Cours Algèbre 2 – IV: Anneaux principaux, euclidiens, factoriels

Andrei Teleman

Département de Mathématiques, Aix-Marseille Université

19 mars 2021

Table of Contents

Table of Contents

1

Définition 1.1

Soit A un anneau commutatif intègre et soient $a, b \in A$. On dit que a divise b (ou que a est un diviseur de b, ou que b est un multiple de a) dans A, s'il existe $q \in A$ tel que $b = aq$.

Définition 1.1

Soit A un anneau commutatif intègre et soient $a, b \in A$. On dit que a divise b (ou que a est un diviseur de b, ou que b est un multiple de a) dans A, s'il existe $q \in A$ tel que $b = aq$.

Remarque 1.2

Un élément inversible $u \in A$ divise tout élément $b \in A$.

1

Définition 1.1

Soit A un anneau commutatif intègre et soient $a, b \in A$. On dit que a divise b (ou que a est un diviseur de b, ou que b est un multiple de a) dans A, s'il existe $q \in A$ tel que $b = aq$.

Remarque 1.2

Un élément inversible $u \in A$ divise tout élément $b \in A$.

Définition 1.3

Soit $a, b \in A$. On dit que a et b sont associés s'il existe un élément inversible $u \in A$ tel que $b = au$.

Exemples 1.1

Deux éléments $a, b \in \mathbb{Z}$ sont associés si et seulement si $b = \pm a$, donc si et seulement si $|a| = |b|$.

2

Exemples 1.1

Deux éléments $a, b \in \mathbb{Z}$ sont associés si et seulement si $b = \pm a$, donc si et seulement si $|a| = |b|$.
Deux polynômes $P(X), Q(X) \in K[X]$ sont associés si et seulement s'il existe $a \in K^*$ tel que $Q(X) = aP(X)$.

2

Exemples 1.1

Deux éléments $a, b \in \mathbb{Z}$ sont associés si et seulement si $b = \pm a$, donc si et seulement si $|a| = |b|$.
Deux polynômes $P(X), Q(X) \in K[X]$ sont associés si et seulement s'il existe $a \in K^*$ tel que $Q(X) = aP(X)$.

Remarque 1.4

Soit A un anneau commutatif intègre.

1. Deux éléments $a, b \in A$ sont associés si et seulement si $a|b$ et $b|a$.
2. La relation sur A définie par la condition "a et b sont associés" est une relation d'équivalence sur A.

Dém: Exercice. Attention aux cas ou $a = 0_A$ ou $b = 0_A$. ∎

Rappelons que, pour un élément $a \in A$ on a noté par (a) l'idéal principal aA engendré par a.

3

Rappelons que, pour un élément $a \in A$ on a noté par (a) l'idéal principal aA engendré par a.

Proposition 1.5

Soient A un anneau commutatif intègre et $a, b \in A$.

1. $a|b$ si et seulement si $(b) \subset (a)$.
2. $(b) = (a)$ si et seulement si a et b sont associés.

Dém: Exercice. ∎

Soit A un anneau commutatif intègre.

Définition 1.6

1. Un élément $p \in A \setminus \{0\}$ est dit irréductible s'il n'est pas inversible et pour toute décomposition $p = bc$, on a soit $b \in A^\times$, soit $c \in A^\times$.

Soit A un anneau commutatif intègre.

Définition 1.6

1. Un élément $p \in A \setminus \{0\}$ est dit irréductible s'il n'est pas inversible et pour toute décomposition $p = bc$, on a soit $b \in A^\times$, soit $c \in A^\times$.
   Equivalent : $p \in A \setminus \{0\}$ est irréductible s'il n'est pas inversible et ses seuls diviseurs sont les éléments inversibles et les éléments qui lui sont associés.

4

Soit A un anneau commutatif intègre.

Définition 1.6

1. Un élément $p \in A \setminus \{0\}$ est dit irréductible s'il n'est pas inversible et pour toute décomposition $p = bc$, on a soit $b \in A^\times$, soit $c \in A^\times$.
   Equivalent : $p \in A \setminus \{0\}$ est irréductible s'il n'est pas inversible et ses seuls diviseurs sont les éléments inversibles et les éléments qui lui sont associés.
2. Un élément $p \in A \setminus \{0\}$ est dit premier s'il n'est pas inversible et l'implication suivante est vraie : $p|bc \Rightarrow p|b \vee p|c$.

5

Remarque 1.7

Soit A un anneau commutatif intègre.

1. Tout élément premier de A est irréductible.

Remarque 1.7

Soit A un anneau commutatif intègre.

1. Tout élément premier de A est irréductible.
2. Un élément $p \in A \setminus \{0\}$ est premier si et seulement si l'idéal principal $(p) = pA$ engendré par p est un idéal premier.

Remarque 1.7

Soit A un anneau commutatif intègre.

1. Tout élément premier de A est irréductible.
2. Un élément $p \in A \setminus \{0\}$ est premier si et seulement si l'idéal principal $(p) = pA$ engendré par p est un idéal premier.

Dém: 1. Soient $p \in A \setminus \{0\}$ premier, $p = bc$ décomposition de p.

Remarque 1.7

Soit A un anneau commutatif intègre.

1. Tout élément premier de A est irréductible.
2. Un élément $p \in A \setminus \{0\}$ est premier si et seulement si l'idéal principal $(p) = pA$ engendré par p est un idéal premier.

Dém: 1. Soient $p \in A \setminus \{0\}$ premier, $p = bc$ décomposition de p.

On a donc $p|bc$, donc (p étant premier) $p|b$ ou $p|c$.

Remarque 1.7

Soit A un anneau commutatif intègre.

1. Tout élément premier de A est irréductible.
2. Un élément $p \in A \setminus \{0\}$ est premier si et seulement si l'idéal principal $(p) = pA$ engendré par p est un idéal premier.

Dém: 1. Soient $p \in A \setminus \{0\}$ premier, $p = bc$ décomposition de p.

On a donc $p|bc$, donc (p étant premier) $p|b$ ou $p|c$.

Supposons $p|b$, i.e. $\exists q \in A$ tel que $b = pq$. On obtient :

$$p = pqc \Rightarrow p(1 - qc) = 0 \overset{A \text{ intègre}}{\Longrightarrow} qc = 1 \Rightarrow c \in A^{\times}.$$

Remarque 1.7

Soit A un anneau commutatif intègre.

1. Tout élément premier de A est irréductible.
2. Un élément $p \in A \setminus \{0\}$ est premier si et seulement si l'idéal principal $(p) = pA$ engendré par p est un idéal premier.

Dém: 1. Soient $p \in A \setminus \{0\}$ premier, $p = bc$ décomposition de p.

On a donc $p|bc$, donc (p étant premier) $p|b$ ou $p|c$.

Supposons $p|b$, i.e. $\exists q \in A$ tel que $b = pq$. On obtient :

$$p = pqc \Rightarrow p(1 - qc) = 0 \overset{A \text{ intègre}}{\Longrightarrow} qc = 1 \Rightarrow c \in A^{\times}.$$

2. Exercice.

Exemples 1.2

1. Un entier $k \in \mathbb{Z}$ est irréductible si et seulement si k est premier, si et seulement si $|k|$ est un nombre premier au sens élémentaire.

Exemples 1.2

1. Un entier $k \in \mathbb{Z}$ est irréductible si et seulement si k est premier, si et seulement si $|k|$ est un nombre premier au sens élémentaire.
2. Un polynôme $P(X) \in \mathbb{C}[X]$ est irréductible si et seulement si il est premier, si et seulement si $\deg(P(X)) = 1$.

Exemples 1.2

1. Un entier $k \in \mathbb{Z}$ est irréductible si et seulement si k est premier, si et seulement si $|k|$ est un nombre premier au sens élémentaire.
2. Un polynôme $P(X) \in \mathbb{C}[X]$ est irréductible si et seulement si il est premier, si et seulement si $\deg(P(X)) = 1$.
3. Un polynôme $P(X) \in \mathbb{R}[X]$ est irréductible si et seulement si il est premier, si et seulement si soit $\deg(P(X)) = 1$, soit $\deg(P(X)) = 2$ et son discriminant est strictement négatif.

Exemples 1.2

1. Un entier $k \in \mathbb{Z}$ est *irréductible* si et seulement si k est *premier*, si et seulement si $|k|$ est un nombre premier au sens élémentaire.
2. Un polynôme $P(X) \in \mathbb{C}[X]$ est *irréductible* si et seulement si il est *premier*, si et seulement si $\deg(P(X)) = 1$.
3. Un polynôme $P(X) \in \mathbb{R}[X]$ est *irréductible* si et seulement si il est *premier*, si et seulement si soit $\deg(P(X)) = 1$, soit $\deg(P(X)) = 2$ et son discriminant est strictement négatif.

On va voir : l'équivalence (premier $\Leftrightarrow$ irréductible) reste vraie dans tout anneau factoriel, en particulier dans tout anneau principal.

