Anneaux de l'arithmétique

Devaux Stéven

July 11, 2017

Tout les anneaux seront intègres. Soit A un anneau.

Tout les anneaux seront intègres. Soit A un anneau.

Définition (premier)

Un élément p non nul non inversible de A est dit premier si :

$$\forall a, b \in A, p|ab \Rightarrow p|a \text{ ou } p|b$$

Tout les anneaux seront intègres. Soit A un anneau.

Définition (premier)

Un élément p non nul non inversible de A est dit premier si :

$$\forall a, b \in A, p|ab \Rightarrow p|a \text{ ou } p|b$$

Définition (irréductible)

Un élément p non nul non inversible de A est dit irréductible si :

$$\forall a, b \in A, (p = ab \Rightarrow a \in A^{\times} \text{ ou } b \in A^{\times})$$

Tout les anneaux seront intègres. Soit A un anneau.

Définition (premier)

Un élément p non nul non inversible de A est dit premier si :

$$\forall a, b \in A, p | ab \Rightarrow p | a \text{ ou } p | b$$

Définition (irréductible)

Un élément p non nul non inversible de A est dit irréductible si :

$$\forall a, b \in A, (p = ab \Rightarrow a \in A^{\times} \text{ ou } b \in A^{\times})$$

Proposition

premier $\Rightarrow$ *irréductible.*

Proposition

premier $\Rightarrow$ irréductible.

Exemple

Dans $\mathbb{Z}[\sqrt{-5}]$, 2 est irréductible mais pas premier. En effet $2.3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Or $2 \nmid (1 \pm \sqrt{-5})$.

Définition (Pgcd et ppcm)

Soienta$a_1, ..., a_n$ dans A :

1. $d \in A$ est un plus grand commun diviseur de $a_1, ..., a_n$ si d satisfait :
   - d est un diviseur commun à $a_1, ..., a_n$.
   - si $d' \in A$ est un autre diviseur commun à $a_1, ..., a_n$ alors $d'|d$.
2. $m \in A$ est un plus petit commun multiple de $a_1, ..., a_n$ si m satisfait :
   - m est un multiple commun à $a_1, ..., a_n$.
   - si $m' \in A$ est un autre multiple commun à $a_1, ..., a_n$ alors $m|m'$.

Définition (Anneau à pgcd)

A est un anneau à pgcd si et seulement si tout couple d'éléments de A admet un pgcd.

Définition (Anneau à pgcd)

A est un anneau à pgcd si et seulement si tout couple d'éléments de A admet un pgcd.

Si A est un anneau à pgcd.

Définition (Anneau à pgcd)

A est un anneau à pgcd si et seulement si tout couple d'éléments de A admet un pgcd.

Si A est un anneau à pgcd.

Théorème (Lemme de Gauss)

Pour tout a, b et c dans A tels que a et b sont premiers entre eux. $a | bc \Rightarrow a | c$.

Définition (Anneau à pgcd)

A est un anneau à pgcd si et seulement si tout couple d'éléments de A admet un pgcd.

Si A est un anneau à pgcd.

Théorème (Lemme de Gauss)

Pour tout a, b et c dans A tels que a et b sont premiers entre eux. $a|bc \Rightarrow a|c$.

Théorème (Lemme d'Euclide)

Tout élément irréductible de A est premier.

Définition (Anneau factoriel)

Un anneau est factoriel si tout ses éléments non nuls non inversibles sont produits d'éléments premiers.

Définition (Anneau factoriel)

Un anneau est factoriel si tout ses éléments non nuls non inversibles sont produits d'éléments premiers.

Définition (Anneau de Bézout)

Un anneau de Bézout est un anneau dans lequel tout idéal de type fini est principal.

Définition (Anneau factoriel)

Un anneau est factoriel si tout ses éléments non nuls non inversibles sont produits d'éléments premiers.

Définition (Anneau de Bézout)

Un anneau de Bézout est un anneau dans lequel tout idéal de type fini est principal.

