Anneaux - Décembre 2004

- *Quand il est nécessaire de justifier, votre argumentation doit convaincre le lecteur. En l'absence de justification dans un tel cas, le résultat final, même correct, n'a pas de valeur. Des expressions telles que « on voit bien que... » ne sont* pas *des justifications.*
- *Pensez à utiliser ce que vous savez de la théorie des groupes pour raccourcir les preuves.*

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,*

$$\forall a \in A \quad \forall b \in A \quad \forall c \in A \quad : \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{et} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

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 :*

Des exemples d'anneaux non-commutatifs sont :

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

Démonstration.

$\square$

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.

$\square$

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.

Lemme 7. *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.

$\square$

Définition 8. *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 9. ***Critère de sous-anneau***

Démonstration.

□

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

Définition 10. *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 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 11. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *un anneau commutatif, la fonction identité* $\sigma : A \to A$ *est un morphisme d'anneaux.*
Soit $\langle A, +, \cdot, 0, 1\rangle$ *et* $\langle B, +, \cdot, 0, 1\rangle$ *deux anneaux commutatifs, la fonction* $\sigma : A \to B$ *telle que* $\sigma(a) = 0$ *pour tout* $a \in A$ *est un morphisme d'anneaux.*

Lemme 12. *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.

$\square$

Lemme 13. *Soit* $\langle A, +, \cdot, 0, 1\rangle$ *et* $\langle B, +, \cdot, 0, 1\rangle$ *deux anneaux commutatifs et* $\sigma : A \rightarrow B$ *un morphisme d'anneaux,* $\langle Im(\sigma), +, \cdot, 0, 1\rangle$ *est un sous-anneau de* B.

Démonstration.

$\square$

Rappel 14. *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 15. *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 16. *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.

$\square$

Lemme 17. ***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.

$\square$

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

Démonstration.

$\square$

Théorème 19. *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.

$\square$

Théorème 20. *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 que $A/ker(\sigma)$ est isomorphe (en tant qu'anneau) à $Im(\sigma)$.*

Démonstration.

$\square$