Mais, en général, dans un anneau intègre, l'implication (irréductible $\Rightarrow$ premier) est fausse :

Mais, en général, dans un anneau intègre, l'implication (irréductible $\Rightarrow$ premier) est fausse :

Proposition 1.8

Considérons

$$\mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} \mid a,\ b \in \mathbb{Z}\}$$

muni de sa structure de sous-anneau de $\mathbb{C}$.
Dans cet anneau 3 est irréductible, mais n'est pas premier.

Mais, en général, dans un anneau intègre, l'implication (irréductible $\Rightarrow$ premier) est fausse :

Proposition 1.8

Considérons

$$\mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} |\ a,\ b \in \mathbb{Z}\}$$

muni de sa structure de sous-anneau de $\mathbb{C}$.
Dans cet anneau 3 est irréductible, mais n'est pas premier.

Pour montrer que 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: on va utiliser l'application $z \mapsto |z|^2$.

Mais, en général, dans un anneau intègre, l'implication (irréductible $\Rightarrow$ premier) est fausse :

Proposition 1.8

Considérons

$$\mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} |\ a,\ b \in \mathbb{Z}\}$$

muni de sa structure de sous-anneau de $\mathbb{C}$.
Dans cet anneau 3 est irréductible, mais n'est pas premier.

Pour montrer que 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: on va utiliser l'application $z \mapsto |z|^2$.

Pour montrer que 3 n'est pas premier dans $\mathbb{Z}[i\sqrt{5}]$:
$3|(2+i\sqrt{5})(2-i\sqrt{5})$, mais 3 ne divise aucun des deux facteurs.

Dém: 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: Soit

$$(a + ib\sqrt{5})(\alpha + i\beta\sqrt{5}) = 3 \tag{1}$$

une décomposition de 3 dans $\mathbb{Z}[i\sqrt{5}]$.

8

Dém: 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: Soit

$$(a+ib\sqrt{5})(\alpha+i\beta\sqrt{5})=3 \tag{1}$$

une décomposition de 3 dans $\mathbb{Z}[i\sqrt{5}]$.
On peut supposer $b\neq 0$, $\beta\neq 0$, sinon (1) sera décomposition dans $\mathbb{Z}$ et 3 est irréductible dans $\mathbb{Z}$.

Dém: 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: Soit

$$(a+ib\sqrt{5})(\alpha+i\beta\sqrt{5})=3 \tag{1}$$

une décomposition de 3 dans $\mathbb{Z}[i\sqrt{5}]$.
On peut supposer $b\neq 0$, $\beta\neq 0$, sinon (1) sera décomposition dans $\mathbb{Z}$ et 3 est irréductible dans $\mathbb{Z}$.

En comparant les modules au carré on obtient

$$(a^2+5b^2)(\alpha^2+5\beta^2)=9$$

qui est impossible car $(a^2+5b^2)\geq 5$, $(\alpha^2+5\beta^2)\geq 5$.

8

Dém: 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: Soit

$$(a + ib\sqrt{5})(\alpha + i\beta\sqrt{5}) = 3 \tag{1}$$

une décomposition de 3 dans $\mathbb{Z}[i\sqrt{5}]$.
On peut supposer $b \neq 0$, $\beta \neq 0$, sinon (1) sera décomposition dans $\mathbb{Z}$ et 3 est irréductible dans $\mathbb{Z}$.

En comparant les modules au carré on obtient

$$(a^2 + 5b^2)(\alpha^2 + 5\beta^2) = 9$$

qui est impossible car $(a^2 + 5b^2) \geq 5$, $(\alpha^2 + 5\beta^2) \geq 5$.

3 n'est pas premier dans $\mathbb{Z}[i\sqrt{5}]$: $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$, donc 3 divise ce produit. Mais

8

Dém: 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: Soit

$$(a + ib\sqrt{5})(\alpha + i\beta\sqrt{5}) = 3 \tag{1}$$

une décomposition de 3 dans $\mathbb{Z}[i\sqrt{5}]$.
On peut supposer $b \neq 0$, $\beta \neq 0$, sinon (1) sera décomposition dans $\mathbb{Z}$ et 3 est irréductible dans $\mathbb{Z}$.

En comparant les modules au carré on obtient

$$(a^2 + 5b^2)(\alpha^2 + 5\beta^2) = 9$$

qui est impossible car $(a^2 + 5b^2) \geq 5$, $(\alpha^2 + 5\beta^2) \geq 5$.

3 n'est pas premier dans $\mathbb{Z}[i\sqrt{5}]$: $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$, donc 3 divise ce produit. Mais

3 ne divise ni $2 + i\sqrt{5}$, ni $2 - i\sqrt{5}$: remarquer $\frac{2 \pm i\sqrt{5}}{3} \notin \mathbb{Z}[i\sqrt{5}]$. ∎

Table of Contents

Rappel : Soient A un anneau commutatif et $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x \mid x \in A\} \subset A$$

est un idéal de $(A, +, \cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Rappel : Soient A un anneau commutatif et $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x |\, x \in A\} \subset A$$

est un idéal de $(A, +, \cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Définition 2.1

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

9

Rappel : Soient A un anneau commutatif et $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x \mid x \in A\} \subset A$$

est un idéal de $(A, +, \cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Définition 2.1

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} \mid n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal.

Rappel : Soient A un anneau commutatif et $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x | \, x \in A\} \subset A$$

est un idéal de $(A, +, \cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Définition 2.1

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} | \, n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal.

En utilisant le TDE pour les polynômes à coefficients dans un corps on va démontrer que l'anneau $K[X]$ est aussi principal.

Soient A un anneau principal et $a_1, \ldots, a_n \in A$.

Soient A un anneau principal et $a_1, \ldots, a_n \in A$.

But : comprendre l'ensemble $\mathrm{Div}(a_1, \ldots, a_n) \subset A$ des diviseurs communs de $a_1, \ldots, a_n$.

10

Soient A un anneau principal et $a_1, \ldots, a_n \in A$.

But : comprendre l'ensemble $\mathrm{Div}(a_1, \ldots, a_n) \subset A$ des diviseurs communs de $a_1, \ldots, a_n$.

Considérons l'idéal

$$(a_1, \ldots, a_n) = a_1 A + \ldots + a_n A \subset A$$

engendré par les a_i.

10

Soient A un anneau principal et $a_1,\dots,a_n \in A$.

But : comprendre l'ensemble $\mathrm{Div}(a_1,\dots,a_n) \subset A$ des diviseurs communs de $a_1,\dots,a_n$.

Considérons l'idéal

$$(a_1,\dots,a_n) = a_1A + \dots + a_nA \subset A$$

engendré par les a_i.
Puisque A est un anneau principal, il existe $d \in A$ tel que

$$(a_1,\dots,a_n) = (d)$$

et d est unique à la multiplication près par un élément inversible de A.

11

Proposition 2.2

Soit d un générateur de l'idéal $(a_1, \ldots, a_n)$. Alors

$$\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d),$$

donc d est un diviseur commun des éléments $a_1, \ldots, a_n$ et l'ensemble des diviseurs communs des éléments $a_1, \ldots, a_n$ coïncide avec l'ensemble des diviseurs de d.

Proposition 2.2

Soit d un générateur de l'idéal $(a_1,\dots,a_n)$. Alors

$$\mathrm{Div}(a_1,\dots,a_n)=\mathrm{Div}(d),$$

donc d est un diviseur commun des éléments $a_1,\dots,a_n$ et l'ensemble des diviseurs communs des éléments $a_1,\dots,a_n$ coïncide avec l'ensemble des diviseurs de d.

Dém: $(a_i)\subset(a_1,\dots,a_n)=(d)$. Il en résulte $d|a_i$ pour $1\leq i\leq n$, donc d est un diviseur commun des a_i. Ceci implique $\mathrm{Div}(d)\subset\mathrm{Div}(a_1,\dots,a_n)$.

11

Proposition 2.2

Soit d un générateur de l'idéal $(a_1, \ldots, a_n)$. Alors

$$\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d),$$

donc d est un diviseur commun des éléments $a_1, \ldots, a_n$ et l'ensemble des diviseurs communs des éléments $a_1, \ldots, a_n$ coïncide avec l'ensemble des diviseurs de d.

Dém: $(a_i) \subset (a_1, \ldots, a_n) = (d)$. Il en résulte $d | a_i$ pour $1 \leq i \leq n$, donc d est un diviseur commun des a_i. Ceci implique $\mathrm{Div}(d) \subset \mathrm{Div}(a_1, \ldots, a_n)$.

Réciproquement soit $\delta \in \mathrm{Div}(a_1, \ldots, a_n)$. Donc δ divise tout élément de la forme $\sum_{i=1}^n a_i x_i$, donc tout élément de $(a_1, \ldots, a_n)$. Mais $d \in (a_1, \ldots, a_n)$, donc $\delta | d$, c'est à dire $\delta \in \mathrm{Div}(d)$. ∎

Définition 2.3

Un générateur d de l'idéal $(a_1,\ldots,a_n)$ s'appelle un pgcd des éléments $a_1,\ldots,a_n$ et est noté $\mathrm{pgcd}(a_1,\ldots,a_n)$.

12

Définition 2.3

Un générateur d de l'idéal $(a_1,\dots,a_n)$ s'appelle un pgcd des éléments $a_1,\dots,a_n$ et est noté $\mathrm{pgcd}(a_1,\dots,a_n)$.

Dans la théorie des anneaux principaux le pgcd d'un ensemble fini $\{a_1,\dots,a_n\}$ est unique seulement à la multiplication près par un élément inversible de A, donc deux pgcd des éléments $\{a_1,\dots,a_n\}$ sont associés.

Définition 2.3

Un générateur d de l'idéal $(a_1,\ldots,a_n)$ s'appelle un pgcd des éléments $a_1,\ldots,a_n$ et est noté $\mathrm{pgcd}(a_1,\ldots,a_n)$.

Dans la théorie des anneaux principaux le pgcd d'un ensemble fini $\{a_1,\ldots,a_n\}$ est unique seulement à la multiplication près par un élément inversible de A, donc deux pgcd des éléments $\{a_1,\ldots,a_n\}$ sont associés.

L'égalité $(a_1,\ldots,a_n)=(d)$ écrite sous la forme

$$a_1A+\ldots+a_nA=dA \tag{2}$$

s'appelle l'égalité ou l'identité de Bézout.

Définition 2.4

Les éléments $a_1, \ldots, a_n \in A$ sont dits premiers entre eux dans leur ensemble s'ils admettent 1 pour pgcd. Les éléments $a_1, \ldots, a_n \in A$ sont dits premiers entre eux deux à deux si $\mathrm{pgcd}(a_i, a_j) = 1$ pour $i \neq j$.

Définition 2.4

Les éléments $a_1,\dots,a_n\in A$ sont dits premiers entre eux dans leur ensemble s'ils admettent 1 pour pgcd. Les éléments $a_1,\dots,a_n\in A$ sont dits premiers entre eux deux à deux si $\mathrm{pgcd}(a_i,a_j)=1$ pour $i\neq j$.

Théorème 2.5

(le théorème de Bézout pour les anneaux principaux) Soient A un anneau principal $a_1,\dots,a_n\in A$. Sont équivalentes :

1. $a_1,\dots,a_n$ sont premiers entre eux dans leur ensemble.
2. Il existe des éléments $u_1,\dots,u_n\in A$ tels que $\sum_{i=1}^n a_i u_i = 1_A$.

Dém: Exercice. ∎

Corollaire 2.6

Soient $a, b, c \in A$. Si a est premier avec b et c, alors il est aussi premier avec bc.

Corollaire 2.6

Soient $a, b, c \in A$. Si a est premier avec b et c, alors il est aussi premier avec bc.

Dém: En utilisant l'égalité de Bézout on obtient des éléments $u_1, u_2, v_1, v_2 \in A$ tels que

$$au_1 + bu_2 = 1_A, \ av_1 + cv_2 = 1_A.$$

Corollaire 2.6

Soient $a, b, c \in A$. Si a est premier avec b et c, alors il est aussi premier avec bc.

Dém: En utilisant l'égalité de Bézout on obtient des éléments $u_1, u_2, v_1, v_2 \in A$ tels que

$$au_1 + bu_2 = 1_A,\ av_1 + cv_2 = 1_A.$$

En multipliants les deux égalités on obtient une égalité de la forme $aU + bcV = 1_A$, donc a et bc sont premiers entre eux. ■

Corollaire 2.6

Soient $a, b, c \in A$. Si a est premier avec b et c, alors il est aussi premier avec bc.

Dém: En utilisant l'égalité de Bézout on obtient des éléments $u_1, u_2, v_1, v_2 \in A$ tels que

$$au_1 + bu_2 = 1_A, \; av_1 + cv_2 = 1_A.$$

En multipliants les deux égalités on obtient une égalité de la forme $aU + bcV = 1_A$, donc a et bc sont premiers entre eux. ■

Corollaire 2.7 (Th. de Gauss dans les anneaux principaux)

Soient $a, b, x \in A$ t. q. $a|bx$. Si a est premier avec b, alors $a|x$

Dém: Exercice. Voir le théorème de Gauss dans $\mathbb{Z}$. ■

Corollaire 2.8

Soient A un anneau principal, $a \in A$ et $b_1, \dots, b_n \in A$ premiers entre eux deux à deux. Si $b_i | a$ pour $1 \leq i \leq n$, alors $b_1 \dots b_n | a$.

Corollaire 2.8

Soient A un anneau principal, $a \in A$ et $b_1, \dots, b_n \in A$ premiers entre eux deux à deux. Si $b_i | a$ pour $1 \leq i \leq n$, alors $b_1 \dots b_n | a$.

Dém: Supposons d'abord $n = 2$. Puisque $b_1 | a$ il existe $q \in A$ tel que $a = b_1 q$.

Corollaire 2.8

Soient A un anneau principal, $a \in A$ et $b_1, \dots, b_n \in A$ premiers entre eux deux à deux. Si $b_i | a$ pour $1 \leq i \leq n$, alors $b_1 \dots b_n | a$.

Dém: Supposons d'abord $n = 2$. Puisque $b_1 | a$ il existe $q \in A$ tel que $a = b_1 q$.

Puisque $b_2 | b_1 q$ et b_1, b_2 sont premiers entre eux, il en résulte $b_2 | q$, donc il existe $c \in A$ tel que $q = b_2 c$.

Corollaire 2.8

Soient A un anneau principal, $a \in A$ et $b_1, \ldots, b_n \in A$ premiers entre eux deux à deux. Si $b_i | a$ pour $1 \leq i \leq n$, alors $b_1 \ldots b_n | a$.

Dém: Supposons d'abord $n = 2$. Puisque $b_1 | a$ il existe $q \in A$ tel que $a = b_1 q$.

Puisque $b_2 | b_1 q$ et b_1, b_2 sont premiers entre eux, il en résulte $b_2 | q$, donc il existe $c \in A$ tel que $q = b_2 c$.

On obtient $a = b_1 q = b_1 b_2 c$, donc $b_1 b_2 | a$.

Corollaire 2.8

Soient A un anneau principal, $a \in A$ et $b_1, \dots, b_n \in A$ premiers entre eux deux à deux. Si $b_i | a$ pour $1 \leq i \leq n$, alors $b_1 \dots b_n | a$.

Dém: Supposons d'abord $n = 2$. Puisque $b_1 | a$ il existe $q \in A$ tel que $a = b_1 q$.

Puisque $b_2 | b_1 q$ et b_1, b_2 sont premiers entre eux, il en résulte $b_2 | q$, donc il existe $c \in A$ tel que $q = b_2 c$.

On obtient $a = b_1 q = b_1 b_2 c$, donc $b_1 b_2 | a$.

Pour le cas général on se réduit au cas $n = 2$ en utilisant la récurrence par rapport à n. ∎

Proposition 2.9

Soit A un anneau principal et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Proposition 2.9

Soit A un anneau principal et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$.

Proposition 2.9

Soit A un anneau principal et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$.

p irréductible $\Rightarrow (\mathrm{pgcd}(p,b) = p) \vee (\mathrm{pgcd}(p,b) = 1)$.

Proposition 2.9

Soit A un anneau principal et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$.

p irréductible $\Rightarrow (\mathrm{pgcd}(p,b) = p) \vee (\mathrm{pgcd}(p,b) = 1)$.

Dans le premier cas il en résulte $p|b$ et dans le deuxième (en utilisant le théorème de Gauss) on obtient $p|c$. ∎

Proposition 2.9

Soit A un anneau principal et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$.

p irréductible $\Rightarrow (\mathrm{pgcd}(p,b) = p) \vee (\mathrm{pgcd}(p,b) = 1)$.

Dans le premier cas il en résulte $p|b$ et dans le deuxième (en utilisant le théorème de Gauss) on obtient $p|c$. ■

Exercice 2.1

Énoncer et démontrer le théorème des restes chinois dans un anneau principal.

17

Soient $a_1, \ldots, a_n \in A$. But : l'ensemble $\mathrm{Mult}(a_1, \ldots, a_n)$ des multiples communs des a_i.

17

Soient $a_1,\ldots,a_n \in A$. But : l'ensemble $\mathrm{Mult}(a_1,\ldots,a_n)$ des multiples communs des a_i.

L'ensemble des multiples de a_i est (a_i), donc

$$\mathrm{Mult}(a_1,\ldots,a_n) = (a_1) \cap \ldots \cap (a_n),$$

en particulier $\mathrm{Mult}(a_1,\ldots,a_n)$ est un idéal de A.

17

Soient $a_1,\dots,a_n \in A$. But : l'ensemble $\mathrm{Mult}(a_1,\dots,a_n)$ des multiples communs des a_i.

L'ensemble des multiples de a_i est (a_i), donc

$$\mathrm{Mult}(a_1,\dots,a_n) = (a_1)\cap\dots\cap(a_n),$$

en particulier $\mathrm{Mult}(a_1,\dots,a_n)$ est un idéal de A.

A principal $\Rightarrow \exists m \in A$ t.q. $(a_1)\cap\dots\cap(a_n) = (m)$ et m est unique à multiplication près par un élément inversible. Donc

17

Soient $a_1,\ldots,a_n \in A$. But : l'ensemble $\mathrm{Mult}(a_1,\ldots,a_n)$ des multiples communs des a_i.

