$\forall a \in A \quad \forall b \in A \quad : \quad (a \cdot b) = (b \cdot a),$$

on dira que l'anneau $\langle A, +, \cdot, 0, 1\rangle$ *est un* anneau commutatif*.*

Exemples 2. *Des exemples d'anneaux commutatifs sont :*

$$\langle \mathbb{Z}, +, \cdot, 0, 1\rangle,\ \langle \mathbb{Q}, +, \cdot, 0, 1\rangle,\ \langle \mathbb{R}, +, \cdot, 0, 1\rangle,\ \langle \mathbb{C}, +, \cdot, 0, 1\rangle.$$

Des exemples d'anneaux non-commutatifs sont :

$$\langle M_n(\mathbb{Q}), +, \cdot, 0, 1\rangle,\ \langle M_n(\mathbb{R}), +, \cdot, 0, 1\rangle,\ \langle M_n(\mathbb{C}), +, \cdot, 0, 1\rangle.$$

Lemme 3. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif, le neutre pour la multiplication est unique.*

Démonstration. **Supposons l'existence d'un autre élément neutre, noté** $1'$**. Si on considère l'expression** $1 \cdot 1'$**, on a qu'elle est à la fois égale à** 1 **(puisque** $1'$ **est un élément neutre pour** $\cdot$**) et à** $1'$ **(puisque** 1 **est un élément neutre pour** $\cdot$**). Ceci permet de conclure que** $1 = 1'$**.** □

Lemme 4. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif, quel que soit* $a \in A$*, on a que* $0 \cdot a = a \cdot 0 = 0$*.*

Démonstration. **Puisque** 0 **est le neutre pour l'addition, on peut écrire** $0 + 0 = 0$**. En utilisant la distributivité de** $\cdot$ **sur** $+$**, on a que** $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$**. En ajoutant l'inverse pour** $+$ **de** $0 \cdot a$ **aux deux membres de l'égalité, on obtient le résultat souhaité.** □

Etant donné $\langle A, +, \cdot, 0, 1\rangle$ **un anneau, on appelle** $\langle A, +, 0\rangle$ **le *groupe additif* de l'anneau. Il est donc naturel de considérer les sous-groupes de** $\langle A, +, 0\rangle$**.**

Définition 5. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif et* $\langle I, +, 0\rangle$ *un sous-groupe de* $\langle A, +, 0\rangle$*, si ce sous-groupe vérifie la propriété suivante :*

$$\forall a \in A \quad \forall b \in I \quad : \quad a \cdot b \in I,$$

on dit que le sous-groupe $\langle I, +, 0\rangle$ *est un* idéal *de l'anneau* $\langle A, +, \cdot, 0, 1\rangle$*.*

Exemple 6. *L'ensemble des nombres pairs* $(2\mathbb{Z})$ *est un idéal de l'anneau* $\langle \mathbb{Z}, +, \cdot, 0, 1\rangle$*.*

On peut montrer que les idéaux de $\langle \mathbb{Z}, +, \cdot, 0, 1\rangle$ **ont une forme particulière.**

Lemme 7. *Tout idéal de* $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ *est de la forme* $n\mathbb{Z}$ *où* $n \in \mathbb{N}$ *(avec* $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$*.*

Démonstration. vu au cours □

Lemme 8. *Soit* $\langle A, +, \cdot, 0, 1 \rangle$ *un anneau commutatif et* $\langle I, +, 0 \rangle$ *un idéal de* $\langle A, +, \cdot, 0, 1 \rangle$ *, alors* I *est un sous-groupe normal de* $\langle A, +, 0 \rangle$*.*

Démonstration. **Vu que** $\langle A, +, 0 \rangle$ **est commutatif, tous ses sous-groupes sont des sous-groupes normaux.** □

Définition 9. *Soit* $\langle A, +, \cdot, 0, 1 \rangle$ *un anneau commutatif, soit* B *un sous-ensemble non vide de* A*, tel que* 0 *et* $1 \in B$*. Si* B *muni des opérations* $+$ *et* $\cdot$ *héritées de* A *est un anneau commutatif, on dit que* $\langle B, +, \cdot, 0, 1 \rangle$ *est* sous-anneau *de* $\langle A, +, \cdot, 0, 1 \rangle$*.*

On peut alors établir un *critère de sous-anneau* (en s'inspirant du critère de sous-groupe).

