CH3) Arithmétique dans un anneau principal

Dans tout ce document, $(A, +, \times)$ désigne un anneau **intègre.** On note A^* le groupe des unités de A (ne pas confondre avec le sous-ensemble $A \setminus \{0\}$).

1. Divisibilité dans un anneau intègre

Définition 1.1. *On note* $/_A$ *la relation sur* $A \setminus \{0\}$ *définie par :*

$$x /_A y \Leftrightarrow \exists z \in A \; y = zx$$

On dit alors que x ***divise*** y**,** *et que* y ***est un multiple de*** x**.**

Cette relation est un **préordre :** elle est réflexive, transitive, mais pas symétrique ni antisymétrique. En fait :

Lemme 1.2. *Soient* x*,* y *dans* $A \setminus \{0\}$*. Alors :*

$$(x /_A y \text{ et } y /_A x) \Leftrightarrow \exists u \in A^* \; y = xu$$

Démonstration. Par hypothèse, il existe u, v dans A tels que :

$$y = xu \text{ et } x = yv$$

Donc :

$$y = xu = yuv$$

D'où :

$$y(uv - 1) = 0$$

Comme $y \neq 0$ et A intègre, on obtient $uv = 1$: u (ainsi que v) est inversible, *i.e.* dans A^*. □

Corollaire 1.3. *Soit* $u \in A^*$*. Alors :*

$$\forall x \in A, \; x /_A u \Leftrightarrow x \in A^*$$

□

2. Anneau principal

Soit x un élément non-nul de A.

Théorème - Définition 2.1. *L'ensemble des multiples de* x *est un idéal de* A*. Il est noté* xA*.*

Un idéal de $(A, +, \times)$ *qui est de la forme* xA *est dit* ***principal****.* □

Exercice 2.2. *Montrer que* xA *est l'idéal engendré par* $\{x\}$*.*

Remarque 2.3. *La relation de divisibilité correspond à la relation d'inclusion entre idéaux. En effet :*

$$x /_A y \Leftrightarrow yA \subset xA$$

Lemme 2.4. *Soient* x*,* y *dans* A*. On a :*

$$xA = yA \Leftrightarrow \exists u \in A^* \; y = xu$$

□

Définition 2.5. *Si* $xA = yA$ *on dit que* x *et* y *sont* ***associés****.On note :*

$$x \sim y$$

Définition 2.6. *L' anneau $(A, +, \times)$ est **principal** si il est intègre et tout idéal de $(A, +, \times)$ est principal.*

Nous savons déjà que $(\mathbb{Z}, +, \times)$ est principal.

Proposition 2.7. *Soit I un idéal de $(A, +, \times)$. On suppose que $(A, +, \times)$ est principal. Alors, tout idéal de l'anneau quotient $(A/I, +, \times)$ est principal.*

Démonstration. Soit $p_I : A \to A/I$ la surjection canonique. Soit J un idéal de $(A/I, +, \times)$. Alors, $J' = (p_I)^{-1}(J)$ est un idéal de $(A, +, \times)$. Comme ce dernier est principal, il existe x dans A tel que :

$$J' = xA$$

On note $\bar{x} = p_I(x)$. Alors $\bar{x}$ appartient à $J = p_I(J')$. Donc :

$$\bar{x}(A/I) \subset J$$

Inversement, pour tout $\bar{y}$ dans J, il existe y dans J' tel que $p_I(y) = \bar{y}$. Comme $J' = xA$, y est un multiple de x : il existe z dans A tel que :

$$y = xz$$

Alors :

$$\bar{y} = p_I(y) = p_I(x)p_I(z) = \bar{x}p_I(z)$$

ce qui montre bien :

$$J \subset \bar{x}(A/I)$$

. □

3. Plus petit multiple commun, plus grand diviseur commun

3.1. **Plus petit multiple commun.** Nous avons déjà vu qu'une intersection d'idéal est un idéal. Dans un anneau principal, tout idéal est principal...

