Anneaux de l'arithmétique

Devaux Stéven

August 26, 2017

Table des matières

Introduction On va d'abord définir les propriétés arithmétiques de base des éléments et des idéaux d'un anneau commutatif et unitaire. Et ensuite on verra comment elles se comportent dans différents types d'anneaux. Ces types d'anneaux seront définis par une propriété arithmétique ou en vérifieront une (d'où le titre). Par exemple un anneau à pgcd sera défini par l'existence de tout pgcd. De plus on étudiera ce qui se passe lorsqu'on construit d'autres anneaux à partir de ces anneaux. Qu'elles propriétés arithmétiques d'un anneau sont conservées lorsqu'on considère un anneau polynôme ? Et enfin on clarifiera les relations d' « inclusions » qui existent entre ces différents types d'anneaux en exhibant des contre-exemples.

1 Propriétés arithmétiques des éléments d'un anneau

On considère un anneau commutatif et unitaire A.

1.1 Propriétés d'un élément

Rappel 1 (Divise)**.** *Soient a, b dans A. On dit que a divise b dans A et on le note alors $a|b$ si :*

$$\exists c \in A \text{ tel que } ac = b$$

Rappel 2 (Intègre)**.** *On dit que A est intègre s'il ne contient pas de diviseurs de zéro autre que zéro, ie:*

$$\forall a, b \in A, ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

De plus dans un tel anneau on peut utiliser la règle de simplification suivante :

$$\forall a, b, c \in A \text{ avec } a \neq 0, ab = ac \Rightarrow b = c$$

En effet si $ab = ac$ alors $a(b - c) = 0$ et comme A est intègre et que $a \neq 0$ alors $b - c = 0$.

Définition 3 (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 4 (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 5. *Si A est intègre alors tout élément premier de A est irréductible.*

Preuve. Soient a, b et p dans A tels que $p = ab$ avec p premier, on a alors $p|a$ ou $p|b$. Supposons que $p|a$ alors il existe c dans A tel que $a = pc$ donc $p = pcb$. Puis par intégrité on obtient $1 = bc$ d'où b est inversible. □

Exemple 6. 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 7 (Extrémal)**.** Un élément p non nul non inversible de A est dit extrémal s'il est étranger[1] à tout ceux qu'il ne divise pas.

[1] Voir la définition 15.

Proposition 8. *Tout élément extrémal de A est premier.*

Preuve. Soient a, b et p dans A tels que $p|ab$ avec p extrémal. Supposons que $p \nmid a$. Alors p est étranger à a. Donc il existe $u, v \in A$ tels que $au + pv = 1$. En multipliant cette égalité par b on obtient $abu + pvb = b$ donc $p|b$. De plus p est non nul non inversible donc p est premier. □

Exemple 9. Prenons $\mathbb{Z}[X]$; 2 est premier dans $\mathbb{Z}[X]$ (car premier dans $\mathbb{Z}$) et $2 \nmid X$ or 2 et X ne sont pas étrangers, en effet supposons par l'absurde qu'il existe $u, v \in \mathbb{Z}[X]$ tels que $2u + vX = 1$. La valeur en 0 de ce polynôme est $2u_0 = 1$ avec $u_0 = u(0) \in \mathbb{Z}$ donc 2 est inversible dans $\mathbb{Z}$ ce qui est absurde.

1.2 Propriétés entre éléments

Définition 10 (Éléments associés)**.** Deux éléments a et b de A sont dit associés, et on note alors $a \sim b$, si $a|b$ et $b|a$.

Proposition 11. *L'association dans A est une relation d'équivalence.*

Preuve. Soient $a, b, c \in A$. On a bien $a.1 = a$ donc $a \sim a$. Si $a|b$ et $b|c$ alors $a|c$ donc si $a \sim b$ et $b \sim c$ alors $a \sim c$. Et enfin par symétrie dans la définition de l'association on a bien $a \sim b \Leftrightarrow b \sim a$. □

Proposition 12. *Si A est intègre alors :*

$$\forall a, b \in A, a \sim b \Leftrightarrow \exists c \in A^\times \text{ tel que } a = bc$$

Preuve. ($\Rightarrow$) Soient a et b dans A tels que $a \sim b$. Si b est nul, alors par association et intégrité, a aussi donc il suffit de prendre $c = 1 \in A^\times$. Si b est non nul, la relation nous donne l'existence de c et d tels que $a = bc$ et $b = ad$ d'où $b = bcd$. Comme $b \neq 0$, par intégrité on obtient $dc = 1$ donc $c \in A^\times$.
($\Leftarrow$) Soient a et b dans A et supposons qu'il existe $c \in A^\times$ tel que $a = bc$ alors $b = ac^{-1}$ donc $b|a$ et $a|b$ d'où $a \sim b$. □

Proposition 13. *Si a et b sont associés dans A, alors a est premier (resp. irréductible, resp. extrémal) si et seulement si b l'est.*

Preuve. On montre le cas extrémal qui est moins clair que les deux autres qui découlent directement des définitions. Soient a, b associés dans A avec a extrémal. Soit $c \in A$ tel que $b \nmid c$ alors $a \nmid c$. Donc il existe $u, v \in A$ tels que $au + cv = 1$. Or $a \sim b$, donc il existe $k \in A$ tel que $a = bk$, d'où : $bku + cv = 1$, donc b et c sont étrangers. □

Définition 14 (Premiers entre eux)**.** Deux éléments a et b dans A sont dits premiers entre eux si pour tout $d \in A$ tel que $d|a$ et $d|b$, d est inversible (ie. $d \sim 1$).

Définition 15 (Éléments étrangers)**.** Deux éléments a et b dans A sont étrangers s'il existe u et v tels que $au + bv = 1$.

Proposition 16. *Si deux éléments de A sont étrangers alors ils sont premiers entre eux.*

Preuve. Soient a et b deux éléments étrangers dans A et $d \in A$ un de leur diviseur commun. Alors il existe $u, v \in A$ tels que $au + bv = 1$. $d|a$ et $d|b$ donc $d|1$ d'où $d \sim 1$ donc a et b sont premiers entre eux. □

Exemple 17. Dans $\mathbb{Z}[X]$, 2 et X sont premiers entre eux mais pas étrangers. On a déjà vu précédemment qu'ils ne sont pas étrangers. Soit $d \in \mathbb{Z}[X]$ un diviseur commun à 2 et X. Supposons par l'absurde que d n'est pas inversible alors $d \sim 2$ car 2 est irréductible. Or $d|X$ donc $2|X$ ce qui est absurde.

Définition 18 (Pgcd et ppcm)**.** Soient $a_1, ..., a_n$ 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 $m|m'$.

Remarque ∴ Ici il n'y a pas unicité du pgcd ou du ppcm. Par exemple dans $\mathbb{Z}$, 2 et -2 sont des pgcd de 6 et 10.

Proposition 19. *Si deux éléments d et d' de A sont des pgcd (resp. des ppcm) de $a_1, ..., a_n \in A$ alors ils sont associés.*

Preuve. Montrons le pour les pgcd. Si d et d' sont deux pgcd de $a_1, ..., a_n$ alors $d|d'$ car d est un pgcd et d' un diviseur commun et inversement $d'|d$. Donc ils sont associés. □

Remarque ∴ Dans l'exemple précédent on a bien $-2 = -1 \times 2$ avec -1 inversible dans $\mathbb{Z}$.

Remarque ∴ Dans la suite quand on utilisera les notations $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$ dans des égalités, elles seront considérées à association près.

Proposition 20. *Si A est intègre et $a, b \in A$ possèdent un ppcm alors ils possèdent un pgcd.*

Preuve. Soient a, b et m dans A tels que $ppcm(a, b) = m$. $m|ab$ donc il existe $d \in A$ tel que $md = ab$. Montrons que d est un pgcd de a et b. $b|m$ donc il existe $k \in A$ tel que $m = bk$. On a donc $bkd = ab$, en simplifiant par b on obtient $kd = a$ donc $d|a$, de même $d|b$. Soit $d' \in A$ un autre diviseur commun à a et b alors il existe $k_1, k_2 \in A$ tels que $a = d'k_1$ et $b = d'k_2$. Donc $ab = d'k_1b = ad'k_2$, en simplifiant par d', $k_1b = k_2a$ est un multiple commun de a et b. D'où $m|k_1b$. On a donc $md'|ab$. Or $ab = md$ donc $d'|d$. □

2 Propriétés arithmétiques des idéaux

Soit A un anneau commutatif et unitaire.

2.1 Propriétés des idéaux

Rappel 21. *On dit que $I \subset A$ est un idéal de $(A, +, \times)$ si $(I, +)$ est un sous groupe de $(A, +)$ qui vérifie la propriété d'absorption suivante :*

$$\forall a, b \in A, a \in I \Rightarrow ab \in I$$

Définition 22 (Idéal premier)**.** Un idéal I de A est dit premier s'il est propre ($I \neq A$) et si pour tout $a, b \in A$ tels que $ab \in I$ on a a ou b dans I.

Définition 23 (Idéal maximal)**.** Un idéal I de A est dit maximal s'il est propre et si A et I sont les seuls idéaux qui le contiennent(ie. $\forall J$ idéal de A, $(I \subset J \subset A) \Rightarrow (J = I$ ou $J = A)$).

Proposition 24. *Soit I un idéal de A et A/I l'anneau quotient [2] de A par I :*

1. *I est premier si et seulement si A/I est intègre.*

2. *I est maximal si et seulement si A/I est un corps.*

Preuve. 1. On a les équivalences suivantes :
I *est premier* $\Leftrightarrow \forall a, b \in A, (ab \in I \Rightarrow a \in I$ *ou* $b \in I)$
$\Leftrightarrow \forall \bar{a}, \bar{b} \in A/I, (\bar{a}\bar{b} = 0 \Rightarrow \bar{a} = 0$ *ou* $\bar{b} = 0)$.
$\Leftrightarrow A/I$ *est intègre*
2. ($\Rightarrow$) Avec I maximal. Soit $\bar{a} \in A/I$ non nul. Alors on a : $I \subsetneq (a) + I \subset A$. Comme I est maximal, $(a) + I = A$ donc en particulier il existe $b \in A$ et $i \in I$ tels que $ab + i = 1$ donc $\bar{a}\bar{b} = \bar{1}$. Donc $\bar{a}$ est inversible.
($\Leftarrow$) Avec A/I un corps. Soit J un idéal de A tel que $I \subsetneq J$. Donc il existe $j \in J \backslash I$. A/I est un corps, et $\bar{j} \neq 0$ car $j \notin I$, donc il existe $\bar{k} \in A/I$ tel que $\bar{j}\bar{k} = 1$. D'où il existe $i \in I$ tel que $jk = 1 + i$. Par absorption de J on a donc $1 \in J$ donc $J = A$. □

Corollaire 25. *Les idéaux maximaux de A sont premiers.*

Exemple 26. Dans $\mathbb{Z}[X]$, (X) est premier mais n'est pas maximal. En effet $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ qui est intègre mais pas un corps.

Définition 27 (Idéaux étrangers)**.** Deux idéaux I et J de A sont dit étrangers si $I + J = A$.

Proposition 28. *Soient $a, b \in A$. a et b sont étrangers si et seulement si (a) et (b) sont étrangers.*

Preuve. On a les équivalences suivantes :

$$a \text{ et } b \text{ sont étrangers } \Leftrightarrow \exists u, v \in A \text{ tels que } au + bv = 1 \Leftrightarrow (a) + (b) = (1) = A$$

□

Définition 29 (Condition de chaine ascendante)**.** On dit qu'un ensemble $\mathcal{I}$ d'idéaux de A vérifie la condition de chaine ascendante (pour l'inclusion) si toute suite croissante d'idéaux de $\mathcal{I}$ est ultimement stationnaire :

$$\forall (I_n)_{n\in\mathbb{N}} \in \mathcal{I}^{\mathbb{N}} \text{ telle que } (I_1) \subset ... \subset (I_n) \subset ..., \exists k \in \mathbb{N} \text{ tel que } \forall m \in \mathbb{N}, m \geq k \Rightarrow (I_k) = (I_m)$$

[2] Voir le rappel 90 à propos des anneaux quotient.

2.2 Liens entre éléments générateurs et idéaux

Définition 30 (Idéal de type fini et principal)**.** Un idéal de type fini est un idéal engendré par un nombre fini d'élément, il est dit principal lorsqu'il est engendré par un seul élément.

Proposition 31. *Soient a et b dans A alors $a|b$ si et seulement si $(b) \subset (a)$.*

Preuve. ($\Rightarrow$) Si $a|b$ alors il existe $c \in A$ tel que $b = ac$. Soit $m \in (b)$ alors il existe $m' \in A$ tel que $m = bm'$ donc au final $m = acm'$ donc $m \in (a)$.
($\Leftarrow$) Si $(b) \subset (a)$, $b \in (a)$ donc il existe $c \in A$ tel que $b = ac$ donc $a|b$. □

Corollaire 32. *Soient $a, b \in A$, a et b sont associés si et seulement si $(a) = (b)$.*

Proposition 33. *Soient a, b et m dans A. m est un ppcm de a et b si et seulement si $(a) \cap (b) = (m)$.*

Preuve. Comme $(a) \cap (b)$ est l'ensemble des multiples communs à a et b on a :

$$\begin{aligned}(a) \cap (b) = (m) &\Leftrightarrow \begin{cases} m \in (a) \cap (b) \\ \forall m' \in (a) \cap (b), m' \in (m) \end{cases} \\ &\Leftrightarrow \begin{cases} m \text{ multiple commun à } a \text{ et } b \\ \forall m' \text{ multiple commun à } a \text{ et } b, m' \text{est multiple de } m \end{cases} \\ &\Leftrightarrow m = \text{ppcm}(a, b)\end{aligned}$$

□

Remarque ∴ On a le même résultat lorsque l'on considère n éléments tels que $(a_1) \cap ... \cap (a_n) = (m)$.

Proposition 34. *Soient a, b et d dans A. Si $(a, b) = (d)$ alors d est un pgcd de a et b.*

Preuve.

$$\begin{aligned}(a, b) = (d) &\Rightarrow \begin{cases} a, b \in (d) \\ \forall d' \in A, (a, b) \subset (d') \Rightarrow (d) \subset (d') \end{cases} \\ &\Rightarrow \begin{cases} d|a \text{ et } d|b \\ \forall d' \in A, d'|a \text{ et } d'|b \Rightarrow d'|d \end{cases} \\ &\Rightarrow d = \text{pgcd}(a, b)\end{aligned}$$

□

Remarque ∴ On a le même résultat lorsque l'on considère n éléments tels que $(a_1, ..., a_n) = (d)$.

Exemple 35. Dans $\mathbb{Z}[X]$, $(2, X) \neq (1)$ pourtant $\text{pgcd}(2, X) = 1$.

Proposition 36. *Soit $a \in A$ non nul, a est premier si et seulement si (a) est premier.*

Preuve. On a les équivalences suivantes :

$$\begin{aligned}(a) \text{ premier} &\Leftrightarrow \forall b, c \in A, bc \in (a) \Rightarrow (b \in (a) \text{ ou } c \in (a)) \\ &\Leftrightarrow \forall b, c \in A, (a|bc \Rightarrow a|b \text{ ou } a|c) \\ &\Leftrightarrow a \text{ est premier}\end{aligned}$$

□

Proposition 37. *Soit a un élément non nul de A. Si (a) est maximal alors a est irréductible.*

Preuve. Supposons que (a) est maximal. Soient $b, c \in A$ tels que $a = bc$ avec c non inversible alors $a \not\sim b$ et $b|a$. On obtient donc les inclusions suivantes $(a) \subsetneq (b) \subset A$, or (a) est maximal donc $(b) = A$ d'où b est inversible et a est irréductible. □

Exemple 38. Dans $\mathbb{Z}[X]$, X est irréductible mais (X) n'est pas maximal.

3 Anneaux de l'arithmétique

3.1 Anneau à pgcd

Définition 39 (Anneau à pgcd)**.** Soit A un anneau, on dit que A est un anneau à pgcd si et seulement s'il est commutatif unitaire et que tout couple d'éléments de A admet un pgcd.

Soit A un anneau à pgcd.

Lemme 40. *Soient a, b et c dans A intègre, alors on a $pgcd(ac, bc) \sim c \times pgcd(a, b)$*

Preuve. Supposons que $\text{pgcd}(a, b) = 1$ quitte à diviser a par leur pgcd. Posons $d = \text{pgcd}(ac, bc)$, comme $c|ac$ et $c|bc$ on a $c|d$. Donc il existe $e \in A$ tel que $d = ce$. On a donc $ce|ac$ et $ce|bc$, par intégrité on obtient : $e|a$ et $e|b$ donc e est inversible. D'où $c = de^{-1}$ donc $d|c$ et $d \sim c$. □

Proposition 41. *Soit B un anneau intègre, tout couple de B possède un pgcd si et seulement si tout couple de B possède un ppcm.*

Preuve. ($\Leftarrow$) Voir la propriété 20.
($\Rightarrow$) Soient a, b et d dans B tels que $d = pgcd(a, b)$ et supposons que tout couple de B possède un pgcd. $d|ab$ donc il existe $m \in B$ tel que $ab = md$. Montrons que m est un ppcm de a et b. m est un multiple commun de a ou b car lorsque on divise a ou b par d dans le produit ab on a m multiple de a ou b. Soit m' un autre multiple commun a a et b. $ab|am'$ et $ab|bm'$ donc $ab|pgcd(am', bm')$ donc $md|m'd$ d'où $m|m'$. □

Remarque :. La propriété précédente nous indique qu'un anneau intègre à pgcd est un anneau intègre à ppcm.

Théorème 42 (Lemme de Gauss)**.** *Soient a, b et c dans A tels que a et b soient premiers entre eux. Si $a|bc$ alors $a|c$.*

Preuve. $a|ac$ et $a|bc$ donc $a|\text{pgcd}(ac, bc)$ or par le lemme 40 $\text{pgcd}(ac, bc) = c$. □

Le théorème suivant est la réciproque de la propriété 5,

Théorème 43 (Lemme d'Euclide)**.** *Tout élément irréductible d'un anneau à pgcd est premier.*

Preuve. Soient $a, b, c \in A$ avec a irréductible et tels que $a|bc$. Par l'existence de tout pgcd, il existe $k \in A$ tel que $a = \text{pgcd}(a, b)k$. Or a est irréductible donc $\text{pgcd}(a, b) \in A^\times$ ou $k \in A^\times$. Si $\text{pgcd}(a, b)$ est inversible alors a et b sont premiers entre eux, le lemme de Gauss donne $a|c$. Sinon si $k \in A^\times$ alors $a|\text{pgcd}(a, b)$ donc $a|b$. □

Proposition 44. *Soient $a, b \in A$. Si A est intègre alors $ab = pgcd(a, b)ppcm(a, b)$.*

Preuve. Posons $\text{ppcm}(a, b) = m$ et $\text{pgcd}(a, b) = 1$, quitte à diviser a par leur pgcd. Il existe donc $k \in A$ tel que $m = ak$. Comme a et b sont premiers entre eux par le lemme de Gauss, on obtient $b|k$ donc $ab|m$. D'où $\text{ppcm}(a, b) = ab$. □

3.2 Anneau factoriel

Définition 45 (Anneau factoriel)**.** Un anneau intègre A est dit factoriel s'il vérifie les deux propriétés suivantes :

- Pour tout élément a, non nul et non inversible, il existe une suite finie $p_1, ..., p_n$ d'éléments irréductibles de A dont a est le produit : $a = p_1...p_n$
- Si, pour un tel élément a, on a deux telles suites $p_1, ..., p_n$ et $q_1, ..., q_m$, alors $m = n$ et il existe une permutation σ de $\{1, ..., n\}$, ainsi que des éléments inversibles $u_1, ..., u_n$ tels que $p_i = u_i q_{\sigma(i)}$ pour tout $i \in \{1, ..., n\}$ (ie. la décomposition de a est unique à l'ordre des facteurs et associations près).

Définition 46 (Système représentatif)**.** Dans un anneau intègre A, on dit que $\mathcal{S}$ est un système représentatif d'irréductibles si tout élément irréductible de A est associé à un unique élément de $\mathcal{S}$.

Soit A un anneau factoriel et $\mathcal{S}$ un système représentatif d'irréductible de A.

Proposition 47. *Pour tout élément $a \in A$ non nul non inversible, il existe une unique décomposition de la forme suivante :*

$$a = u_a \prod_{p \in \mathcal{S}} p^{v_p(a)}$$

avec u_a un élément inversible de A et $v_p(a) \in \mathbb{N}$ presque tous nuls.

Preuve. (Existence) Soit $a \in A$ non nul non inversible. Comme A est factoriel a est décomposable en produit d'irréductibles comme dans la définition 45. Soit $a = p_1...p_n$ une décomposition en produit d'irréductibles de a. Alors par définition de $\mathcal{S}$, pour tout $k \in \{1, ..., n\}$, il existe $s_k \in \mathcal{S}$ tel que $p_k \sim s_k$. Donc pour tout $k \in \{1, ..., n\}$, il existe $s_k \in \mathcal{S}$, et $u_k \in A^\times$ tels que $p_k = u_k s_k$. D'où $a = \prod_{k \in \{1,...,n\}} u_k s_k$, par commutativité on $a = U \prod_{k \in \{1,...,n\}} s_k$ avec $U = u_1...u_n$. En indexant le produits par $\mathcal{S}$ on obtient : $a = U \prod_{s \in \mathcal{S}} s^{v_s}$. De plus les v_s sont presque tous nuls en effet si $v_s \neq 0$ alors il existe $k \in \{1, ..., n\}$ tel que $s \sim p_k$. Donc $(v_s)_{s \in \mathcal{S}}$ admet au plus n éléments non nuls.
(Unicité) Soit $a \in A$ non nul non inversible. Soient $u, u' \in A^\times$ et $(v_p)_{p \in \mathcal{S}}, (w_p)_{p \in \mathcal{S}} \in \mathbb{N}^{\mathcal{S}}$, tels que :

$$a = u \prod_{p \in \mathcal{S}} p^{v_p} = u' \prod_{p \in \mathcal{S}} p^{w_p}$$

Supposons par l'absurde qu'il existe $q \in \mathcal{S}$ tel que $v_q \neq w_q$ alors $v_q < w_q$ ou $v_q > w_q$. Considérons le cas ou $v_q < w_q$. Alors on peut diviser les deux produits par q^{v_q} ce qui donne : $u \prod_{p \in \mathcal{S} \setminus \{q\}} p^{v_p} = u' q^{w_q - v_q} \prod_{p \in \mathcal{S} \setminus \{q\}} p^{w_p}$. Ce sont deux décompositions en facteurs en irréductible de même valeur dans un anneau factoriel donc elle sont identiques à associations près. D'où il existe $p \in \mathcal{S} \setminus \{q\}$ tel que $p \sim q$ ce qui est absurde par définition d'un système représentatif d'irréductibles. □

Lemme 48. *Soient $a, b \in A$ alors on a $a|b$ si et seulement si pour tout $p \in \mathcal{S}, v_p(a) \leq v_p(b)$.*

Preuve. Montrons d'abord que $p \in \mathcal{S}$ divise $b \in A$ si et seulement si $v_p(b) \geq 1$. Si $p|b$ alors il existe $k \in A$ tel que $b = pk$. Posons $k = u_k \prod_{q \in \mathcal{S}} q^{v_q(k)}$ alors $b = p^{1+v_p(k)} u_k \prod_{q \in \mathcal{S}\setminus\{p\}} q^{v_q(k)}$ par unicité d'une telle décomposition, et $v_p(b) = 1 + v_p(k) \geq 1$. La réciproque est directement donné par la décomposition de b. Maintenant si $a|b$ supposons par l'absurde qu'il existe $p \in \mathcal{S}$ tel que $v_p(a) > v_p(b)$. Quitte à diviser b et a par $p^{v_p(b)}$, supposons $v_p(a) > v_p(b) = 0$. Alors $p|a$ donc $p|b$ ce qui est absurde. Finalement si pour tout $p \in \mathcal{S}, v_p(a) \leq v_p(b)$ alors il suffit d'identifier a dans la décomposition de b, c'est à dire $b = au_a^{-1}u_b \prod_{p \in \mathcal{S}} p^{v_p(b)-v_p(a)}$. Donc $a|b$. □

Corollaire 49. *Le nombre de diviseurs d'un élément non nul non inversible est fini à associations près.*

Remarque ∴ Cela vient du fait que pour $a \in A$ non nul non inversible la suite $(v_p(a))_{p \in \mathcal{S}}$ est presque nulle.

Corollaire 50. *Les idéaux principaux de A vérifient la condition de chaine ascendante.*

Preuve. Soient $a \in A$ et $(a_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}}$ telle que $(a) \subset (a_1) \subset ... \subset (a_n) \subset ...$. Supposons que a est non nul non inversible. En effet si a et tout les (a_k) sont nuls alors la suite est déjà stationnaire égale à $\{0\}$. Et si a est inversible, alors $(a) = A$ et donc la suite est déjà stationnaire égale à A. Comme a est non nul non inversible, il possède un nombre fini de diviseurs à association près. Supposons par l'absurde que la suite n'est pas ultimement stationnaire alors pour tout $n \in \mathbb{N}$, il existe $m > n$ tel que $(a_m) \neq (a_n)$, d'où $a_n \not\sim a_m$ et $a_m|a$ donc a à une infinité de diviseurs à association près ce qui est absurde. □

Proposition 51. *Tout anneau factoriel est un anneau à pgcd.*

Preuve. Soient $a, b \in A$ posons $d = \prod_{p \in \mathcal{S}} p^{\min(v_p(a), v_p(b))}$. Montrons qu'il s'agit d'un pgcd de a et b. Pour tout $p \in \mathcal{S}, v_p(d) = \min(v_p(a), v_p(b))$. Donc par le lemme précédent on a : $d|a$ et $d|b$. Soit $d' \in A$ tel que $d'|a$ et $d'|b$. Alors on a pour tout $p \in \mathcal{S}, v_p(d') \leq v_p(a)$ et $v_p(d') \leq v_p(b)$. Donc par définition de d : pour tout $p \in \mathcal{S}, v_p(d') \leq v_p(d)$ d'où $d'|d$. □

Proposition 52. *Un anneau intègre est factoriel si et seulement si tout ses éléments non nuls non inversibles sont produits d'éléments premiers.*

Preuve. ($\Rightarrow$) Dans A tout élément non nul non inversible admet une décomposition en facteurs irréductibles, mais comme un anneau factoriel est un anneau à pgcd, tout irréductible est premier. Donc tout élément de A est produit d'éléments premiers.
($\Leftarrow$) Soit B un anneau dans lequel tout élément non nul non inversible est produit d'éléments premiers, soit $a \in B$. Alors $\exists p_1, ..., p_n \in B$ premiers tels que $a = p_1...p_n$. Comme dans tout anneau intègre, les éléments premiers sont irréductibles, a est produit d'irréductibles. Supposons que a admet une autre décomposition en facteurs irréductibles $a = q_1...q_m$. On a alors $p_1...p_n = q_1...q_m$. Donc $p_1|q_1...q_n$ comme p_1 est premier il divise un des q_k, supposons qu'il s'agit de q_1 quitte à changer les indices. Il existe donc $u_1 \in B$ tel que $q_1 = p_1u_1$ or q_1 est irréductible et p_1 est non inversible donc u_1 est inversible. Et on obtient donc $p_1 \sim q_1$ et $p_2...p_n = u_1q_2...q_m$. On a de nouveau $p_2|u_1q_2...q_m$, p_2 est premier donc ne divise pas u_1, il divise donc un des q_k avec $k \in \{2, ..., n\}$, on suppose qu'il s'agit de q_2 et comme précédemment on obtient : $p_2 \sim q_2$ et $p_3...p_n = u_2q_3...q_m$. On continue par récurrence mais au final trois cas se présentent en fonction de m et n :

-Supposons par l'absurde que $m < n$. Alors on obtient au bout de m opérations : $p_{m+1}...p_n = u_m$. Donc p_{m+1} est inversible ce qui est absurde.

-Supposons par l'absurde que $m > n$. Alors on obtient au bout de n opérations : $1 = u_n q_{n+1}...q_m$. Donc q_{n+1} est inversible ce qui est absurde.

Donc nécessairement $n = m$ et dans ce cas on obtient bien : pour tout $k \in \{1, ..., n\}, p_k \sim q_k$. Donc a admet une unique décomposition en facteurs irréductibles à produits d'inversibles, associations et ordre près. □

3.3 Anneau de Bézout

Définition 53 (Anneau de Bézout)**.** (Par Bourbaki [1] exercice 20 page 279) Un anneau de Bézout est un anneau intègre dans lequel tout idéal de type finis est principal.

Soit A un anneau de Bézout.

Proposition 54. *A est un anneau à pgcd, de plus un pgcd de $a_1, ..., a_n \in A$ est $d \in A$ tel que $(d) = (a_1, ..., a_n)$.*

Preuve. Soient $a_1, ..., a_n$ dans A alors il existe d tel que $(d) = (a_1, ..., a_n)$ par la propriété 34 on a que d est leur pgcd. □

Théorème 55 (de Bachet-Bézout)**.** *Soient $a, b \in A$, si $d = pgcd(a, b)$ alors il existe $u, v \in A$ tels que $au + bv = d$.*

Preuve. Soient a et b dans A et $d \in A$ un de leur pgcd. A est de Bézout alors il existe c dans A tel que $(a, b) = (c)$ par la propriété 34 : c est un pgcd de a et b donc $d \sim c$ d'où $(a, b) = (c) = (d)$. $d \in (a, b)$ donc il existe $u, v \in A$ tels que $au + bv = d$. □

En corollaire car c'est la même démonstration : Réciproque de la propriété 16

Corollaire 56 (Théorème de Bézout)**.** *Pour $a, b \in A$. Si a et b sont premiers entre eux alors ils sont étrangers.*

Réciproque de la propriété 8.

Proposition 57. *Un élément premier de A est extrémal.*

Preuve. Soient $p, a \in A$ tels que p soit premier et $p \nmid a$. On veut montrer qu'alors ils sont étrangers, or d'après le théorème de Bézout il nous suffit de montrer qu'ils sont premiers entre eux. Soit $d \in A$ tel que $d|p$ et $d|a$, comme p est irréductible $d \in A^\times$ ou $d \sim p$. Or $p \nmid a$ et $d|a$ donc forcément d est inversible. □

Réciproque de la propriété 37.

Proposition 58. *Si $a \in A$ est irréductible alors (a) est maximal*

Preuve. Soit $a \in A$ irréductible et J un idéal de A tel que $(a) \subsetneq J \subset A$. Alors il existe $b \in J$ tel que $b \notin (a)$ donc $a \nmid b$. Or dans un anneau de Bézout on a la chaine d'implication suivante :

$$a \text{ irréductible} \Rightarrow a \text{ premier} \Rightarrow a \text{ extrémal}$$

Donc a et b sont étrangers d'où $(a) + (b) = (1) \subset J$ donc $J = A$. □

3.4 Anneau principal

Définition 59 (Anneau principal)**.** Un anneau intègre est principal si tout ses idéaux sont principaux.

Soit A un anneau principal.

Proposition 60. *Les idéaux de A vérifient la condition de chaine ascendante.*

Preuve. Soit $(I_n)_{n\in\mathbb{N}}$ une suite d'idéaux de A croissante. Posons $U = \cup_{n\in\mathbb{N}} I_n$. U est un idéal, on le montre grâce à la croissance de la suite. Comme A est principal, il existe $u \in A$ tel que $(u) = U$. Or $u \in U$ alors il existe $m \in \mathbb{N}$ tel que $u \in I_m$ et on a donc $(u) \subset I_m \subset (u)$ donc $I_m = U$. Finalement pour tout $k \geq m$ on obtiens $U = I_m \subset I_k \subset U$ donc la suite est ultimement stationnaire. □

Proposition 61. *Tout élément non nul non inversible de A admet un facteur irréductible.*

Preuve. Soit $a \in A$ un élément non nul non inversible supposons qu'il n'admet pas de facteur irréductible. a n'est pas irréductible donc (a) n'est pas maximal donc il existe un idéal propre B_1 de A tel que $(a) \subsetneq B_1$. A est principal donc il existe b_1 dans A tel que $(b_1) = B_1$. Comme $(a) \subsetneq (b_1)$, b_1 n'est pas irréductible car a n'a pas de facteur irréductible. Donc (b_1) n'est pas maximal donc on peut trouver b_2 dans A non irréductible pour les mêmes raisons tel que $(a) \subsetneq (b_1) \subsetneq (b_2)$. On construit ainsi une suite d'idéaux de A strictement croissante ce qui est absurde. □

Théorème 62. *Un anneau B est principal si et seulement s'il est factoriel et de Bézout.*

Preuve. ($\Rightarrow$) Soit I un idéal de type fini de B qui est principal alors I est principal donc B est de Bézout. Montrons que B est aussi factoriel. Posons :

$$E = \{a \in B\backslash\{0\} | a \notin B^\times \text{ qui n'est pas décomposable en produit de facteur irréductible de } B\}$$

Supposons que $E \neq \varnothing$. Soit $a_1 \in E$, donc a_1 n'est pas irréductible, il existe $b, c \in B^\times$ tels que $a_1 = bc$. Supposons que b et c ne sont pas dans E : alors b et c admettent des décompositions en produits d'irréductibles de B, donc a_1 aussi ce qui est absurde car $a_1 \in E$. Donc b ou c est dans E. Quitte à choisir nommons a_2 celui qui est dans E. On obtient $a_2|a_1$ mais $a_1 \not\sim a_2$ d'où $(a_1) \subsetneq (a_2)$. De la même manière on continue et on forme une suite d'idéaux telle que : $(a_1) \subsetneq ... \subsetneq (a_n) \subsetneq ...$, ce qui contredit la condition de chaine ascendante des idéaux de B. Donc E est vide. Tout élément non nul non inversible de B admet une décomposition en facteur irréductible de B. Comme B est de Bézout donc un anneau à pgcd, il s'agit d'une décomposition en facteurs premiers donc B est factoriel.
($\Leftarrow$) Soit B un anneau de Bézout et factoriel montrons qu'il est principal. Soit I un idéal de B et supposons qu'il n'est pas principal. Soit $a_0 \in I$ alors on a $(a_0) \subset I$. Comme I n'est pas principal, il existe $a_1 \in I\backslash(a_0)$. B est de Bézout donc il existe $b_1 \in B$ tel que $(a_0, a_1) = (b_1)$. $(b_1) \subset I$ mais I n'est pas principal donc on a $(a_0) \subsetneq (b_1) \subsetneq I$. On construit ainsi une suite croissante d'idéaux telle que $(a_0) \subsetneq (b_1) \subsetneq ... \subsetneq (b_n) \subsetneq ...$. Ce qui contredit la condition de chaine ascendante des idéaux principaux de B. Donc I est principal. □

3.5 Anneau euclidien

Définition 63 (Anneau euclidien)**.** Un anneau intègre A est dit euclidien s'il existe une application $\nu : A\backslash\{0\} \to \mathbb{N}$ telle que :

$$\forall (a, b) \in A \times A\backslash\{0\}, \exists q, r \in A \text{ tels que } a = bq + r \text{ avec } r = 0 \text{ ou } \nu(r) < \nu(b)$$

Une telle application est nommée stathme.

Proposition 64. *Un anneau euclidien est principal.*

Preuve. Soit I un idéal de A qui est euclidien. Montrons que I est principal. Supposons $I \neq A$ et I non nul sinon il est déjà principal. Alors $E = \{x \in I \text{ tel que } x \neq 0\} \neq \varnothing$, soit $a \in E$ tel que $\forall b \in E, \nu(a) \leq \nu(b)$ et montrons que $I \subset (a)$. Supposons qu'il existe $b \in I$ tel que $b \notin (a)$ alors $\exists q, r \in A$ tels que $b = aq + r$ avec $r \neq 0$ donc tel que $\nu(r) < \nu(a)$. Or $r \in E$ par absorption de I, ce qui contredit la minimalité de a. Donc $I \subset (a)$ et l'inclusion inverse est vrai car $a \in I$. □

Exemple 65. $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ est euclidien. Montrons que l'application :

$$\begin{array}{rccc} N: & \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ & a+ib & \longmapsto & (a+ib)(a-ib) = a^2 + b^2 \end{array}$$

est un stathme euclidien.
Soient $u, v \in \mathbb{Z}[i]$ avec v non nul. Examinons $\frac{u}{v}$ dans $Frac(\mathbb{Z}[i])$[3] $= \mathbb{Q}[i]$. $\frac{u}{v} = \frac{u\bar{v}}{N(v)}$ donc il existe $a, b \in \mathbb{Q}$ tels que $\frac{u}{v} = a + ib$, a et b sont dans $\mathbb{Q}$ donc il existe $a_0, b_0 \in \mathbb{Z}$ tels que $|a - a_0| \leq 1/2$ et $|b - b_0| \leq 1/2$. Posons $a_1 = a - a_0$ et $b_1 = b - b_0$. On a donc $\frac{u}{v} - a_0 + ib_0 = a_1 + ib_1$, d'où $u - v(a_0 + ib_0) = v(a_1 + ib_1) \in \mathbb{Z}[i]$. $N(v(a_1 + ib_1)) = N(v)N(a_1 + ib_1) = N(v)(a_1^2 + b_1^2) \leq 1/2N(v)$. Donc en posant $q = a_0 + ib_0$ et $r = v(a_1 + ib_1)$ on a $u = vq + r$ avec $N(r) < N(v)$ ou $r = 0$.

Exemple 66. Il existe des anneaux principaux non euclidiens, dans [2] il est démontré que c'est le cas de $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.

4 Construction d'anneaux

4.1 Anneaux de polynômes

Soit A un anneau commutatif unitaire.

Rappel 67 (Anneau des polynômes)**.** *L'anneau* $A[X] = \{\sum_{i=0}^{n} a_i X^i | a_i \in A, n \in \mathbb{N}\}$*, muni des lois d'addition et de multiplication de polynômes usuelles, est appelé l'anneau des polynômes à une indéterminée* X *sur* A*.*

Rappel 68 (Degré d'un polynôme)**.** *Soit* $f \in A[X]$ *non nul tel que* $f = \sum_{i=0}^{n} a_i X^i$*. Le degré de* f*, alors noté* $\deg(f)$*, est donné par :* $\deg(f) = \max(\{i \in \mathbb{N} | a_i \neq 0\})$*.*

Théorème 69. *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.*

[3]Voir la définition 83.

Preuve. 1. $\Rightarrow$ 2. Montrons que l'application deg : $A[X]\backslash\{0\} \longrightarrow \mathbb{N}$, qui donne le degré d'un polynôme non nul est un stathme euclidien. Soient $f, g \in A[X]$ avec $f = \sum_{i=0}^{n} a_i X^i$ et $g = \sum_{i=0}^{m} b_i X^i$ tels que g est non nul et a_n et b_m aussi. Si f est nul ou $\deg(f) < \deg(g)$ on pose $q = 0$ et $r = f$ ce qui satisfait à la définition d'un stathme. Si $\deg(f) \geq \deg(g)$. Raisonnons par récurrence sur $k = \deg(f) - \deg(g) \in \mathbb{N}$. Initialisation : Si $n = \deg(f) = \deg(g)$, posons $q = a_n b_n^{-1}$ et $r = f - qg$. On a bien $f = qg + r$ et $\deg(r) < \deg(f) = \deg(g)$ ou $r = 0$ (car les deux monômes de plus haut degré de f et qg s'annulent).
Hérédité : Soit $k \in \mathbb{N}$. Supposons que l'on peut trouver un couple «(q, r)» dès que $\deg(f) - \deg(g) \leq k$. Supposons $\deg(f) - \deg(g) = k+1$. Posons $q' = a_n b_m^{-1} X^{k+1}$ et $r' = f - q'g$. De même que précédemment on obtient $\deg(r') < \deg(f)$ ou $r = 0$. Donc on peut appliquer l'hypothèse de récurrence à r' et g. Il existe q'' et r dans $A[X]$ tels que $r' = q''g + r$ avec $r = 0$ ou $\deg(r) < \deg(g)$.
D'où,$f = q'g + r' = (q' + q'')g + r$ avec $r = 0$ ou $\deg(r) < \deg(g)$.
2. $\Rightarrow$ 3. Corollaire direct de la propriété 64.
3. $\Rightarrow$ 4. Corollaire direct du théorème 62.
4. $\Rightarrow$ 1. Soit $a \in A$ non nul. Comme $A[X]$ est de Bézout le pgcd de a et X existe. Soit $d \in A[X]$ un de leur pgcd. Comme $d|a$, $\deg(d) = 0$ or $d|X$ donc il existe $q \in A[X]$ tel que $X = dq$.
$deg(X) = deg(dq) = deg(q) = 1$ donc il existe $q', r \in A$ tels que $q = q'X + r$. D'où $X = dq'X + dr$ et dont on tire $r = 0$ et $dq' = 1$ donc d est inversible. $\text{pgcd}(a, X) = 1$ et comme $A[X]$ est en particulier de Bézout, il existe $u, v \in A[X]$ tels que $au + Xv = 1$. Le monôme de degré 0 de $au + bv$ vaut un et est de la forme $au' = 1$ avec $u' \in A$ donc a est inversible. □

Définition 70 (Contenu)**.** Si A est à pgcd. Soit $f = \sum_{i=0}^{n} a_i X^i$ non nul. Un contenu $\mathcal{C}(f)$ de f est un pgcd des coefficients a_i de f.

Définition 71. (Partie primitive) Soit un polynôme $f \in A[X]$. Si son contenu est inversible on dit que f est primitif. Le polynôme $f^\sharp \in A[X]$ tel que $f = \mathcal{C}(f)f^\sharp$ est dit partie primitive de f.

Lemme 72. *Soit A un anneau à pgcd. Si $a \in A$ et $f \in A[X]$ alors $\mathcal{C}(af) = a\mathcal{C}(f)$.*

Preuve. Soient $a \in A$ et $f = \sum_{i=0}^{n} b_i X^i$. Comme A est un anneau à pgcd :

$$\mathcal{C}(af) = \text{pgcd}(ab_1, ..., ab_n) = a\text{pgcd}(b_1, ...b_n) = a.\mathcal{C}(f)$$

□

Remarque ∴ La partie primitive d'un polynôme est donc un polynôme primitif.

Lemme 73 (de Gauss)**.** *Si A est à pgcd et $f, g \in A[X]$ non nuls alors $\mathcal{C}(fg) = \mathcal{C}(f)\mathcal{C}(g)$.*

Preuve. Soient $f, g \in A[X]$ non nul. Supposons f et g primitifs quitte à les diviser par leur contenu. Ceci nous ramène à montrer que le produit de deux polynômes primitifs est primitif. Si $\deg(f)$ ou $\deg(g)$ est nul c'est déjà fait. Procédons par récurrence sur le degré de g. Soit $m \in \mathbb{N}$ supposons qu'alors le produit de f avec tout autre polynôme primitif de degré strictement inférieur à m est primitif. Posons $f = \sum_{i=0}^{n} a_i X^i$ et $g = \sum_{i=0}^{m} b_i X^i$. Soit $d \in A$ tel que d divise les coefficients de fg. En particulier, pour tout $p \in \{1, ..., n\}, d|a_p b_m$ donc $d|\text{pgcd}(a_0 b_m, ..., a_n b_m) = b_m$. Et par ailleurs pour tout $p \in \{1, ..., n\}$ et tout $q \in \{1, ..., m-1\}, d|a_p b_q$. En posant $\tilde{g} = \sum_{i=0}^{m-1} b_i X^i$, on a donc $d|\mathcal{C}(f\tilde{g}) = \mathcal{C}(\tilde{g})\mathcal{C}(f\tilde{g}^\sharp)$. Comme $\deg(\tilde{g}^\sharp) < m$ par hypothèse de récurrence $\mathcal{C}(f\tilde{g}^\sharp) = 1$, on obtient $d|\mathcal{C}(\tilde{g})$. Au final $d|\text{pgcd}(b_0, ..., b_{m-1})$ et $d|b_m$ donc $d \sim 1$ car g est primitif. □

Théorème 74. *Si A est un anneau intègre à pgcd alors $A[X]$ aussi.*

Preuve. (Traduite et adaptée de la preuve présente dans [3]) Soient $f, g \in A[X]$. Supposons f et g non nul. Soit K le corps des fractions[4] de A. Alors $f^\sharp, g^\sharp \in A[X] \subset K[X]$ admettent un pgcd dans $K[X]$, notons le d'. Comme d' est unique à produit d'éléments de K près, on peut le supposer dans $A[X]$ quitte à le multiplier par le dénominateur commun de ses coefficients, et le supposer primitif quitte à le diviser par son contenu. Maintenant montrons que $d = \text{pgcd}(\mathcal{C}(f), \mathcal{C}(g))d'$ est un pgcd de f et g dans $A[X]$.
Premièrement montrons que d' est un pgcd de $f^\sharp$ et $g^\sharp$ dans $A[X]$. Comme $d'|f^\sharp$ dans $K[X]$ on peut écrire $\frac{f^\sharp}{d'} = \frac{a}{b}q$ avec $a, b \in A$ et $q \in A[X]$ primitif. Comme $bf^\sharp = ad'q$, on a $b = \mathcal{C}(bf^\sharp) \sim \mathcal{C}(ad'q) = a$ donc $\frac{a}{b} \in A^\times$ donc $d'|f^\sharp$ dans $A[X]$. De même $d'|g^\sharp$ dans $A[X]$. Comme $K[X]$ est de Bézout, il existe $u, v \in A[X]$ et $c \in A\backslash\{0\}$ tels que $cd' = uf^\sharp + vg^\sharp$. Soit $h \in A[X]$ un diviseur commun de $f^\sharp$ et $g^\sharp$ dans $A[X]$. Alors $h|cd'$, et $\mathcal{C}(h)|\mathcal{C}(f^\sharp) = 1$. En écrivant $\frac{cd'}{h} = \frac{a}{b}k$ avec $a, b \in A\backslash\{0\}$ et $k \in A[X]$ primitif. Et en étudiant le contenu de $bcd' = ahk$, on obtient $bc \sim a$, $\frac{d'}{h} = \frac{a}{bc}k \sim k \in A[X]$, d'où h divise d' dans $A[X]$.
Deuxièmement montrons que d est le pgcd voulu. Il est maintenant clair que :

$$d = \text{pgcd}(\mathcal{C}(f), \mathcal{C}(g))d'|\mathcal{C}(f)f^\sharp = f$$

et que $d|g$ dans $A[X]$. Soit $h \in A[X]$ qui divise f et g. Comme $h|f$ on a $\mathcal{C}(h)|\mathcal{C}(f)$ et $h^\sharp|f^\sharp$. Pareillement $\mathcal{C}(h)|\mathcal{C}(g)$ et $h^\sharp|g^\sharp$. Au total, $\mathcal{C}(h)|\text{pgcd}(\mathcal{C}(f), \mathcal{C}(g))$, $h^\sharp|d'$ Donc $h|d$. □

Lemme 75. *Soit A un anneau intègre à pgcd . Si $f, g \in A[X]$ sont non nuls avec $g|f$ et $\deg(f) = \deg(g)$ alors $f^\sharp = g^\sharp$.*

Preuve. g divise f dans $A[X]$ donc il existe $q \in A[X]$ tel que $f = qg$. On a donc $\deg(f) = \deg(q) + \deg(g)$ car A est intègre, or $\deg(f) = \deg(g)$ d'où $\deg(q) = 0$ donc $q \in A$. Ce qui donne $\mathcal{C}(f) = \mathcal{C}(qg) = q\mathcal{C}(g)$. D'où $\mathcal{C}(f)f^\sharp = q\mathcal{C}(g)g^\sharp$ et par intégrité on a $f^\sharp = g^\sharp$. □

Proposition 76. *Soit A un anneau intègre à pgcd. Si les idéaux principaux de A vérifient la condition de chaine ascendante alors ceux de $A[X]$ aussi.*

Preuve. Soit $[(f_n)]_{n\in\mathbb{N}}$ une suite croissante d'idéaux principaux de $A[X]$. Supposons de plus f_1 non nul non inversible, car si la suite est nulle ou si tout élément est inversible la suite est déjà stationnaire. Et sinon il suffit de commencer la suite au premier terme non nul non inversible. Pour des questions de degré on sait que pour tout $f, g \in A[X]$, $\deg(g) \leq \deg(f)$ si $(f) \subset (g)$. Raisonnons par récurrence sur le degré de f_1.
Montrons pour tout $n \in \mathbb{N}$ la propriété suivante, $\mathcal{P}(n)$:« Si $\deg(f_1) = n$ alors la suite est ultimement stationnaire ».
Initialisation : Si $\deg(f_1) = 0$ alors pour tout $n \in \mathbb{N}$, $\deg(f_n) = 0$. Donc $[(f_n)]_n$ est une suite d'idéaux principaux de A donc $\mathcal{P}(0)$ est déjà vérifiée par l'hypothèse sur les idéaux principaux de A.
Hérédité : Soit $n \in \mathbb{N}$ et supposons que pour tout entier naturel $k \leq n$ la propriété $\mathcal{P}(k)$ est vérifié, montrons qu'alors $\mathcal{P}(n+1)$ aussi. Deux cas se présentent, si la suite admet un terme (f_k) tel que $\deg(f_k) \leq n$ alors on prend f_k comme premier terme de la suite et c'est fini. Sinon les degrés des générateurs sont tous égaux à $n+1$. Par le lemme 75, on a que les parties primitives de tout les générateurs sont égales à celle de f_1.Posons $f^\sharp = f_1^\sharp$. Soit $k \in \mathbb{N}$, $f_{k+1}|f_k$ se réécrit $\mathcal{C}(f_{k+1})f^\sharp|\mathcal{C}(f_k)f^\sharp$ par intégrité on obtient $\mathcal{C}(f_{k+1})|\mathcal{C}(f_k)$. Or la suite $[(\mathcal{C}(f_k))]_k$ d'idéaux de A est croissante donc stationnaire. On en déduit que la suite $[(f_k)]_{k\in\mathbb{N}} = [(\mathcal{C}(f_k)f^\sharp)]_{k\in\mathbb{N}}$ est stationnaire. □

[4]Voir la définition 83.

Proposition 77. *Tout anneau à pgcd dont les idéaux principaux vérifient la condition de chaine ascendante est un anneau factoriel.*

Preuve. Soit A un anneau à pgcd dont les idéaux principaux vérifient la condition de chaine ascendante. Posons,

$$E = \{a \in A | a \text{ est non nul non inversible et n'est pas décomposable en facteurs irréductibles }\}$$

et supposons par l'absurde que E est non vide. Soit $a \in E$. Alors a n'est pas irréductible donc il existe $b, c \in A$ non nul non inversible tels que $a = bc$. Alors b ou c n'est pas irréductible par définition de a. Donc on a montré que pour tout $a \in E$, il existe $b \in E$ tel que $b|a$ et $b \not\sim a$. Avec ceci on peut donc construire par récurrence à partir de $a \in E$ une suite strictement croissante d'idéaux : $(a) \subsetneq (a_1) \subsetneq ... \subsetneq (a_n) \subsetneq ....$ Cela contredis la condition de chaine ascendante des idéaux principaux de A. Donc E est vide. Au final tout élément non nul non inversible est décomposable en produit de facteurs irréductibles, donc premiers car A est un anneau à pgcd. Donc A est factoriel □

Corollaire 78. *$A[X]$ est un anneau factoriel si et seulement si A aussi.*

Remarque :. Pour montrer que c'est suffisant il suffit de se servir des propositions précédentes. Et pour montrer que c'est nécessaire on prend une décomposition en facteurs premiers d'un éléments de A dans $A[X]$ et montre qu'il s'agit d'une décomposition en premiers de A.

4.2 Localisation

Soit A un anneau unitaire intègre.

Rappel 79 (Partie multiplicative)**.** *Un sous ensemble $S \subset A$ est une partie multiplicative si $1 \in S$ et si :*

$$\forall a, b \in A, a \in S \text{ et } b \in S \Rightarrow ab \in S$$

Soit S une partie multiplicative de A.

Rappel 80. *La relation sur $A \times S$ suivante :*

$$(a, s) \approx (a', s') \Leftrightarrow (as' - a's) = 0$$

est une relation d'équivalence.

Rappel 81 (Localisé)**.** *L'ensemble quotient $A \times S/\approx$ s'appelle le localisé en S de A que l'on note $S^{-1}A$. Nous noterons $\frac{a}{s}$ la classe de (a, s). De plus pour tout $a \in A$, $(a, 1) \in A$ sera noté a*

Rappel 82. *$S^{-1}A$ muni des lois de compositions internes suivantes :*

$$+ : S^{-1}A \times S^{-1}A \to S^{-1}A, \frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

$$\times : S^{-1}A \times S^{-1}A \to S^{-1}A, \frac{a}{b} \times \frac{a'}{b'} = \frac{aa'}{bb'}$$

est un anneau.

Définition 83 (Corps des fractions)**.** On appelle corps des fractions de A le corps $S^{-1}A$ avec $S = A\backslash\{0\}$ et on le note $Frac(A)$.

Théorème 84. *Si A est un anneau à pgcd alors $S^{-1}A$ aussi.*

Preuve. Soient $a, b \in A$, montrons que si $d = \text{pgcd}(a, b)$ dans A alors d est un pgcd de a et b dans $S^{-1}A$. Posons $d = \text{pgcd}_A(a, b)$, il est clair que d divise a et b dans $S^{-1}A$. Soit $\frac{d'}{s} \in S^{-1}A$ un diviseur commun à a et b dans $S^{-1}A$. Alors d' est aussi un diviseur commun à a et b dans $S^{-1}A$. Montrons qu'il divise d dans $S^{-1}A$ et alors ce sera le cas pour $\frac{d'}{s}$. Il existe $\frac{u}{v}$ et $\frac{u'}{v'}$ dans $S^{-1}A$ tels que $d'\frac{u}{v} = a$ et $d'\frac{u'}{v'} = b$. On en déduit que $d'\frac{uv'}{vv'} = a$ et $d'\frac{u'v}{vv'} = b$. Posons $k = uv'$,$k' = u'v$ et $m = vv'$. On écrit $d'k = am$ et $d'k' = bm$, et comme d' et m sont dans A on peut poser $m_0 = pgcd_A(d', m)$, $d' = d''m_0$ et $m = m'm_0$. On obtient que $m'|d''k$ et $m'|d''k'$ avec m' et d'' premiers entre eux donc par le lemme de Gauss $m'|k$ et $m'|k'$. Donc il existe k_0 et k_1 dans A tels que $d''k_0 = a$ et $d''k_1 = b$ alors $d''|a$ et $d''|b$ dans A d'où $d''|d$ dans A. Au final on a $d' = d''m_0|dm_0$ dans A, donc $d'|dm$ avec $m = vv' \in S$ donc $d'|d$ dans $S^{-1}A$. Maintenant soient $\frac{a}{s}$ et $\frac{b}{t}$ dans $S^{-1}A$ montrons que $d = \text{pgcd}(a, b)$ dans A, est un de leur pgcd. Il est clair que d est un de leur diviseur commun dans $S^{-1}A$. Soit d' un diviseur commun de $\frac{a}{s}$ et $\frac{b}{t}$, alors il existe $\frac{u}{v} \in S^{-1}A$ tel que $\frac{a}{s} = d'\frac{u}{v}$ donc $a = d'\frac{us}{v}$ donc d' divise a dans $S^{-1}A$ de même $d'|b$. Comme $a, b \in A$ leur pgcd dans $S^{-1}A$ existe et c'est d donc $d'|d$ dans $S^{-1}A$. □

Lemme 85. *Soit $p \in A$ avec A à pgcd et p premier. Si p divise un élément de S dans A alors il est inversible dans $S^{-1}A$ ou premier dans $S^{-1}A$.*

Preuve. Supposons qu'il existe $s \in S$ tel que $p|s$ dans A. Alors il existe $k \in A$ tel que $s = pk$. Donc en divisant par s dans $S^{-1}A$ on a $p\frac{k}{s} = 1$ donc p est inversible dans $S^{-1}A$. Supposons que p ne divise aucun élément de S. Soient $\frac{a}{s}$ et $\frac{b}{t}$ dans $S^{-1}A$ tels que p divise leur produit alors p divise ab dans $S^{-1}A$. Donc il existe $\frac{u}{v} \in S^{-1}A$ tel que $p\frac{u}{v} = ab$, d'où $pu = abv$. Comme p est premier dans A et que $p|abv$ dans A, $p|a$ ou $p|b$ ou $p|v$. Or $v \in S$ donc $p|a$ ou $p|b$ dans A. D'où $p|\frac{a}{s}$ ou $p|\frac{b}{t}$ dans $S^{-1}A$. □

Théorème 86. *Si A est factoriel alors $S^{-1}A$ aussi.*

Preuve. Soit $\frac{a}{s} \in S^{-1}A$ non nul non inversible avec A factoriel. Alors $a \in A$ et est non nul non inversible donc il existe $p_1, ..., p_n \in A$ premiers dans A tels que $a = p_1...p_n$. On a $\frac{a}{s} = \frac{p_1...p_n}{s}$. Comme $\frac{a}{s}$ est non nul non inversible dans $S^{-1}A$, au moins un des facteurs premiers de a ci-dessus n'est pas inversible. Donc il existe un entier naturel $m \leq n$ non nul et $q_1, ..., q_m \in \{p_1, ..., p_n\}$ et $u \in S^{-1}A^\times$ tels que $p_1...p_n = uq_1...q_m$ avec $q_1, ..., q_m$ premier dans $S^{-1}A$. Donc $\frac{a}{s} = \frac{u}{s}q_1...q_m$ donc on a trouvé une factorisation en facteurs premiers de $\frac{a}{s}$ dans $S^{-1}A$. De plus $S^{-1}A$ est intègre donc $S^{-1}A$ est factoriel. □

Théorème 87. *Si A est un Anneau de Bézout alors $S^{-1}A$ aussi.*

Preuve. Soient $(\frac{a_i}{s_i})_{i\in\{1,...,n\}}$ dans $S^{-1}A$ avec A de Bézout. Notons entre crochets les idéaux engendrés dans $S^{-1}A$. Montrons que l'idéal de type fini $[\frac{a_1}{s_1}, ..., \frac{a_n}{s_n}]$ est principal. On constate que $[\frac{a_1}{s_1}, ..., \frac{a_n}{s_n}] = [a_1, ..., a_n]$ en effet pour tout $i \in \{1, ..., n\}, a_i|\frac{a_i}{s_i}$ et $\frac{a_i}{s_i}|a_i$ dans $S^{-1}A$. Posons $d = \text{pgcd}(a_1, ..., a_n)$ alors montrons que $[d] = [a_1, ..., a_n]$, d est un diviseur commun de $a_1, ..., a_n$ dans $S^{-1}A$ donc on a $[a_1, ..., a_n] \subset [d]$. Comme A est de Bézout on a $(d) = (a_1, ..., a_n) \subset [a_1, ..., a_n]$ donc $d \in [a_1, ..., a_n]$. Au final $[d] = [a_1, ..., a_n]$. □

Corollaire 88. *Si A est principal alors $S^{-1}A$ aussi.*

4.3 Anneau quotient

Soit A un anneau commutatif unitaire et I un idéal de A

Rappel 89. *La relation binaire sur A suivante :*

$$\forall a, b \in A, a \backsim b \Leftrightarrow a - b \in I$$

est une relation d'équivalence. De plus elle est compatile avec les lois de A c'est à dire :

$$\forall a, b, c \in A, a \backsim b \Rightarrow a + c \backsim b + c \text{ et } ac \backsim bc$$

Rappel 90 (Anneau quotient)**.** *On appelle anneau quotient A par I l'anneau $(A/\backsim, +, \times)$ avec $A/\backsim$ l'ensemble des classes d'équivalences des éléments de A modulo $\backsim$. Et les lois de compositions internes $+$ et $\times$ déduites de celles de A. On notera $\bar{a}$ l'élément de $A/\backsim$ qui est la classe d'équivalence de $a \in A$.*

Remarque :. On notera A/I l'anneau quotient de A par I.

Pour étudier les propriétés arithmétiques de A/I, l'intégrité étant nécessaire et au vu de la propriété 24 on pose que I est premier.

Proposition 91. *Si A est de Bézout alors A/I aussi.*

Preuve. Soit $(\bar{a_1}, .., \bar{a_n}) \subset A/I$ un idéal de type finis, montrons qu'il est principal. A est de Bézout donc il existe $d \in A$ tel que $(a_1, ..., a_n) = (d) \in A$. Pour tout $k \in \{1, ..., n\}$, il existe $c_k \in A$ tel que $dc_k = a_k$ donc $\bar{d}\bar{c_k} = \bar{a_k}$. Par ailleurs il existe $u_1, ..., u_n \in A$ tels que $a_1u_1 + ... + a_nu_n = d$ donc $\bar{a_1}\bar{u_1} + ... + \bar{a_n}\bar{u_n} = \bar{d}$. Au total on a donc $(\bar{a_1}, .., \bar{a_n}) = (\bar{d}) \subset A/I$. □

Proposition 92. *Si A est principal(resp. euclidien) alors A/I aussi.*

Preuve. On a les implications suivantes :

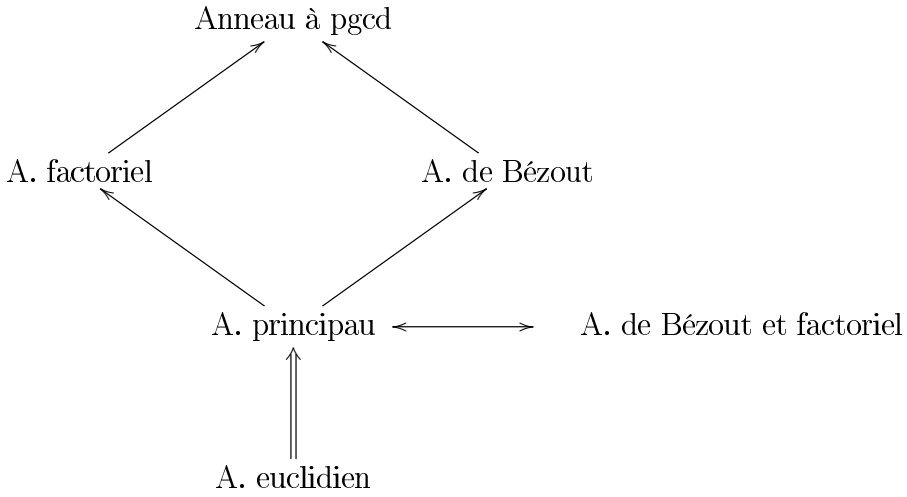
A est euclidien $\Rightarrow A$ est principal $\Rightarrow I$ est maximal
$\Rightarrow A/I$ est un corps
$\Rightarrow A/I$ est euclidien donc principal □

Exemple 93. $\mathbb{Z}$ est factoriel mais $\mathbb{Z}[X]/(X^2 + 5) \simeq \mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Remarque :. Cet exemple montre aussi que si A est à pgcd A/I n'est pas forcément à pgcd.

4.4 Exemples d'anneaux

Pour l'instant on a le graphe suivant :



Avec $\rightarrow$ qui signifie une inclusion, et $\Rightarrow$ une inclusion stricte.

4.4.1 Un anneau de Bézout qui n'est pas factoriel

Cet exemple et son explication est inspiré de la preuve du théorème 6 dans [4].
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. Alors Q^+ est un anneau intègre.

Proposition 94. *Q^+ est un anneau de Bézout qui n'est pas factoriel*

Preuve. Montrons d'abord que Q^+ est de Bézout. Pour ce faire montrons que les Q_k le sont. On remarque que pour tout entier naturel k, $Q_k = \mathbb{Q}[X_k]$, en effet pour $k = 2$ on a $Q_2 = \mathbb{Q}[X_1, X_2] = \mathbb{Q}[X_2^2, X_2] = \mathbb{Q}[X_2]$. