Chapitre 3 : Arithmétique dans un anneau principal

L3-S5. Algèbre générale 1

Licence Mathématiques
Université d'Avignon

Année 2018–2019

I. Divisibilité dans un anneau intègre

1. Multiples et diviseurs

$(A, +, \times)$ désigne un anneau (commutatif) **intègre.** On note $U(A)$ le groupe des unités de A.

Définition : Divisibilité

Soit $x, y \in A$. On dit que x *divise* y ou que y *est un multiple de* x si

$$\exists z \in A,\ y = xz.$$

On note alors $x\big|_A y$ ou simplement $x|y$.

I. Divisibilité dans un anneau intègre

1. Multiples et diviseurs

$(A, +, \times)$ désigne un anneau (commutatif) **intègre.** On note $U(A)$ le groupe des unités de A.

Définition : Divisibilité

Soit $x, y \in A$. On dit que x *divise* y ou que y *est un multiple de* x si

$$\exists z \in A, \; y = xz.$$

On note alors $x|_A y$ ou simplement $x|y$.

Exemples

1. 1_A divise x et x divise x.
2. x divise 0 (rem. $0|x \iff x = 0$).

Remarques.

❶ La relation $\,|_A\,$ sur $A \setminus \{0\}$ est un *préordre :* elle est réflexive, transitive, mais pas symétrique ni antisymétrique. Cependant :

Lemme

Soit x, y dans $A \setminus \{0\}$. Alors :

$$(x|_A y \ \text{ et } \ y|_A x) \iff \exists u \in U(A),\ y = xu$$

Remarques.

❶ La relation $|_A$ sur $A \setminus \{0\}$ est un *préordre :* elle est réflexive, transitive, mais pas symétrique ni antisymétrique. Cependant :

Lemme

Soit x, y dans $A \setminus \{0\}$. Alors :

$$(x|_A y \text{ et } y|_A x) \iff \exists u \in U(A),\ y = xu$$

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

$$x|_A y \iff y \in xA \iff yA \subset xA.$$

Remarques.

❶ La relation $|_A$ sur $A \setminus \{0\}$ est un *préordre :* elle est réflexive, transitive, mais pas symétrique ni antisymétrique. Cependant :

Lemme

Soit x, y dans $A \setminus \{0\}$. Alors :

$$(x|_A y \text{ et } y|_A x) \iff \exists u \in U(A),\ y = xu$$

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

$$x|_A y \iff y \in xA \iff yA \subset xA.$$

❸ Soit $u \in U(A)$. Alors, pour tout $x \in A$,

$$x|_A u \iff x \in U(A).$$

2. Eléments associés

Définition

Soit $x, y \in A$. On dit que x *est associé à* y si x et y se divisent mutuellement. On note $x \sim y$.

C'est une relation d'équivalence.

2. Eléments associés

Définition

Soit $x, y \in A$. On dit que x *est associé à* y si x et y se divisent mutuellement. On note $x \sim y$.

C'est une relation d'équivalence.

Théorème

Soit $x, y \in A$. On a

$$x \sim y \iff xA = yA \iff (\exists u \in U(A),\ y = xu).$$

Deux éléments associés ont les mêmes multiples et les mêmes diviseurs.

2. Eléments associés

Définition

Soit $x, y \in A$. On dit que x *est associé à* y si x et y se divisent mutuellement. On note $x \sim y$.

C'est une relation d'équivalence.

Théorème

Soit $x, y \in A$. On a

$$x \sim y \iff xA = yA \iff (\exists u \in U(A),\ y = xu).$$

Deux éléments associés ont les mêmes multiples et les mêmes diviseurs.

Exemple

Dans $\mathbb{Z}$, $x \sim y \iff |x| = |y|$.

II. Anneau principal

Soit x un élément non-nul de l'anneau commutatif A. Rappelons que l'idéal engendré par x

$$xA \overset{\text{déf.}}{=} \{xu/u \in A\}$$

est le plus petit idéal de A contenant x. C'est aussi l'ensemble des multiples de x.

Définition : Idéal principal

Un idéal I de A est dit *principal* s'il existe un élément $x \in A$ tel que $I = xA$.

II. Anneau principal

Soit x un élément non-nul de l'anneau commutatif A. Rappelons que l'idéal engendré par x

$$xA \overset{\text{déf.}}{=} \{xu/u \in A\}$$

est le plus petit idéal de A contenant x. C'est aussi l'ensemble des multiples de x.

Définition : Idéal principal

Un idéal I de A est dit *principal* s'il existe un élément $x \in A$ tel que $I = xA$.

Définition : Anneau principal

L'anneau A est dit *principal* s'il est intègre et si tous ses idéaux sont principaux.

L'anneau $\mathbb{Z}$ est principal : les idéaux de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}, n \in \mathbb{N}$.

Proposition

Soit $(A, +, \times)$ un anneau principal et I un idéal de A. Alors, tout idéal de l'anneau quotient $(A/I, +, \times)$ est principal.

Proposition

Soit $(A, +, \times)$ un anneau principal et I un idéal de A. Alors, tout idéal de l'anneau quotient $(A/I, +, \times)$ est principal.

Attention, l'anneau quotient A/I n'étant pas forcément intègre, il n'est pas forcément principal.

Proposition

Soit $(A, +, \times)$ un anneau principal et I un idéal de A. Alors, tout idéal de l'anneau quotient $(A/I, +, \times)$ est principal.

Attention, l'anneau quotient A/I n'étant pas forcément intègre, il n'est pas forcément principal.

Exemple

Les idéaux de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ sont principaux mais si n est non nul et non premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal car il n'est pas intègre.

Proposition

Soit $(A, +, \times)$ un anneau principal et I un idéal de A. Alors, tout idéal de l'anneau quotient $(A/I, +, \times)$ est principal.

Attention, l'anneau quotient A/I n'étant pas forcément intègre, il n'est pas forcément principal.

Exemple

Les idéaux de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ sont principaux mais si n est non nul et non premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal car il n'est pas intègre.
Par contre, si n est un nombre premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc il est intègre et c'est donc un anneau principal.

III. PPCM, PGCD

1. Plus petit multiple commun

Définition

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

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

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

III. PPCM, PGCD

1. Plus petit multiple commun

Définition

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

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

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

Le ppcm n'est pas unique, mais il l'est modulo les unités.

Plus précisément, si m et m' sont des ppcm de a et b alors il existe une unité $u \in U(A)$ telle que $m' = um$, autrement dit m et m' sont associés.

Exemple

Dans $\mathbb{Z}$, tout couple d'entiers admet deux ppcm, m et $-m$. En imposant au ppcm d'être dans $\mathbb{N}$, on a l'unicité.

Exemple

Dans $\mathbb{Z}$, tout couple d'entiers admet deux ppcm, m et $-m$. En imposant au ppcm d'être dans $\mathbb{N}$, on a l'unicité.

Lemme

Soit $(A, +, \times)$ un anneau principal et $a, b, m \in A$. Alors

$$m \sim \operatorname{ppcm}(a, b) \iff \begin{cases} a|m \ , \ b|m, \\ \forall x \in A, \ a|x \ \text{ et } \ b|x \implies m|x \end{cases}$$

Tout générateur m de $aA \cap bA$ est un multiple commun à a et b, et c'est “le plus petit” au sens de la divisibilité.

Plus généralement :

Théorème - Définition

Soit $(A,+,\times)$ un anneau principal et $(a_i)_{1\leqslant i\leqslant n}$ une famille d'éléments de A. Tout élément qui engendre l'idéal $\bigcap\limits_{1\leqslant i\leqslant n} a_iA$ est appelé *plus petit multiple commun aux* a_i. On note :

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

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

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

Il est défini modulo les unités de A.

2. Plus grand diviseur commun

Définition

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

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

On a donc $aA + bA = (a \wedge b)A$.

2. Plus grand diviseur commun

Définition

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

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

On a donc $aA + bA = (a \wedge b)A$.

Le pgcd n'est pas unique, mais il l'est modulo les unités.

Plus précisément, si d et d' sont des pgcd de a et de b alors il existe une unité $u \in U(A)$ telle que $d' = ud$.

2. Plus grand diviseur commun

Définition

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

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

On a donc $aA + bA = (a \wedge b)A$.