Définition 3.1. *Soit $(A, +, \times)$ un anneau principal. Soient a, b deux éléments de A. Tout élément qui engendre l'idéal $aA \cap bA$ est appelé **plus petit multiple commun à a et b.** On note :*

$$ppcm(a, b) \text{ ou } a \vee b$$

On a donc :

$$aA \cap bA = (a \vee b)A$$

Remarque 3.2. *Le ppcm n'est pas unique, mais il l'est modulo les unités. Plus précisément, si μ et μ' sont des ppcm de a et de b alors il existe une unité $u \in A^*$ telle que :*

$$\mu' = u\mu$$

Lemme 3.3. *Soit $(A, +, \times)$ un anneau principal. Soient a, b deux éléments de A. Un élément μ de A est un ppcm de a et b si et seulement :*

$$\begin{cases} a \,/_A\, \mu \text{ et } b \,/_A\, \mu & , \\ \forall x \in A, & a \,/_A\, x \text{ et } b \,/_A\, x \implies \mu \,/_A\, x \end{cases}$$

Démonstration. La première assertion signifie exactement que μ est dans $aA \cap bB$, et la seconde, que tout élément de $aA \cap bA$ est un multiple de μ, *i.e.* que μ engendre l'idéal $aA \cap bA$. □

Plus généralement :

Théorème - Définition 3.4. *Soit $(A,+,\times)$ un anneau principal. Soient $(a_i)_{1\leq i\leq n}$ une famille d'éléments de A. Tout élément qui engendre l'idéal $\bigcap_{1\leq i\leq n} a_i A$ est appelé* ***plus petit multiple commun aux*** *a_i. On note :*

$$ppcm(a_1,a_2,...,a_n) \text{ ou } a_1 \vee a_2 \vee ... \vee a_n$$

Il est caractérisé comme étant un élément μ de A tel que :

$$\begin{cases} \forall i & a_i \,/_A\, \mu \\ \forall x \in A, & (\forall i,\ a_i \,/_A\, x) \implies \mu \,/_A\, x \end{cases}$$

Il est défini modulo les unités de A. □

3.2. Plus grand diviseur commun.

Définition 3.5. *Soit $(A,+,\times)$ un anneau principal. Soient a, b deux éléments de A. Tout élément qui engendre l'idéal $aA+bA$ est appelé* ***plus grand diviseur commun à*** *a* ***et*** *b. On note :*

$$pgcd(a,b) \text{ ou } a \wedge b$$

On a donc :

Théorème 3.6 (de Bezout dans un anneau principal quelconque). *Soit $(A,+,\times)$ un anneau principal. Soient a, b deux éléments de A. Si un élément δ de A est un pgcd de a et de b alors :*

$$\exists u \in A\ \exists v \in A,\ \delta = au + by.$$

La réciproque est vraie si δ est inversible. □

Lemme 3.7. *Soit $(A,+,\times)$ un anneau principal. Soient a, b deux éléments de A. Un élément δ de A est un pgcd de a et b si et seulement :*

$$\begin{cases} \delta \,/_A\, a \text{ et } \delta \,/_A\, b & , \\ \forall x \in A, & x \,/_A\, a \text{ et } x \,/_A\, b \implies x \,/_A\, \delta \end{cases}$$

Démonstration. La première assertion signifie exactement que δ est dans l'idéal $aA+bA$ engendré par a et b, et la seconde, que tout élément de $aA+bA$ est un multiple de δ, *i.e.* que δ engendre l'idéal $aA+bA$. □

Plus généralement :

Théorème - Définition 3.8. *Soit $(A,+,\times)$ un anneau principal. Soient $(a_i)_{1\leq i\leq n}$ une famille d'éléments de A. Tout élément qui engendre l'idéal engendré par $\{a_1,a_2,...,a_n\}$ est appelé* ***plus grand diviseur commun aux*** *a_i. On note :*

$$pgcd(a_1,a_2,...,a_n) \text{ ou } a_1 \wedge a_2 \wedge ... \wedge a_n$$

Il est caractérisé comme étant un élément δ de A tel que :

$$\begin{cases} \forall i & \delta \,/_A\, a_i \\ \forall x \in A, & (\forall i,\ x \,/_A\, a_i) \implies x \,/_A\, \delta \end{cases}$$

Il est défini modulo les unités de A. □

3.3. Éléments premiers entre eux.