Lemme 10. ***Critère de sous-anneau***

Soit $\langle A, +, \cdot, 0, 1 \rangle$ **un anneau commutatif et** $B \subseteq A$**, on a que** $\langle B, +, \cdot, 0, 1 \rangle$ **est un sous-anneau de** $\langle A, +, \cdot, 0, 1 \rangle$ **si et seulement si il satisfait les conditions suivantes :**

- $1 \in B$,
- **pour tout** $a \in B$**, l'inverse de** a **pour la loi** $+$ **(noté** $-a$**) appartient à** B**,**
- **pour tout** $a, b \in B$ **on a que** $a + b \in B$ **et** $a \cdot b \in B$**.**

Démonstration. **On commence par prouver que** $0 \in B$**, vu que** $1 \in B$**, on sait que** $-1 \in B$ **(car l'inverse**[1] **pour la loi** $+$ **de tout élément de** B **est dans** B**). Vu que la loi** $+$ **est interne et partout définie, on a que** $1+(-1)$ **appartient à** B **et** $1+(-1) = 0$ **par définition de l'inverse pour** $+$**.**

Il reste à prouver que $+$ **est associative et commutative (On aura ainsi prouvé que** $\langle B, +, 0\rangle$ **est un sous-groupe de** $\langle A, +, 0\rangle$**.), que** $\cdot$ **est associative et que** $\cdot$ **est distributive sur** $+$**. Toutes ces propriétés étant des propriétés universelles vraies sur** A**, elles restent naturellement vraies dans** B **qui est un sous-ensemble de** A**.** □

On peut également définir une notion de *morphisme d'anneaux*.

Définition 11. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *et* $\langle B, +, \cdot, 0, 1\rangle$ *deux anneaux commutatifs, un* morphisme d'anneaux σ *est un* morphisme de groupes *entre les groupes*

[1] On adoptera la convention usuelle d'appeler opposé l'inverse d'un élément pour la loi $+$.

additifs $\langle A, +, 0\rangle$ *et* $\langle B, +, 0\rangle$ *vérifiant les deux propriétés additionnelles suivantes :*

1. $\sigma(1) = 1$,
2. $\forall a \in A \quad \forall b \in A \quad : \quad \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

Le noyau d'un tel morphisme est son noyau en tant que morphisme de groupes additifs, c'est-à-dire $ker(\sigma) = \{a \in A \mid \sigma(a) = 0\}$.

Exemple 12. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif, la fonction identité* $\sigma : A \to A$ *est un morphisme d'anneaux.*
La conjugaison dans les complexes est un isomorphisme de $\langle \mathbb{C}, +, \cdot, 0, 1\rangle$ *dans lui même.*

Lemme 13. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *et* $\langle B, +, \cdot, 0, 1\rangle$ *deux anneaux commutatifs et* $\sigma : A \to B$ *un morphisme d'anneaux,* $ker(\sigma)$ *est un idéal de* A.

Démonstration. **On doit d'abord montrer que** $\langle ker(\sigma), +, 0\rangle$ **est un sous-groupe commutatif de** $\langle A, +, 0\rangle$**. Pour ce faire, on va utiliser le critère du sous-groupe**[2] **:**

[2]On peut faire une preuve très courte en utilisant la théorie des groupes : par hypothèse σ est un morphisme entre les groupes additifs des anneaux, donc son noyau est un sous-groupe de $\langle A, +, 0\rangle$.