Le pgcd n'est pas unique, mais il l'est modulo les unités.
Plus précisément, si d et d' sont des pgcd de a et de b alors il existe une unité $u \in U(A)$ telle que $d' = ud$.

Exemple

Dans $\mathbb{Z}$, tout couple d'entiers admet deux pgcd, d et $-d$. En imposant au pgcd d'être dans $\mathbb{N}$, on a l'unicité.

Identité de Bezout dans un anneau principal

Soit $(A, +, \times)$ un anneau principal et $a, b, d \in A$. Si d est un pgcd de a et b alors :

$$\exists u, v \in A,\ d = au + bv.$$

La réciproque est vraie si $d|a$ et $d|b$, en particulier si d est inversible.

Identité de Bezout dans un anneau principal

Soit $(A, +, \times)$ un anneau principal et $a, b, d \in A$. Si d est un pgcd de a et b alors :

$$\exists u, v \in A,\ d = au + bv.$$

La réciproque est vraie si $d|a$ et $d|b$, en particulier si d est inversible.

Lemme

Soit $(A, +, \times)$ un anneau principal et $a, b, d \in A$. Alors

$$d \sim \text{pgcd}(a, b) \iff \begin{cases} d|a \ \text{ et } \ d|b, \\ \forall x \in A,\ x|a \text{ et } x|b \implies x|d \end{cases}$$

Tout générateur d de $aA + bA$ est un diviseur commun à a et b, et c'est “le plus grand” au sens de la divisibilité.

Plus généralement :

Théorème - Définition

Soit $(A,+,\times)$ un anneau principal et $(a_i)_{1\leqslant i\leqslant n}$ une famille d'éléments de A. Tout élément qui engendre l'idéal $a_1A+a_2A+\cdots+a_nA$ est appelé *plus grand diviseur commun aux* a_i. On note :

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

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

$$\begin{cases} \forall i,\ d|a_i \\ \forall x\in A,\ (\forall i,\ x|a_i) \implies x|d \end{cases}$$

Il est défini modulo les unités de A. □

3. Éléments premiers entre eux

Définition

Soit $(A, +, \times)$ un anneau principal et $a, b \in A$. On dit que *a et b sont premiers entre eux* si :

$$\forall d \in A,\ d|a \ \text{ et } \ d|b \implies d \in U(A)$$

En d'autres termes, a et b sont premiers entre eux si leurs diviseurs communs sont tous inversibles, ce qui équivaut à : ils admettent un pgcd inversible, soit encore 1 est un pgcd de a et b.

3. Éléments premiers entre eux

Définition

Soit $(A, +, \times)$ un anneau principal et $a, b \in A$. On dit que *a et b sont premiers entre eux* si :

$$\forall d \in A,\ d|a \ \text{ et } \ d|b \implies d \in U(A)$$

En d'autres termes, a et b sont premiers entre eux si leurs diviseurs communs sont tous inversibles, ce qui équivaut à : ils admettent un pgcd inversible, soit encore 1 est un pgcd de a et b.

Exemple

Dans $\mathbb{Z}$, deux entiers a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1.

Théorème de Bezout

Soit $(A,+,\times)$ un anneau principal et $a,b\in A$. Alors, a et b sont premiers entre eux si et seulement si $aA+bA=A$, ce qui équivaut à :

$$\exists u,v\in A,\ au+bv=1$$

IV. Décomposition en facteurs premiers

1. Élément premier, élément irréductible

Définition : élément irréductible

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

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p = ab \implies a \in U(A) \ \text{ ou } \ b \in U(A) \end{cases}$$

IV. Décomposition en facteurs premiers

1. Élément premier, élément irréductible

Définition : élément irréductible

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

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p = ab \implies a \in U(A) \text{ ou } b \in U(A) \end{cases}$$

Remarques.

① Le “ou” est exclusif : un seul des éléments a, b appartient à $U(A)$.

IV. Décomposition en facteurs premiers

1. Élément premier, élément irréductible

Définition : élément irréductible

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

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p = ab \implies a \in U(A) \ \text{ ou } \ b \in U(A) \end{cases}$$

Remarques.

① Le “ou” est exclusif : un seul des éléments a, b appartient à $U(A)$.

② Tout élément de A associé à un élément irréductible dans A est encore irréductible dans A.

IV. Décomposition en facteurs premiers

1. Élément premier, élément irréductible

Définition : élément irréductible

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

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p = ab \implies a \in U(A) \ \text{ ou } \ b \in U(A) \end{cases}$$

Remarques.

① Le "ou" est exclusif : un seul des éléments a, b appartient à $U(A)$.

② Tout élément de A associé à un élément irréductible dans A est encore irréductible dans A.

③ Exemple simple : 3 est irréductible dans $\mathbb{Z}$ mais pas dans $\mathbb{Q}$.

Lemme

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

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p = ab \implies p \sim a \ \text{ ou } \ p \sim b \end{cases}$$

L'élément p est irréductible si et seulement si les seuls diviseurs de p sont les unités ou les associés à p.

Définition : élément premier

Un élément $p \in A \setminus \{0\}$ est *premier* si :

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p|ab \implies p|a \ \text{ ou } \ p|b \end{cases}$$

Tout élément de A associé à un élément premier dans A est encore premier dans A.

Définition : élément premier

Un élément $p \in A \setminus \{0\}$ est *premier* si :

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p|ab \implies p|a \quad \text{ou} \quad p|b \end{cases}$$

Tout élément de A associé à un élément premier dans A est encore premier dans A.

Exemples

- $1_A \in A$ n'est pas premier car $1_A \in U(A)$. Les unités d'un anneau ne sont pas des éléments premiers.

Définition : élément premier

Un élément $p \in A \setminus \{0\}$ est *premier* si :

$$\begin{cases} p \notin U(A) \\ \forall a, b \in A,\ p|ab \implies p|a \ \text{ ou } \ p|b \end{cases}$$

Tout élément de A associé à un élément premier dans A est encore premier dans A.

Exemples

- $1_A \in A$ n'est pas premier car $1_A \in U(A)$. Les unités d'un anneau ne sont pas des éléments premiers.
- Dans $\mathbb{Z}$, les éléments premiers sont les nombres premiers (i.e. les entiers naturels admettant exactement deux diviseurs distincts entiers et positifs) et leurs opposés.

2. Équivalence premier-irréductible

Théorème

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

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

Contre-exemple

Dans l'anneau $\mathbb{Z}[i\sqrt{5}] \overset{\text{déf.}}{=} \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$, l'élément 3 est irréductible mais non premier.

3. Décomposition en facteurs premiers

Définition

Une *décomposition de* $a \in A \backslash \{0\}$ *en facteurs irréductibles* est la donnée d'un élément u de $U(A)$ et d'éléments irréductibles $p_1, p_2, \dots, p_n$ de A tels que $a = up_1p_2 \dots p_n$.

3. Décomposition en facteurs premiers

Définition

Une *décomposition de* $a \in A\backslash\{0\}$ *en facteurs irréductibles* est la donnée d'un élément u de $U(A)$ et d'éléments irréductibles $p_1, p_2, \ldots, p_n$ de A tels que $a = up_1p_2\ldots p_n$.

Théorème d'existence et d'unicité

Soit $(A, +, \times)$ un anneau principal.
Existence : Tout élément de $A\backslash\{0\}$ admet une décomposition en facteurs irréductibles.

3. Décomposition en facteurs premiers

Définition

Une *décomposition de* $a \in A\backslash\{0\}$ *en facteurs irréductibles* est la donnée d'un élément u de $U(A)$ et d'éléments irréductibles $p_1, p_2, \ldots, p_n$ de A tels que $a = up_1p_2 \ldots p_n$.

Théorème d'existence et d'unicité

Soit $(A, +, \times)$ un anneau principal.
Existence : Tout élément de $A\backslash\{0\}$ admet une décomposition en facteurs irréductibles.
Unicité : Soit $a \in A\backslash\{0\}$. Considérons deux décompositions de a en facteurs irréductibles :

$a = up_1p_2 \cdots p_n$ avec $u \in U(A)$ et $p_1, p_2, \ldots, p_n$ irréductibles

$a = vq_1q_2 \cdots q_m$ avec $v \in U(A)$ et $q_1, q_2, \ldots, q_m$ irréductibles.

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