Définition 3.9. *Soit $(A,+,\times)$ un anneau principal. Soient a, b deux éléments de A. On dit que a* ***et*** *b* ***sont premiers entre eux*** *si :*

$$\forall d \in A,\ d \,/_A\, a \text{ et } d \,/_A\, b \implies d \in A^*$$

En d'autre termes, a et b sont premiers entre eux si leurs seuls diviseurs communs sont tous les inversibles (c'est à dire les éléments de A qui de toute manière divisent tous les éléments de A).

Clairement, deux éléments a et b sont premiers entre eux si et seulement leur pgcd est 1. En particulier :

Théorème 3.10. *Soit $(A, +, \times)$ un anneau principal. Soient a, b deux éléments de A. Alors, a et b sont premiers entre eux si et seulement si l'idéal $aA + bA$ qu'ils engendrent est A tout entier. Ceci équivaut à :*

$$\exists u, v \in A \;\; ux + vy = 1$$

□

4. Décomposition en facteurs premiers

4.1. Élément premier, élément irréductible.

Définition 4.1. *Un élément p de $A \setminus \{0\}$ est **irréductible** si :*

$$\begin{cases} p \notin A^*, \\ \forall a, b \in A, \quad p = ab \implies a \in A^* \text{ ou } b \in A^* \end{cases}$$

Lemme 4.2. *Soit $p \in A \setminus \{0\}$. Alors p est irréductible si et seulement si :*

$$\begin{cases} p \notin A^*, \\ \forall a, b \in A, \quad p = ab \implies p \sim a \text{ ou } p \sim b \end{cases}$$

□

Définition 4.3. *Un élément p de $A \setminus \{0\}$ est **premier** si :*

$$\begin{cases} p \notin A^*, \\ \forall a, b \in A, \quad p \,/_A\, ab \implies p \,/_A\, a \text{ ou } p \,/_A\, b \end{cases}$$

4.2. Équivalence premier-irréductible.

Théorème 4.4. *Soit $(A, +, \times)$ un anneau principal. Un élément de $A \setminus \{0\}$ est premier si et seulement si il est irréductible.*

Remarque 4.5. *L'implication premier $\implies$ irréductible est vraie dans tout anneau intègre, mais l'implication inverse utilise le fait que $(A, +, \times)$ est supposé principal.*

Démonstration. Soit $p \in A \setminus \{0\}$. On suppose $p \notin A^*$.

Si p est premier: Soient a, b tels que $p = ab$. Donc p divise a ou b ; disons qu'il divise a : $a = pa'$. Alors $p = pa'b$, d'où b inversible puisque A est intègre.

Si p est irréductible: Soient a, b tels que p divise ab. Soit d le pgcd de a et de p. Alors d divise p ainsi que a. Nous avons l'alternative suivante : soit d est inversible, soit il ne l'est pas. Dans le premier cas, a et p sont premiers entre eux, et il existe u, v tel que :

$$1 = au + pv$$

On multiplie les deux termes par b :

$$b = abu + pbv$$

Comme p divise ab, on voit qu'il divise b.

Dans l'autre cas, d n'est pas inversible. Comme p est irréductible, et que d divise p, c'est que d et p sont associés. En particulier, p divise a puisque d divise a.

□

4.3. **Décomposition en facteurs premiers : existence.**

Définition 4.6. *Soit a un élément non-nul de A. Une décomposition de a en facteurs irréductibles est la donnée d'un élément u de A^* et d' éléments irréductibles p_1, p_2, ... , p_n de A tels que :*

$$a = up_1p_2...p_n$$

Théorème 4.7. *Soit $(A, +, \times)$ un anneau principal. Alors, tout élément non nul de A admet une décomposition en facteurs irréductibles.*

Démonstration. Soit $\mathcal{A}$ l'ensemble des éléments de A qui admettent une décomposition en facteurs irréductibles. Supposons par l'absurde que $\mathcal{A}$ ne soit pas $A \setminus \{0\}$ tout entier, *i.e.* qu'il existe un élément a_1 non nul hors de $\mathcal{A}$. Alors, a_1 n'est pas irréductible. On peut donc l'écrire comme un produit de deux éléments non inversibles de A. De plus, si ces deux facteurs étaient dans $\mathcal{A}$, leur produit, a_1, serait aussi dans $\mathcal{A}$. Donc l'un d'entre eux n'est pas dans $\mathcal{A}$. On peut donc écrire :

$$a_1 = a_2\alpha_1$$

où $a_2 \notin \mathcal{A}$. En itérant l'argument, on construit par récurrence une suite $(a_n)_{n\in\mathbb{N}}$ telle que, pour tout n, on a :

$$\begin{cases} a_n = a_{n+1}\alpha_n, \\ a_{n+1} \notin \mathcal{A},\ \alpha_n \notin A^* \end{cases}$$