- $0 \in ker(\sigma)$**, en effet** $\sigma(0) = 0$**, car** σ **est un morphisme de groupes (entre les groupes additifs** $\langle A, +, 0\rangle$ **et** $\langle B, +, 0\rangle$**).**
- **Soit** a**,** $b \in ker(\sigma)$**, on doit prouver que** $a + b \in ker(\sigma)$**, c'est à dire on doit prouver que** $\sigma(a+b) = 0$**. En utilisant le fait que** σ **est un morphisme, on peut écrire** $\sigma(a+b) = \sigma(a)+\sigma(b)$**, vu que** a**,** $b \in ker(\sigma)$**, on a que** $\sigma(a) = 0 = \sigma(b)$**, et donc que** $\sigma(a+b) = 0$**.**
- **Soit** $a \in ker(\sigma)$**, on doit prouver que** $-a \in ker(\sigma)$**, c'est à dire on doit prouver que** $\sigma(-a) = 0$**. En utilisant le fait que** σ **est un morphisme, on peut écrire** $\sigma(-a) = -\sigma(a)$**, et vu que** $a \in ker(\sigma)$**, on a que** $\sigma(a) = 0$**, et donc que** $\sigma(-a) = 0$**.**

On a donc prouvé que $\langle ker(\sigma), +, 0\rangle$ **est un groupe, il reste à prouver que** $ker(\sigma)$ **vérifie la propriété supplémentaire qui fera de lui un idéal. On doit donc montrer que pour tout élément** $a \in A$ **et pour tout élément** $b \in ker(\sigma)$**, on a que** $a \cdot b \in ker(\sigma)$**. Il faut donc montrer que** $\sigma(a \cdot b) = 0$**. Vu que** σ **est un morphisme d'anneaux, on peut écrire** $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = \sigma(a) \cdot 0 = 0$ **(vu que** $b \in ker(\sigma)$ **et vu le lemme 4). Ce qui conclut la preuve.** □

Lemme 14. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *et* $\langle B, +, \cdot, 0, 1\rangle$ *deux anneaux commutatifs et* $\sigma : A \to B$ *un morphisme d'anneaux,* $\langle Im(\sigma), +, \cdot, 0, 1\rangle$ *est un sous-anneau*

de B.

Démonstration. **Rappelons que $Im(\sigma) = \{\sigma(a) \mid a \in A\}$. On va utiliser le critère de sous-anneau.**

- $1 \in Im(\sigma)$ **car** $1 \in A$**, et** $\sigma(1) = 1$ **car** σ **est un morphisme d'anneaux.**
- **Soit** $b \in Im(\sigma)$**, on doit prouver que** $-b \in Im(\sigma)$**. Vu que** $b \in Im(\sigma)$**, il existe** $a \in A$ **tel que** $b = \sigma(a)$**. Vu que** $\langle A, +, 0\rangle$ **est un groupe, on a que** $-a \in A$**. Si on considère** $\sigma(-a)$**, on a que** $\sigma(-a) = -\sigma(a)$ **(car** σ **est un morphisme de groupes) et donc** $\sigma(-a) = -b$**, ce qui signifie que** $-b \in Im(\sigma)$**.**
- **Soit** b_1**,** $b_2 \in Im(\sigma)$**, on doit prouver que** $b_1 + b_2 \in Im(\sigma)$ **et** $b_1 \cdot b_2 \in Im(\sigma)$**. Vu que** b_1**,** $b_2 \in Im(\sigma)$**, on peut trouver** a_1**,** $a_2 \in A$ **tels que** $\sigma(a_1) = b_1$ **et** $\sigma(a_2) = b_2$**. Vu que** σ **est un morphisme d'anneaux, d'une part, on a que** $b_1 + b_2 = \sigma(a_1) + \sigma(a_2) = \sigma(a_1 + a_2)$ **et d'autre part, on a que** $b_1 \cdot b_2 = \sigma(a_1) \cdot \sigma(a_2) = \sigma(a_1 \cdot a_2)$**. Vu que** $\langle A, +, \cdot, 0, 1\rangle$ **est un anneau, on a que** $a_1 + a_2 \in A$ **et** $a_1 \cdot a_2 \in A$**, ce qui permet de conclure que** $b_1 + b_2 \in Im(\sigma)$ **et** $b_1 \cdot b_2 \in Im(\sigma)$**.**