Si A est de Bézout,

Définition (Anneau factoriel)

Un anneau est factoriel si tout ses éléments non nuls non inversibles sont produits d'éléments premiers.

Définition (Anneau de Bézout)

Un anneau de Bézout est un anneau dans lequel tout idéal de type fini est principal.

Si A est de Bézout,

Théorème (de Bézout)

Pour tout $a, b \in A$ *avec* $d = pgcd(a, b)$ *il existe* $u, v \in A$ *tels que* $au + bv = d$.

Définition (Anneau principal)

A est principal si tout ses idéaux sont principaux.

Définition (Anneau principal)

A est principal si tout ses idéaux sont principaux.

Définition (Anneaux euclidiens)

A est dit euclidien s'il existe une application, $\nu : A\backslash\{0\} \rightarrow \mathbb{N}$ telle que : $\forall (a, b) \in A \times A\backslash\{0\}, \exists q, r \in A$ *tels que :*
$a = bq + r$ *avec* $r = 0$ *ou* $\nu(r) < \nu(b)$

$$
\begin{tikzcd}
 & \text{Anneau à pgcd} & & \\
\text{A. factoriel} \arrow[ur] & & \text{A. de Bézout} \arrow[ul] & \\
 & \text{A. principal} \arrow[ul] \arrow[ur] \arrow[rr, leftrightarrow] & & \text{A. de Bézout et factoriel} \\
 & \text{A. euclidien} \arrow[u, Rightarrow] & &
\end{tikzcd}
$$

Théorème

Si A est un anneau à pgcd alors $S^{-1}A$ aussi.

Théorème

Si A est factoriel alors $S^{-1}A$ aussi.

Théorème

Si A est un anneau de Bézout alors $S^{-1}A$ aussi.

Théorème

Si A est principal alors $S^{-1}A$ aussi.

Soit I un idéal premier de A.

Soit I un idéal premier de A.

Proposition

Si A est de Bézout alors A/I aussi.

Proposition

Si A est principal(resp. euclidien) alors A/I aussi.

Soit I un idéal premier de A.

Proposition

Si A est de Bézout alors A/I aussi.

Proposition

Si A est principal(resp. euclidien) alors A/I aussi.

Exemple

$\mathbb{Z}$ est factoriel mais $\mathbb{Z}[X]/(X^2+5) \simeq \mathbb{Z}[\sqrt{-5}]$ n'est pas à pgcd.

Théorème

A est un anneau à pgcd ssi $A[X]$ aussi.

Théorème

A est un anneau factoriel ssi $A[X]$ aussi.

Théorème

A est un anneau à pgcd ssi $A[X]$ aussi.

Théorème

A est un anneau factoriel ssi $A[X]$ aussi.

Théorème

Les assertions suivantes sont équivalentes :

1. *A est un corps.*
2. *$A[X]$ est euclidien.*
3. *$A[X]$ est principal.*
4. *$A[X]$ est de Bézout.*

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$.

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$. Puis considérons l'anneau $Q_2 = \mathbb{Q}[X_1, Y]/(Y^2 - X_1) = \mathbb{Q}[\sqrt{X_1}] = \mathbb{Q}[X_2]$ avec $X_2 = \sqrt{X_1}$. Alors on a $Q_1 \subset Q_2$.

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$. Puis considérons l'anneau $Q_2 = \mathbb{Q}[X_1, Y]/(Y^2 - X_1) = \mathbb{Q}[\sqrt{X_1}] = \mathbb{Q}[X_2]$ avec $X_2 = \sqrt{X_1}$. Alors on a $Q_1 \subset Q_2$.Maintenant posons pour tout $k > 2$, $Q_k = \mathbb{Q}[X_{k-1}, Y]/(Y^2 - X_{k-1}) = \mathbb{Q}[X_k]$ avec $X_k = \sqrt{X_{k-1}}$

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$. Puis considérons l'anneau $Q_2 = \mathbb{Q}[X_1, Y]/(Y^2 - X_1) = \mathbb{Q}[\sqrt{X_1}] = \mathbb{Q}[X_2]$ avec $X_2 = \sqrt{X_1}$. Alors on a $Q_1 \subset Q_2$.Maintenant posons pour tout $k > 2$, $Q_k = \mathbb{Q}[X_{k-1}, Y]/(Y^2 - X_{k-1}) = \mathbb{Q}[X_k]$ avec $X_k = \sqrt{X_{k-1}}$alors on a la suite d'inclusion :

$$Q_1 \subset Q_2 \subset ... \subset Q_k \subset ...$$

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$. Puis considérons l'anneau $Q_2 = \mathbb{Q}[X_1, Y]/(Y^2 - X_1) = \mathbb{Q}[\sqrt{X_1}] = \mathbb{Q}[X_2]$ avec $X_2 = \sqrt{X_1}$. Alors on a $Q_1 \subset Q_2$.Maintenant posons pour tout $k > 2$, $Q_k = \mathbb{Q}[X_{k-1}, Y]/(Y^2 - X_{k-1}) = \mathbb{Q}[X_k]$ avec $X_k = \sqrt{X_{k-1}}$alors on a la suite d'inclusion :

$$Q_1 \subset Q_2 \subset ... \subset Q_k \subset ...$$

Puis désignons par Q^+ l'union de ces anneaux.

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$. Puis considérons l'anneau $Q_2 = \mathbb{Q}[X_1, Y]/(Y^2 - X_1) = \mathbb{Q}[\sqrt{X_1}] = \mathbb{Q}[X_2]$ avec $X_2 = \sqrt{X_1}$. Alors on a $Q_1 \subset Q_2$.Maintenant posons pour tout $k > 2$, $Q_k = \mathbb{Q}[X_{k-1}, Y]/(Y^2 - X_{k-1}) = \mathbb{Q}[X_k]$ avec $X_k = \sqrt{X_{k-1}}$alors on a la suite d'inclusion :

$$Q_1 \subset Q_2 \subset ... \subset Q_k \subset ...$$

Puis désignons par Q^+ l'union de ces anneaux. On trouve que Q^+ est de Bézout car union croissante d'anneaux de Bézout,

Considérons l'anneau $Q_1 = \mathbb{Q}[X_1]$ des polynômes en une indéterminé X_1 sur $\mathbb{Q}$. Puis considérons l'anneau $Q_2 = \mathbb{Q}[X_1, Y]/(Y^2 - X_1) = \mathbb{Q}[\sqrt{X_1}] = \mathbb{Q}[X_2]$ avec $X_2 = \sqrt{X_1}$. Alors on a $Q_1 \subset Q_2$.Maintenant posons pour tout $k > 2$, $Q_k = \mathbb{Q}[X_{k-1}, Y]/(Y^2 - X_{k-1}) = \mathbb{Q}[X_k]$ avec $X_k = \sqrt{X_{k-1}}$alors on a la suite d'inclusion :

$$Q_1 \subset Q_2 \subset ... \subset Q_k \subset ...$$

Puis désignons par Q^+ l'union de ces anneaux. On trouve que Q^+ est de Bézout car union croissante d'anneaux de Bézout,et pas factoriel car X_1 n'est pas factorisable en facteurs irréductibles.

Proposition

$Q^+[X]$ l'anneau des polynômes en une indéterminée X sur Q^+ est à pgcd mais est ni factoriel ni de Bézout.

$$
\begin{tikzcd}
 & \text{Anneau à pgcd} & & \\
\text{A. factoriel} \arrow[ur, Rightarrow] & & \text{A. de Bézout} \arrow[ul, Rightarrow] & \\
 & \text{A. principal} \arrow[ul, Rightarrow] \arrow[ur, Rightarrow] \arrow[rr, leftrightarrow] & & \text{A. de Bézout et factoriel} \\
 & \text{A. euclidien} \arrow[u, Rightarrow] & &
\end{tikzcd}
$$