L'ensemble des multiples de a_i est (a_i), donc

$$\mathrm{Mult}(a_1,\ldots,a_n) = (a_1) \cap \ldots \cap (a_n),$$

en particulier $\mathrm{Mult}(a_1,\ldots,a_n)$ est un idéal de A.

A principal $\Rightarrow \exists m \in A$ t.q. $(a_1) \cap \ldots \cap (a_n) = (m)$ et m est unique à multiplication près par un élément inversible. Donc

Remarque 2.10

Soient $a_1,\ldots,a_n \in A$ et soit m un générateur de l'intersection $(a_1) \cap \ldots \cap (a_n)$. Alors $\mathrm{Mult}(a_1,\ldots,a_n) = (m)$, donc l'ensemble des multiples communs de a_i coïncide avec l'ideal principal engendré par m.

Définition 2.11

Un générateur m de l'idéal $(a_1)\cap\ldots\cap(a_n)$ s'appelle un ppcm des éléments $a_1,\ldots,a_n\in A$ et est noté $\mathrm{ppcm}(a_1,\ldots,a_n)$.

Définition 2.11

Un générateur m de l'idéal $(a_1) \cap \ldots \cap (a_n)$ s'appelle un ppcm des éléments $a_1, \ldots, a_n \in A$ et est noté $\mathrm{ppcm}(a_1, \ldots, a_n)$.

Comme le pgcd, le ppcm est unique à multiplication près par un élément inversible.

18

Définition 2.11

Un générateur m de l'idéal $(a_1) \cap \ldots \cap (a_n)$ s'appelle un ppcm des éléments $a_1, \ldots, a_n \in A$ et est noté $\mathrm{ppcm}(a_1, \ldots, a_n)$.

Comme le pgcd, le ppcm est unique à multiplication près par un élément inversible.

Proposition 2.12

Soient $a, b \in A$. Alors

$$\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b) = ab$$

à multiplication près par un élément inversible.

Dém: Soient $d := \mathrm{pgcd}(a, b)$, $m := \mathrm{ppcm}(a, b)$. On peut supposer $d \neq 0_A$. Pourquoi ? Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$.

Dém: Soient $d := \mathrm{pgcd}(a,b)$, $m := \mathrm{ppcm}(a,b)$. On peut supposer $d \neq 0_A$. Pourquoi ? Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$.

En utilisant l'égalité et le théorème de Bézout : a', b' sont premiers entre eux.

19

Dém: Soient $d := \mathrm{pgcd}(a, b)$, $m := \mathrm{ppcm}(a, b)$. On peut supposer $d \neq 0_A$. Pourquoi ? Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$.

En utilisant l'égalité et le théorème de Bézout : a', b' sont premiers entre eux.

On va démontrer $(a'b'd) = (m)$.

Dém: Soient $d := \mathrm{pgcd}(a,b)$, $m := \mathrm{ppcm}(a,b)$. On peut supposer $d \neq 0_A$. Pourquoi ? Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$.

En utilisant l'égalité et le théorème de Bézout : a', b' sont premiers entre eux.

On va démontrer $(a'b'd) = (m)$.

Pour l'inclusion $(a'b'd) \subset (m)$, remarquons que le produit $a'b'd = b'a = a'b$ est un multiple commun de a et b, donc appartient à l'idéal (m). On a donc $(a'b'd) \subset (m)$.

Dém: Soient $d := \mathrm{pgcd}(a,b)$, $m := \mathrm{ppcm}(a,b)$. On peut supposer $d \neq 0_A$. Pourquoi ? Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$.

En utilisant l'égalité et le théorème de Bézout : a', b' sont premiers entre eux.

On va démontrer $(a'b'd) = (m)$.

Pour l'inclusion $(a'b'd) \subset (m)$, remarquons que le produit $a'b'd = b'a = a'b$ est un multiple commun de a et b, donc appartient à l'idéal (m). On a donc $(a'b'd) \subset (m)$.

Pour l'inclusion inverse, soient $u, v \in A$ tels que $m = ua = vb$. Ceci implique $ua'd = vb'd$.

Dém: Soient $d := \mathrm{pgcd}(a,b)$, $m := \mathrm{ppcm}(a,b)$. On peut supposer $d \neq 0_A$. Pourquoi ? Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$.

En utilisant l'égalité et le théorème de Bézout : a', b' sont premiers entre eux.

On va démontrer $(a'b'd) = (m)$.

Pour l'inclusion $(a'b'd) \subset (m)$, remarquons que le produit $a'b'd = b'a = a'b$ est un multiple commun de a et b, donc appartient à l'idéal (m). On a donc $(a'b'd) \subset (m)$.

Pour l'inclusion inverse, soient $u, v \in A$ tels que $m = ua = vb$. Ceci implique $ua'd = vb'd$.

A est intègre, donc

$$ua'd = vb'd \overset{d \neq 0_A}{\Longrightarrow} ua' = vb'.$$

Puisque a', b' sont premiers entre eux, le théorème de Gauss donne $b'|u$, donc il existe $w \in A$ tel que $u = wb'$.

Puisque a', b' sont premiers entre eux, le théorème de Gauss donne $b'|u$, donc il existe $w \in A$ tel que $u = wb'$.

On obtient $m = wb'a = wb'a'd$, donc $m \in (b'a'd)$, soit $(m) \subset (b'a'd)$.

Puisque a', b' sont premiers entre eux, le théorème de Gauss donne $b'|u$, donc il existe $w \in A$ tel que $u = wb'$.

On obtient $m = wb'a = wb'a'd$, donc $m \in (b'a'd)$, soit $(m) \subset (b'a'd)$.

L'égalité annoncée $(a'b'd) = (m)$ est donc démontrée.

20

Puisque a', b' sont premiers entre eux, le théorème de Gauss donne $b'|u$, donc il existe $w \in A$ tel que $u = wb'$.

On obtient $m = wb'a = wb'a'd$, donc $m \in (b'a'd)$, soit $(m) \subset (b'a'd)$.

L'égalité annoncée $(a'b'd) = (m)$ est donc démontrée.

D'après la proposition 1.5 il existe un élément inversible $s \in A$ tel que $m = a'b'ds$, d'où $md = a'db'ds = abs$. ∎

Table of Contents

Soit A un anneau commutatif intègre, l'élément nul est noté 0.

Définition 3.1

Un stathme euclidien sur A est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ vérifiant les deux propriétés

1. $\forall (a,b) \in A \times (A \setminus \{0\})\ \exists (q,r) \in A \times A$ tels que
   - (i) $a = bq + r$ et
   - (ii) soit $r = 0$, soit $r \neq 0$ et $\nu(r) < \nu(b)$.

21

Soit A un anneau commutatif intègre, l'élément nul est noté 0.

Définition 3.1

Un stathme euclidien sur A est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ vérifiant les deux propriétés

1. $\forall (a,b) \in A \times (A \setminus \{0\})\ \exists (q,r) \in A \times A$ tels que
   - (i) $a = bq + r$ et
   - (ii) soit $r = 0$, soit $r \neq 0$ et $\nu(r) < \nu(b)$.
2. $\forall (a,b) \in (A \setminus \{0\}) \times (A \setminus \{0\}),\ \nu(a) \leq \nu(ab)$.

21

Soit A un anneau commutatif intègre, l'élément nul est noté 0.

Définition 3.1

Un stathme euclidien sur A est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ vérifiant les deux propriétés

1. $\forall (a,b) \in A \times (A \setminus \{0\})\ \exists (q,r) \in A \times A$ tels que
   - (i) $a = bq + r$ et
   - (ii) soit $r = 0$, soit $r \neq 0$ et $\nu(r) < \nu(b)$.
2. $\forall (a,b) \in (A \setminus \{0\}) \times (A \setminus \{0\}),\ \nu(a) \leq \nu(ab)$.

Dans la définition d'un stathme euclidien on ne requiert pas l'unicité du couple (q,r)!

Soit A un anneau commutatif intègre, l'élément nul est noté 0.

Définition 3.1

Un stathme euclidien sur A est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ vérifiant les deux propriétés

1. $\forall (a,b) \in A \times (A \setminus \{0\})\ \exists (q,r) \in A \times A$ tels que
   - (i) $a = bq + r$ et
   - (ii) soit $r = 0$, soit $r \neq 0$ et $\nu(r) < \nu(b)$.
2. $\forall (a,b) \in (A \setminus \{0\}) \times (A \setminus \{0\}),\ \nu(a) \leq \nu(ab)$.

Dans la définition d'un stathme euclidien on ne requiert pas l'unicité du couple (q,r)!

Définition 3.2

Un anneau intègre A est dit euclidien s'il existe un stathme euclidien sur A.

Exemples 3.1 (d'anneaux euclidiens)

1. $\mathbb{Z}$. En effet, l'application $\mathbb{Z} \setminus \{0\} \to \mathbb{N}$ donnée par $k \mapsto |k|$ est un stathme euclidien sur l'anneau $\mathbb{Z}$.

Exemples 3.1 (d'anneaux euclidiens)

1. $\mathbb{Z}$. En effet, l'application $\mathbb{Z} \setminus \{0\} \to \mathbb{N}$ donnée par $k \mapsto |k|$ est un stathme euclidien sur l'anneau $\mathbb{Z}$.
2. L'anneau des polynômes $K[X]$ où K est un corps. En effet, l'application $K[X] \setminus \{0\} \to \mathbb{N}$ donnée par $P(X) \mapsto \deg(P(X))$ est un stathme euclidien sur l'anneau $K[X]$.

Exemples 3.1 (d'anneaux euclidiens)

1. $\mathbb{Z}$. En effet, l'application $\mathbb{Z}\setminus\{0\}\to\mathbb{N}$ donnée par $k\mapsto |k|$ est un stathme euclidien sur l'anneau $\mathbb{Z}$.
2. L'anneau des polynômes $K[X]$ où K est un corps. En effet, l'application $K[X]\setminus\{0\}\to\mathbb{N}$ donnée par $P(X)\mapsto \deg(P(X))$ est un stathme euclidien sur l'anneau $K[X]$.

Théorème 3.3 (l'anneau des entiers de Gauss)

Soit $\mathbb{Z}[i] := \{u+iv \mid u,\ v\in\mathbb{Z}\}$ muni de sa structure de sous-anneau de $\mathbb{C}$. L'application

$$\nu:\mathbb{Z}[i]\setminus\{0\}\to\mathbb{N},\ \nu(u+iv)=u^2+v^2$$

est un stathme euclidien sur $\mathbb{Z}[i]$. En particulier $\mathbb{Z}[i]$ est un anneau euclidien.

23

On va utiliser un lemme de géométrie élémentaire.

Lemme 3.4

Soit $x \in \mathbb{R}^2$. Il existe $x' \in \mathbb{Z}^2$ tel que $d(x, x') < 1$.

Dém: Exercice. ∎

On va utiliser un lemme de géométrie élémentaire.

Lemme 3.4

Soit $x \in \mathbb{R}^2$. Il existe $x' \in \mathbb{Z}^2$ tel que $d(x, x') < 1$.

Dém: Exercice. ∎

Dém: (du théorème) Nous avons l'identité $\nu(ab) = \nu(a)\nu(b)$, donc ν vérifie la 2me condition dans la définition d'un stathme.

On va utiliser un lemme de géométrie élémentaire.

Lemme 3.4

Soit $x \in \mathbb{R}^2$. Il existe $x' \in \mathbb{Z}^2$ tel que $d(x, x') < 1$.

Dém: Exercice. ■

Dém: (du théorème) Nous avons l'identité $\nu(ab) = \nu(a)\nu(b)$, donc ν vérifie la 2me condition dans la définition d'un stathme.

Pour la 1re condition : Soient

$$a = u + iv, \; b = s + it \in \mathbb{Z}[i] \text{ avec } b \neq 0.$$

On va utiliser un lemme de géométrie élémentaire.

Lemme 3.4

Soit $x \in \mathbb{R}^2$. Il existe $x' \in \mathbb{Z}^2$ tel que $d(x, x') < 1$.

Dém: Exercice. ∎

Dém: (du théorème) Nous avons l'identité $\nu(ab) = \nu(a)\nu(b)$, donc ν vérifie la 2me condition dans la définition d'un stathme.

Pour la 1re condition : Soient

$$a = u + iv, \ b = s + it \in \mathbb{Z}[i] \text{ avec } b \neq 0.$$

À montrer l'existence d'un couple $(q, r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ t. q.

$$a = qb + r \text{ avec } r = 0 \text{ ou } (r \neq 0 \text{ et } \nu(r) < \nu(b)).$$

On va utiliser un lemme de géométrie élémentaire.

Lemme 3.4

Soit $x \in \mathbb{R}^2$. Il existe $x' \in \mathbb{Z}^2$ tel que $d(x, x') < 1$.

Dém: Exercice. ∎

Dém: (du théorème) Nous avons l'identité $\nu(ab) = \nu(a)\nu(b)$, donc ν vérifie la 2me condition dans la définition d'un stathme.

Pour la 1re condition : Soient

$$a = u + iv,\ b = s + it \in \mathbb{Z}[i] \text{ avec } b \neq 0.$$

À montrer l'existence d'un couple $(q, r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ t. q.

$$a = qb + r \text{ avec } r = 0 \text{ ou } (r \neq 0 \text{ et } \nu(r) < \nu(b)).$$

On applique le lemme à $z := \frac{a}{b} \in \mathbb{C}$ (qui s'identifie à $\mathbb{R}^2$).

Il existe $q \in \mathbb{Z}[i]$ tel que $d(z,q) < 1$, i.e. tel que $|z-q| < 1$.

Il existe $q \in \mathbb{Z}[i]$ tel que $d(z, q) < 1$, i.e. tel que $|z - q| < 1$.

On obtient $|\frac{a}{b} - q|^2 < 1$, donc $|a - qb|^2 < |b|^2$.

Il existe $q \in \mathbb{Z}[i]$ tel que $d(z,q) < 1$, i.e. tel que $|z - q| < 1$.

On obtient $|\frac{a}{b} - q|^2 < 1$, donc $|a - qb|^2 < |b|^2$.

Posons $r := a - qb \in \mathbb{Z}[i]$.

Il existe $q \in \mathbb{Z}[i]$ tel que $d(z, q) < 1$, i.e. tel que $|z - q| < 1$.

On obtient $|\frac{a}{b} - q|^2 < 1$, donc $|a - qb|^2 < |b|^2$.

Posons $r := a - qb \in \mathbb{Z}[i]$. Avec ce choix on a bien $a = qb + r$.

Il existe $q \in \mathbb{Z}[i]$ tel que $d(z,q) < 1$, i.e. tel que $|z - q| < 1$.

On obtient $|\frac{a}{b} - q|^2 < 1$, donc $|a - qb|^2 < |b|^2$.

Posons $r := a - qb \in \mathbb{Z}[i]$. Avec ce choix on a bien $a = qb + r$.

Si $r \neq 0$, l'inégalité $|a - qb|^2 < |b|^2$ devient $\nu(r) < \nu(b)$, donc le couple (q,r) trouvé satisfait les conditions requises. ∎

Il existe $q \in \mathbb{Z}[i]$ tel que $d(z, q) < 1$, i.e. tel que $|z - q| < 1$.

On obtient $|\frac{a}{b} - q|^2 < 1$, donc $|a - qb|^2 < |b|^2$.

Posons $r := a - qb \in \mathbb{Z}[i]$. Avec ce choix on a bien $a = qb + r$.

Si $r \neq 0$, l'inégalité $|a - qb|^2 < |b|^2$ devient $\nu(r) < \nu(b)$, donc le couple (q, r) trouvé satisfait les conditions requises. ∎

Théorème 3.5

Tout anneau euclidien est principal.

Dém: Soient A un anneau euclidien et $\nu : A \setminus \{0\} \to \mathbb{N}$ un stathme euclidien sur A. Soit $I \subset A$ un idéal de A. On peut supposer $I \neq \{0\}$.

Posons

$$m := \min\left\{\nu(x) \mid x \in I \setminus \{0\}\right\}.$$

et soit $a \in I \setminus \{0\}$ tel que $\nu(a) = m$.

Posons

$$m := \min\left\{\nu(x) |\ x \in I \setminus \{0\}\right\}.$$

et soit $a \in I \setminus \{0\}$ tel que $\nu(a) = m$.

Nous allons montrer que $I = (a)$. Puisque $a \in I$, l'inclusion $(a) \subset I$ est évidente.

Posons

$$m := \min\left\{\nu(x) | \, x \in I \setminus \{0\}\right\}.$$

et soit $a \in I \setminus \{0\}$ tel que $\nu(a) = m$.

Nous allons montrer que $I = (a)$. Puisque $a \in I$, l'inclusion $(a) \subset I$ est évidente.

Pour l'autre inclusion, soit $x \in I$. Puisque ν est un stathme euclidien sur A, il existe $(q, r) \in A \times A$ tel que $x = aq + r$ avec $r = 0$ ou $\nu(r) < \nu(a) = m$.

Posons

$$m := \min\left\{\nu(x) | \, x \in I \setminus \{0\}\right\}.$$

et soit $a \in I \setminus \{0\}$ tel que $\nu(a) = m$.

Nous allons montrer que $I = (a)$. Puisque $a \in I$, l'inclusion $(a) \subset I$ est évidente.

Pour l'autre inclusion, soit $x \in I$. Puisque ν est un stathme euclidien sur A, il existe $(q, r) \in A \times A$ tel que $x = aq + r$ avec $r = 0$ ou $\nu(r) < \nu(a) = m$.

Dans l'égalité $x = aq + r$ nous avons $x \in I$ et $aq \in I$, donc $r \in I$. Nous affirmons que $r = 0$.

Posons

$$m := \min\left\{\nu(x) \mid x \in I \setminus \{0\}\right\}.$$

et soit $a \in I \setminus \{0\}$ tel que $\nu(a) = m$.

Nous allons montrer que $I = (a)$. Puisque $a \in I$, l'inclusion $(a) \subset I$ est évidente.

Pour l'autre inclusion, soit $x \in I$. Puisque ν est un stathme euclidien sur A, il existe $(q, r) \in A \times A$ tel que $x = aq + r$ avec $r = 0$ ou $\nu(r) < \nu(a) = m$.

Dans l'égalité $x = aq + r$ nous avons $x \in I$ et $aq \in I$, donc $r \in I$. Nous affirmons que $r = 0$.

Par l'absurde : sinon, on aurait $r \in I \setminus \{0\}$ et $\nu(r) < m$, ce qui contredit la définition de m. Donc $r = 0$, d'où $x = aq \in (a)$. ∎

Corollaire 3.6

Les anneaux

1. $\mathbb{Z}$,
2. $K[X]$ (où K est un corps),
3. $\mathbb{Z}[i]$

sont des anneaux euclidiens, donc principaux.

Corollaire 3.6

Les anneaux

1. $\mathbb{Z}$,
2. $K[X]$ (où K est un corps),
3. $\mathbb{Z}[i]$

sont des anneaux euclidiens, donc principaux.

Exemple 3.1

L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal, mais n'est pas euclidien (voir TD).

Table of Contents

Définition 4.1

Soit A un anneau intègre. A est dit anneau factoriel si les deux propriétés suivantes sont vérifiées :

1. Pour tout $a \in A$, non nul et non inversible, il existe une suite finie $(p_1, \dots, p_m)$ d'éléments irréductibles de A telle que $a = \prod_{i=1}^m p_i$.

Définition 4.1

Soit A un anneau intègre. A est dit anneau factoriel si les deux propriétés suivantes sont vérifiées :

1. Pour tout $a \in A$, non nul et non inversible, il existe une suite finie $(p_1, \dots, p_m)$ d'éléments irréductibles de A telle que $a = \prod_{i=1}^{m} p_i$.
2. Soient $(p_1, \dots, p_m)$, $(q_1, \dots, q_n)$ deux suites finies d'éléments irréductibles de A telles que $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$. Alors $n = m$ et il existe une permutation σ de l'ensemble $\{1, \dots, m\}$ telle que pour tout i les éléments p_i, $q_{\sigma(i)}$ sont associés.

Définition 4.1

Soit A un anneau intègre. A est dit anneau factoriel si les deux propriétés suivantes sont vérifiées :

1. Pour tout $a \in A$, non nul et non inversible, il existe une suite finie $(p_1, \ldots, p_m)$ d'éléments irréductibles de A telle que $a = \prod_{i=1}^{m} p_i$.
2. Soient $(p_1, \ldots, p_m)$, $(q_1, \ldots, q_n)$ deux suites finies d'éléments irréductibles de A telles que $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$. Alors $n = m$ et il existe une permutation σ de l'ensemble $\{1, \ldots, m\}$ telle que pour tout i les éléments p_i, $q_{\sigma(i)}$ sont associés.

Donc A est dit factoriel si tout $a \in A$, non nul et non inversible, se décompose en produit d'irréductibles et la décomposition est unique à l'ordre des facteurs et à association près.

Remarque 4.2

Soient A un anneau factoriel, $(p_1, \dots, p_m)$ une suite finie d'éléments irréductibles de A et p un élément irréductible de A tel que $p \mid \prod_{i=1}^m p_i$. Alors il existe i tel que p est associé avec p_i.

Remarque 4.2

Soient A un anneau factoriel, $(p_1, \ldots, p_m)$ une suite finie d'éléments irréductibles de A et p un élément irréductible de A tel que $p \mid \prod_{i=1}^m p_i$. Alors il existe i tel que p est associé avec p_i.

Dém: Soit $b \in A$ tel que $a := \prod_{i=1}^m p_i = bp$. Si b est inversible, alors $m = 1$ et p est associé avec p_1.

Remarque 4.2

Soient A un anneau factoriel, $(p_1, \ldots, p_m)$ une suite finie d'éléments irréductibles de A et p un élément irréductible de A tel que $p \mid \prod_{i=1}^{m} p_i$. Alors il existe i tel que p est associé avec p_i.

Dém: Soit $b \in A$ tel que $a := \prod_{i=1}^{m} p_i = bp$. Si b est inversible, alors $m = 1$ et p est associé avec p_1.

Si b n'est pas inversible, on le décompose en facteurs irréductibles et on introduit cette décomposition dans le produit bp. On obtient une nouvelle décomposition de a en facteurs irréductibles (dans laquelle p figure).

Remarque 4.2

Soient A un anneau factoriel, $(p_1, \ldots, p_m)$ une suite finie d'éléments irréductibles de A et p un élément irréductible de A tel que $p \mid \prod_{i=1}^m p_i$. Alors il existe i tel que p est associé avec p_i.

Dém: Soit $b \in A$ tel que $a := \prod_{i=1}^m p_i = bp$. Si b est inversible, alors $m = 1$ et p est associé avec p_1.

Si b n'est pas inversible, on le décompose en facteurs irréductibles et on introduit cette décomposition dans le produit bp. On obtient une nouvelle décomposition de a en facteurs irréductibles (dans laquelle p figure).

D'après l'unicité de la décomposition : p est associé avec un p_i.

■

Proposition 4.3

Soit A un anneau factoriel et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Proposition 4.3

Soit A un anneau factoriel et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$.

Proposition 4.3

Soit A un anneau factoriel et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$. Puisque A est factoriel, on peut décomposer b et c en produits de facteurs irréductibles :

$$b = \prod_{i=1}^{m} p_i ,\ c = \prod_{j=1}^{n} q_j .$$

Proposition 4.3

Soit A un anneau factoriel et soit $p \in A$. Sont équivalentes :

1. p est irréductible.
2. p est premier.

Dém: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$. Puisque A est factoriel, on peut décomposer b et c en produits de facteurs irréductibles :

$$b = \prod_{i=1}^{m} p_i, \ c = \prod_{j=1}^{n} q_j .$$

Alors $bc = (\prod_{i=1}^m p_i)(\prod_{j=1}^n q_j)$. D'après la remarque précédente p est associé avec l'un des facteurs p_i ou avec l'un des facteurs q_j. Donc $p|b$ ou $p|c$. ∎

Corollaire 4.4

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.
2. Tout élément non nul et non inversible de A s'écrit comme produit d'éléments premiers.

Dém: Exercice. ∎

30

Corollaire 4.4

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.
2. Tout élément non nul et non inversible de A s'écrit comme produit d'éléments premiers.

Dém: Exercice. ∎

Soit A un anneau commutatif. Une suite $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est dite croissante si $I_n \subset I_{n+1}$ pour tout $n \in \mathbb{N}$.

Corollaire 4.4

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.
2. Tout élément non nul et non inversible de A s'écrit comme produit d'éléments premiers.

Dém: Exercice. ∎

Soit A un anneau commutatif. Une suite $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est dite croissante si $I_n \subset I_{n+1}$ pour tout $n \in \mathbb{N}$.

Une suite croissante d'idéaux est dite stationnaire s'il existe $k \in \mathbb{N}$ tel que pour tout $n \geq k$ on a $I_n = I_k$.

Remarque 4.5

Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors la réunion $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.

Remarque 4.5

Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors la réunion $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.

Remarque 4.6

Soient A un anneau principal. Toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est stationnaire.

Dém: A est principal $\Rightarrow$ la réunion $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal principal. Soit a un générateur de I.

Remarque 4.5

Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors la réunion $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.

Remarque 4.6

Soient A un anneau principal. Toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est stationnaire.

Dém: A est principal $\Rightarrow$ la réunion $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal principal. Soit a un générateur de I.

Il existe $k \in \mathbb{N}$ tel que $a \in I_k$, d'où $I = (a) \subset I_k$.

Remarque 4.5

Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors la réunion $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.

Remarque 4.6

Soient A un anneau principal. Toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est stationnaire.

Dém: A est principal $\Rightarrow$ la réunion $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal principal. Soit a un générateur de I.

Il existe $k \in \mathbb{N}$ tel que $a \in I_k$, d'où $I = (a) \subset I_k$.

Mais aussi $I_k \subset \bigcup_{n\in\mathbb{N}} I_n = I$. En conclusion $I = I_k$.

Remarque 4.5

Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors la réunion $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.

Remarque 4.6

Soient A un anneau principal. Toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est stationnaire.

Dém: A est principal $\Rightarrow$ la réunion $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal principal. Soit a un générateur de I.

Il existe $k \in \mathbb{N}$ tel que $a \in I_k$, d'où $I = (a) \subset I_k$.

Mais aussi $I_k \subset \bigcup_{n\in\mathbb{N}} I_n = I$. En conclusion $I = I_k$.

Pour $n \geq k$ on a $I_k \subset I_n \subset I$, donc $I_n = I$. ∎

Proposition 4.7

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.

Proposition 4.7

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.
2. Les deux propriétés suivantes sont vérifiées :
   1. Toute suite croissante d'idéaux principaux est stationnaire.
   2. Tout élément irréductible est premier.

Proposition 4.7

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.
2. Les deux propriétés suivantes sont vérifiées :
   1. Toute suite croissante d'idéaux principaux est stationnaire.
   2. Tout élément irréductible est premier.