□

Rappel 15. *Soit $\langle A, +, \cdot, 0, 1\rangle$ un anneau commutatif, $X \subseteq A$ et $a \in A$, on*

définit $a + X = \{a + x \mid x \in X\}$.

Définition 16. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif,* I *un idéal de* A *et* a *un élément de* A*, on définit la* classe latérale de a modulo I*, notée* $a + I$ *comme suit :*

$$a + I = \{a + i \mid i \in I\}.$$

On note A/I l'ensemble des classes latérales et on l'appelle le *quotient de A par I*. On a donc

$$A/I = \{a + I \mid a \in A\}.$$

Lemme 17. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif,* I *un idéal de* A*,* a *et* b *deux éléments de* A*, on a que* $a + I$ *et* $b + I$ *sont en bijection.*

Démonstration. **Ce lemme n'est que la transcripton en notation additive du résultat suivant démontré en théorie des groupes : soit $\langle G, \cdot, 1\rangle$ un groupe et $\langle H, \cdot, 1\rangle$ un sous-groupe de G, soit g, $g' \in G$:** $g'H = (g' \cdot g^{-1})(gH)$ □

Lemme 18. ***Egalité des classes***

Soit $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif,* I *un idéal de* A*,* a *et* b *deux éléments de* A*, on a que*

$$a + I = b + I \quad \textit{si et seulement si} \quad b - a \in I.$$

Démonstration. I **est un idéal de** A **donc (par définition d'idéal),** $\langle I, +, 0\rangle$ **est un sous-groupe** $\langle A, +, 0\rangle$**, on peut donc appliquer le lemme d'égalité des classes vu au cours pour les groupes.**

Soit $a, b \in A$**, le lemme d'égalité des classes garantit que**

$$a + I = b + I \text{ si et seulement si } -a + b \in I.$$

Or $\langle A, +, 0\rangle$ **est un groupe commutatif, donc** $-a+b = b-a$**, ce qui fournit le résultat demandé.**

□

On peut munir le quotient de A **par** I **d'une addition et d'une multiplication définies comme suit :**

- $(a + I) + (b + I) = (a + b) + I$**,**
- $(a + I) \cdot (b + I) = (a \cdot b) + I$**.**

Lemme 19. *Les opérations* $+$ *et* $\cdot$ *définies sur* A/I *sont bien définies.*

Démonstration. **Pour l'addition, on est dans le cas de la théorie des groupes** I **est idéal de** A **et donc** $\langle I, +, 0\rangle$ **est un sous-goupe normal de** $\langle I, +, 0\rangle$ **(lemme 8). Donc l'addition des classes est bien définies.**

Pour la multiplication, on doit montrer que si $a + I = a' + I$ **et** $b + I = b' + I$ **alors** $a \cdot b + I = a' \cdot b' + I$**. Par le lemme d'égalité des**

classes pour les groupes (vu au cours), il suffit de montrer que $a' \cdot b' \in a \cdot b + I$, mais par hypothèse et vu le lemme d'égalité des classes, on a $a' \in a + I$ et $b' \in b + I$, c'est-à-dire qu'il existe i, $j \in I$ tels que $a' = a + i$ et $b' = b + j$, donc

$$a' \cdot b' = a \cdot b + a \cdot j + i \cdot b + i \cdot j = a \cdot b + k \quad k \in I.$$

En effet, si i, $j \in I$ et a, $b \in A$, par définition de l'idéal, on a que $a \cdot j$, $i \cdot b$ et $i \cdot j$ appartiennent à I et donc leur somme appartient à I.

□

Théorème 20. *Soit $\langle A, +, \cdot, 0, 1\rangle$ un anneau commutatif, I un idéal de A, le quotient A/I muni des deux opérations $+$ et $\cdot$ (définies ci-dessus) est un anneau commutatif où $0 + I$ est le neutre pour $+$ et $1 + I$ est le neutre pour $\cdot$. Cet anneau est appelé l'*anneau quotient *et est noté $\langle A/I, +, \cdot, 0 + I, 1 + I\rangle$*

Démonstration.

- **$\langle A/I, +, 0 + I\rangle$ est un groupe en appliquant la théorie vue au cours, car I est un sous-groupe normal de A (pour la loi additive).**
- **$\cdot$ est interne et partout définie par définition et bien définie par le lemme 19.**

– $1 + I$ **est le neutre pour** $\cdot$**, en effet pour tout** $a + I \in A/I$**,**

$$(1 + I) \cdot (a + I) = (1 \cdot a) + I = a + I$$

car 1 **est le neutre pour la multiplication dans** A**. De la même façon, on prouve que** $(a + I) \cdot (1 + I) = a + I$**.**

– **On prouve de la même façon que la multiplication dans** A/I **hérite de l'associativité de la multiplication dans** A**. Le même argument reste valable pour la commutativité et la distributivité.**

ATTENTION ceci ne signifie pas que A/I **est un sous-anneau de** A**, en effet on n'a même pas l'inclusion de** A/I **dans** A **puisque les objets de** A/I **ne sont pas du même type que ceux** A**.**

□

Remarque 21. *Etant donné* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif,* I *un idéal de* A*, si on considère le quotient de* A *par* I*, il existe un morphisme naturel* μ *de* A *dans* A/I*, où* $\mu(a) = a + I$*. Ce morphisme est par définition de* A/I *surjectif, mais en général pas injectif. De plus, on a que* $ker(\mu) = I$*. On demande au lecteur non convaincu de vérifier ces propriétés.*

Théorème 22. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *et* $\langle B, +, \cdot, 0, 1\rangle$ *deux anneaux commutatifs,*

$\sigma : A \to B$ un morphisme d'anneaux. On a que $A/ker(\sigma)$ est isomorphe (en tant qu'anneau) à $Im(\sigma)$.

Démonstration. **On sait par le cours que $A/ker(\sigma)$ est isomorphe à $Im(\sigma)$ en tant que groupe additif. L'isomorphisme vu au cours est $\tau : A/ker(\sigma) \to Im(\sigma)$ donné par $\tau\big(a + ker(\sigma)\big) = \sigma(a)$. Il reste à montrer que cet isomorphisme de groupe est en fait également un isomorphime d'anneaux, c'est-à-dire qu'il faut vérifier les propriétés additionnelles qui définissent la notion de morphisme d'anneaux.**

- $\tau(1 + ker(\sigma)) = \sigma(1)$ **par définition de τ et**

  $\sigma(1) = 1$ **puisque σ est un morphisme d'anneaux.**

- **Soit $a + ker(\sigma)$, $b + ker(\sigma) \in A/ker(\sigma)$, on a que**

  $\tau\big(a + ker(\sigma) \cdot b + ker(\sigma)\big) = \tau\big(a \cdot b + ker(\sigma)\big)$ **par définition de la multiplication des classes et**

  $\tau\big(a \cdot b + ker(\sigma)\big) = \sigma(a \cdot b)$ **par définition de τ. Et puisque σ est un morphisme d'anneaux $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$ qui par définition de τ est bien égal à $\tau\big(a + ker(\sigma)\big) \cdot \tau\big(b + ker(\sigma)\big)$.**

□