On voit que pour tout n, a_{n+1} divise a_n, et donc :

$$a_nA \subset a_{n+1}A$$

Les a_nA forment donc une suite croissante d'idéaux, dont l'union est donc un idéal de A. Comme A est principal, il existe $a_\infty \in A$ tel que :

$$a_\infty A = \bigcup_{n\geq 1} a_nA$$

D'une part, a_∞ divise tous les a_n (car $a_nA \subset a_\infty A_\infty$). Par ailleurs, a_∞ appartient à l'union des a_nA : il existe donc un entier n tel que $a_\infty \in a_nA$. Donc a_n divise a_∞.

D'après le lemme 1.2 a_∞ et a_n sont associés, et donc $a_nA = a_\infty A$. Donc :

$$a_nA \subset a_{n+1}A \subset a_\infty A = a_nA$$

On en déduit que a_n et a_{n+1} sont associés, mais c'est absurde puisque $\alpha_n \notin A^*$. □

4.4. **Décomposition en facteurs premiers : unicité.**

Théorème 4.8. *Soit $(A, +, \times)$ un anneau principal et a un élément non nul de A. Considérons deux décompositions de a en facteurs irréductibles :*

$$a = up_1p_2...p_n \text{ avec } u \in A^* \text{ et } p_1, p_2, \dots, p_n \text{ irréductibles}$$

et

$$a = vq_1q_2...q_m \text{ avec } v \in A^* \text{ et } q_1, q_2, \dots, q_m \text{ irréductibles}$$

Alors, $n = m$, et à une permutation des facteurs près, on a $p_i \sim q_i$ pour tout i.

Démonstration. Soit $P(n)$ l'assertion : *L'énoncé du théorème est vrai pour tout élément x de A qui admet une décomposition en facteurs irréductibles avec exactement n facteurs irréductibles.*

Nous allons montrer par récurence sur n que $P(n)$ est vraie pour tout $n \geq 0$, ce qui montrera le théorème.

Initialisation: Montrons $P(0)$: cette assertion signifie qu'un élément inversible ne peut être multiple d'un élément irréductible. Ceci découle du Corollaire 1.3 (puisque par définition, un irréductible n'est pas inversible).

Hérédité: Supposons que $P(n-1)$ est vrai, avec $n \geq 1$, et montrons $P(n)$. Soit donc a un élément de A admettant une décomposition avec exactement n facteurs irréductibles :

$$a = up_1p_2...p_n$$

Soit $a = vq_1q_2...q_m$ une autre décomposition en facteurs irréductibles. Le terme p_n de la première décomposition divise a, et donc $vq_1q_2...q_m$. Comme p_n est irréductible, il est premier. Donc il divise soit q_m, soit $vq_1q_2...q_{m-1}$. Si on est dans le second cas, on itère l'argument : p_n divise soit q_{m-1}, soit $vq_1q_2...q_{m-2}$. De proche en proche, on montre que soit p_n divise un des q_i soit il divise v. Mais cette dernière alternative est impossible d'après le Corollaire 1.3.

On a donc montré que p_n divise un des q_i, disons, quitte à permuter les q_i, qu'il divise q_m. On a donc $q_m = p_n\alpha$. Comme q_m est irréductible et que p_n n'est pas inversible, α est une unité. Donc, $p_n \sim q_m$, et :

$$up_1p_2...p_{n-1} = (v\alpha)q_1q_2...q_{m-1}$$

Le facteur $v\alpha$ est inversible, donc on a égalité entre deux décompositions en facteurs irréductibles, une des décompositions faisant intervenir $n-1$ facteurs irréductibles. Par hypothèse de récurrence $P(n-1)$, on a $m-1 = n-1$, *i.e.* $m = n$, et, après permutation des facteurs, chaque p_i est associé à q_i. Donc $P(n)$ est vrai.

□