Dém: L'implication difficile : 2.$\Rightarrow$1. Il suffit de montrer que tout élément non-nul et non-inversible de A se décompose en produit d'éléments irréductibles.

Proposition 4.7

Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :

1. A est factoriel.
2. Les deux propriétés suivantes sont vérifiées :
   1. Toute suite croissante d'idéaux principaux est stationnaire.
   2. Tout élément irréductible est premier.

Dém: L'implication difficile : 2.$\Rightarrow$1. Il suffit de montrer que tout élément non-nul et non-inversible de A se décompose en produit d'éléments irréductibles.

Soit $a \in A$ non-nul et non-inversible. Supposons par l'absurde que a ne se décompose pas en produit d'irréductibles.

En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles.

En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles.

Au moins l'un des deux facteurs, noté a_1, ne se décompose pas en produit d'irréductibles. Par récurrence on obtient une suite $(a_n)_{n\in\mathbb{N}}$ telle que

1. $a_0 = a$.

33

En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles.

Au moins l'un des deux facteurs, noté a_1, ne se décompose pas en produit d'irréductibles. Par récurrence on obtient une suite $(a_n)_{n\in\mathbb{N}}$ telle que

1. $a_0 = a$.
2. $\forall n \in \mathbb{N}, a_n$ ne se décompose pas en produit d' irréduct.

En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles.

Au moins l'un des deux facteurs, noté a_1, ne se décompose pas en produit d'irréductibles. Par récurrence on obtient une suite $(a_n)_{n\in\mathbb{N}}$ telle que

1. $a_0 = a$.
2. $\forall n \in \mathbb{N}$, a_n ne se décompose pas en produit d' irréduct.
3. $\forall n \in \mathbb{N}$, $a_{n+1}|a_n$.

En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles.

Au moins l'un des deux facteurs, noté a_1, ne se décompose pas en produit d'irréductibles. Par récurrence on obtient une suite $(a_n)_{n\in\mathbb{N}}$ telle que

1. $a_0 = a$.
2. $\forall n \in \mathbb{N}$, a_n ne se décompose pas en produit d' irréduct.
3. $\forall n \in \mathbb{N}$, $a_{n+1} | a_n$.
4. $\forall n \in \mathbb{N}$ et a_{n+1}, a_n ne sont pas associés.

En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles.

Au moins l'un des deux facteurs, noté a_1, ne se décompose pas en produit d'irréductibles. Par récurrence on obtient une suite $(a_n)_{n\in\mathbb{N}}$ telle que

1. $a_0 = a$.
2. $\forall n \in \mathbb{N}$, a_n ne se décompose pas en produit d' irréduct.
3. $\forall n \in \mathbb{N}$, $a_{n+1} | a_n$.
4. $\forall n \in \mathbb{N}$ et a_{n+1}, a_n ne sont pas associés.

Posons $I_n := (a_n)$. La suite d'idéaux principaux $(I_n)_n$ est croissante et n'est pas stationnaire. Ceci contredit l'hypothèse.

∎

34

Théorème 4.8

Tout anneau principal est factoriel.

Dém: C′est une conséquence directe de la proposition 2.9, la remarque 4.6 et la proposition 4.7. ∎

Théorème 4.8

Tout anneau principal est factoriel.

Dém: C'est une conséquence directe de la proposition 2.9, la remarque 4.6 et la proposition 4.7. ∎

Le théorème suivant (démonstration omise) fournit une classe importante d'anneaux factoriels.

Théorème 4.8

Tout anneau principal est factoriel.

Dém: C'est une conséquence directe de la proposition 2.9, la remarque 4.6 et la proposition 4.7. ∎

Le théorème suivant (démonstration omise) fournit une classe importante d'anneaux factoriels.

Théorème 4.9

Soit A un anneau factoriel. Alors l'anneau $A[X]$ des polynômes à coefficients dans A est factoriel.

Théorème 4.8

Tout anneau principal est factoriel.

Dém: C'est une conséquence directe de la proposition 2.9, la remarque 4.6 et la proposition 4.7. ■

Le théorème suivant (démonstration omise) fournit une classe importante d'anneaux factoriels.

Théorème 4.9

Soit A un anneau factoriel. Alors l'anneau $A[X]$ des polynômes à coefficients dans A est factoriel.

Exemple 4.1

L'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$ est factoriel, mais il n'est pas principal.

Corollaire 4.10

Soient K un corps et $n \in \mathbb{N}^*$. Alors l'anneau $K[X_1, \ldots, X_n]$ des polynômes en n variables à coefficients dans K est un anneau factoriel.

Corollaire 4.10

Soient K un corps et $n \in \mathbb{N}^*$. Alors l'anneau $K[X_1, \ldots, X_n]$ des polynômes en n variables à coefficients dans K est un anneau factoriel.

A remarquer que, pour $n \geq 2$ l'anneau $K[X_1, \ldots, X_n]$ n'est pas principal.

Soient A un anneau factoriel et $\mathcal{P}$ l'ensemble des éléments premiers de A. La relation $\mathrm{Ass} \subset \mathcal{P}\times\mathcal{P}$ sur $\mathcal{P}$ définie par

$$\mathrm{Ass} := \{(p,q) \in \mathcal{P}\times\mathcal{P} |\ p,\ q \text{ sont associés}\}$$

est une relation d'équivalence sur $\mathcal{P}$.

Soient A un anneau factoriel et $\mathcal{P}$ l'ensemble des éléments premiers de A. La relation $\mathrm{Ass} \subset \mathcal{P}\times\mathcal{P}$ sur $\mathcal{P}$ définie par

$$\mathrm{Ass} := \{(p,q)\in\mathcal{P}\times\mathcal{P} |\ p,\ q \text{ sont associés}\}$$

est une relation d'équivalence sur $\mathcal{P}$.

Dans chaque classe d'équivalence $C \in \mathcal{P}/\mathrm{Ass}$ choisissons un représentant $p_C \in C$.

Soient A un anneau factoriel et $\mathcal{P}$ l'ensemble des éléments premiers de A. La relation $\mathrm{Ass} \subset \mathcal{P} \times \mathcal{P}$ sur $\mathcal{P}$ définie par

$$\mathrm{Ass} := \{(p,q) \in \mathcal{P} \times \mathcal{P} |\ p,\ q \text{ sont associés}\}$$

est une relation d'équivalence sur $\mathcal{P}$.

Dans chaque classe d'équivalence $C \in \mathcal{P}/\mathrm{Ass}$ choisissons un représentant $p_C \in C$.

Soit $P := \{p_C |\ C \in \mathcal{P}/\mathrm{Ass}\}$ le sous-ensemble de $\mathcal{P}$ formé avec les représentants choisis.

Soient A un anneau factoriel et $\mathcal{P}$ l'ensemble des éléments premiers de A. La relation $\mathrm{Ass} \subset \mathcal{P} \times \mathcal{P}$ sur $\mathcal{P}$ définie par

$$\mathrm{Ass} := \{(p, q) \in \mathcal{P} \times \mathcal{P} |\ p,\ q \text{ sont associés}\}$$

est une relation d'équivalence sur $\mathcal{P}$.

Dans chaque classe d'équivalence $C \in \mathcal{P}/\mathrm{Ass}$ choisissons un représentant $p_C \in C$.

Soit $P := \{p_C |\ C \in \mathcal{P}/\mathrm{Ass}\}$ le sous-ensemble de $\mathcal{P}$ formé avec les représentants choisis.

Soit $p \in P$. La valuation associée à p est l'application

$$v_p : A \setminus \{0_A\} \to \mathbb{N},\ v_p(a) := \max\{k \in \mathbb{N} |\ p^k | a\}.$$

Remarque 4.11

Soit A un anneau factoriel.

1. Soit $a \in A \setminus \{0\}$. Alors $a = u \prod_{v_p(a) \neq 0} p^{v_p(a)}$, où $u \in A$ est inversible.
2. Soient $a, b \in A \setminus \{0\}$. Alors $a | b$ si et seulement si pour tout $p \in P$ on a $v_p(a) \leq v_p(b)$.

Remarque 4.11

Soit A un anneau factoriel.

1. Soit $a \in A \setminus \{0\}$. Alors $a = u \prod_{v_p(a) \neq 0} p^{v_p(a)}$, où $u \in A$ est inversible.
2. Soient $a, b \in A \setminus \{0\}$. Alors $a|b$ si et seulement si pour tout $p \in P$ on a $v_p(a) \leq v_p(b)$.

Dans la 1ère égalité on utilise la convention : le produit d'un sous-ensemble E d'éléments de A vaut 1_A si $E = \emptyset$.

Remarque 4.11

Soit A un anneau factoriel.

1. Soit $a \in A \setminus \{0\}$. Alors $a = u \prod_{v_p(a) \neq 0} p^{v_p(a)}$, où $u \in A$ est inversible.
2. Soient $a, b \in A \setminus \{0\}$. Alors $a|b$ si et seulement si pour tout $p \in P$ on a $v_p(a) \leq v_p(b)$.

Dans la 1ère égalité on utilise la convention : le produit d'un sous-ensemble E d'éléments de A vaut 1_A si $E = \emptyset$.

Dém: Si 1. $a \in A^\times$ c'est clair. Si $a \notin A^\times$, on obtient une décomposition $a = \prod_{i=1}^n q_i$ avec q_i premiers.

Remarque 4.11

Soit A un anneau factoriel.

1. Soit $a \in A \setminus \{0\}$. Alors $a = u \displaystyle\prod_{v_p(a) \neq 0} p^{v_p(a)}$, où $u \in A$ est inversible.
2. Soient $a, b \in A \setminus \{0\}$. Alors $a|b$ si et seulement si pour tout $p \in P$ on a $v_p(a) \leq v_p(b)$.

Dans la 1ère égalité on utilise la convention : le produit d'un sous-ensemble E d'éléments de A vaut 1_A si $E = \emptyset$.

Dém: Si 1. $a \in A^\times$ c'est clair. Si $a \notin A^\times$, on obtient une décomposition $a = \prod_{i=1}^n q_i$ avec q_i premiers.

Soit $p_i \in P$ associé avec q_i. On obtient $a = u \prod_{i=1}^n p_i$ avec $u \in A^\times$.

En regroupant les facteurs on arrive à une décomposition

$$a = u\prod_{s=1}^{l} p_{i_s}^{n_s} \text{ où } n_s \in \mathbb{N}^*,\ p_{i_s} \neq p_{i_t} \text{ pour } s \neq t.$$

Facile : $n_s = v_{p_{i_s}}(a)$ et $v_p(a) = 0$ pour $p \notin \{p_{i_1}, \dots, p_{i_l}\}$.

2. Exercice. ∎

En regroupant les facteurs on arrive à une décomposition

$$a = u\prod_{s=1}^{l} p_{i_s}^{n_s} \text{ où } n_s \in \mathbb{N}^*,\ p_{i_s} \neq p_{i_t} \text{ pour } s \neq t.$$

Facile : $n_s = v_{p_{i_s}}(a)$ et $v_p(a) = 0$ pour $p \notin \{p_{i_1}, \dots, p_{i_l}\}$.

2. Exercice. ∎

Soient $a_1, \dots, a_n$ éléments non-nuls de A. Nous avons noté par $\mathrm{Div}(a_1, \dots, a_n)$, $\mathrm{Mult}(a_1, \dots, a_n)$ l'ensemble des diviseurs communs, respectivement l'ensemble des multiples communs des éléments $a_1, \dots, a_n$.

Proposition 4.12

Soient A un anneau factoriel et $a_1, \ldots, a_n$ éléments non-nuls de A. Alors

1. Il existe $d \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d)$, donc

Proposition 4.12

Soient A un anneau factoriel et $a_1,\dots,a_n$ éléments non-nuls de A. Alors

1. Il existe $d \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Div}(a_1,\dots,a_n) = \mathrm{Div}(d)$, donc d est un diviseur commun des éléments $a_1,\dots,a_n$ et l'ensemble des diviseurs communs des éléments $a_1,\dots,a_n$ coïncide avec l'ensemble des diviseurs de d.

Proposition 4.12

Soient A un anneau factoriel et $a_1, \dots, a_n$ éléments non-nuls de A. Alors

1. Il existe $d \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Div}(a_1, \dots, a_n) = \mathrm{Div}(d)$, donc d est un diviseur commun des éléments $a_1, \dots, a_n$ et l'ensemble des diviseurs communs des éléments $a_1, \dots, a_n$ coïncide avec l'ensemble des diviseurs de d.
2. Il existe $m \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Mult}(a_1, \dots, a_n) = (m)$, donc

Proposition 4.12

Soient A un anneau factoriel et $a_1, \ldots, a_n$ éléments non-nuls de A. Alors

1. Il existe $d \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d)$, donc d est un diviseur commun des éléments $a_1, \ldots, a_n$ et l'ensemble des diviseurs communs des éléments $a_1, \ldots, a_n$ coïncide avec l'ensemble des diviseurs de d.
2. Il existe $m \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Mult}(a_1, \ldots, a_n) = (m)$, donc l'ensemble des multiples communs des éléments $a_1, \ldots, a_n$ coïncide avec l'idéal principal engendré par m.

Proposition 4.12

Soient A un anneau factoriel et $a_1, \ldots, a_n$ éléments non-nuls de A. Alors

1. Il existe $d \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d)$, donc d est un diviseur commun des éléments $a_1, \ldots, a_n$ et l'ensemble des diviseurs communs des éléments $a_1, \ldots, a_n$ coïncide avec l'ensemble des diviseurs de d.
2. Il existe $m \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que $\mathrm{Mult}(a_1, \ldots, a_n) = (m)$, donc l'ensemble des multiples communs des éléments $a_1, \ldots, a_n$ coïncide avec l'idéal principal engendré par m.

Notation : $d = \mathrm{pgcd}(a_1, \ldots, a_n)$, $m = \mathrm{ppcm}(a_1, \ldots, a_n)$.

Dém: On va démontrer l'existence, l'unicité est proposée comme exercice. Pour $p \in P$ posons

$$k_p := \min\{v_p(a_i) \mid 1 \leq i \leq n\},\ l_p := \max\{v_p(a_i) \mid 1 \leq i \leq n\}.$$

Dém: On va démontrer l'existence, l'unicité est proposée comme exercice. Pour $p \in P$ posons

$$k_p := \min\{v_p(a_i) |\ 1 \leq i \leq n\},\ l_p := \max\{v_p(a_i) |\ 1 \leq i \leq n\}.$$

En utilisant la remarque 4.11 c'est facile de voir que $d := \prod_{k_p \neq 0} p^{k_p}$, $m := \prod_{l_p \neq 0} p^{l_p}$ satisfont les égalités requises

$$\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d),\ \mathrm{Mult}(a_1, \ldots, a_n) = (m).$$

■

Dém: On va démontrer l'existence, l'unicité est proposée comme exercice. Pour $p \in P$ posons

$$k_p := \min\{v_p(a_i) \mid 1 \leq i \leq n\},\ l_p := \max\{v_p(a_i) \mid 1 \leq i \leq n\}.$$

En utilisant la remarque 4.11 c'est facile de voir que $d := \prod_{k_p \neq 0} p^{k_p}$, $m := \prod_{l_p \neq 0} p^{l_p}$ satisfont les égalités requises

$$\mathrm{Div}(a_1, \dots, a_n) = \mathrm{Div}(d),\ \mathrm{Mult}(a_1, \dots, a_n) = (m).$$

■

Exercice 4.1

Soient a, b éléments non-nuls de l'anneau factoriel A. Alors $\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b) = ab$ à multiplication près par un élément inversible.

Conclusions :

Nous avons les implications :

EUCLIDIEN $\Rightarrow$ PRINCIPAL $\Rightarrow$ FACTORIEL

Conclusions :

Nous avons les implications :
EUCLIDIEN $\Rightarrow$ PRINCIPAL $\Rightarrow$ FACTORIEL

Aucune implication inverse n'est vraie !

Conclusions :

Nous avons les implications :
EUCLIDIEN $\Rightarrow$ PRINCIPAL $\Rightarrow$ FACTORIEL

Aucune implication inverse n'est vraie!

Dans un anneau factoriel nous avons :

1. premier $\Leftrightarrow$ irréductible.

Conclusions :

Nous avons les implications :
EUCLIDIEN $\Rightarrow$ PRINCIPAL $\Rightarrow$ FACTORIEL

Aucune implication inverse n'est vraie!

Dans un anneau factoriel nous avons :

1. premier $\Leftrightarrow$ irréductible.
2. tout élément non-nul, non-inversible admet une décomposition en produit de facteurs premiers (irréductibles),

Conclusions :

Nous avons les implications :
EUCLIDIEN $\Rightarrow$ PRINCIPAL $\Rightarrow$ FACTORIEL

Aucune implication inverse n'est vraie !

Dans un anneau factoriel nous avons :

1. premier $\Leftrightarrow$ irréductible.
2. tout élément non-nul, non-inversible admet une décomposition en produit de facteurs premiers (irréductibles), décomposition unique à ordre et "association" près.

Conclusions :

Nous avons les implications :
EUCLIDIEN $\Rightarrow$ PRINCIPAL $\Rightarrow$ FACTORIEL

Aucune implication inverse n'est vraie!

Dans un anneau factoriel nous avons :

1. premier $\Leftrightarrow$ irréductible.
2. tout élément non-nul, non-inversible admet une décomposition en produit de facteurs premiers (irréductibles), décomposition unique à ordre et "association" près.
3. pgcd, ppcm existent, $\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b) = ab$ à multiplication près par un élément inversible.

Conclusions :

Nous avons les implications :
EUCLIDIEN ⇒ PRINCIPAL ⇒ FACTORIEL

Aucune implication inverse n'est vraie!

Dans un anneau factoriel nous avons :

1. premier ⇔ irréductible.
2. tout élément non-nul, non-inversible admet une décomposition en produit de facteurs premiers (irréductibles), décomposition unique à ordre et "association" près.
3. pgcd, ppcm existent, $\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b) = ab$ à multiplication près par un élément inversible.

L'égalité de Bézout et le théorème de Bézout ne se généralisent pas aux anneaux factoriels.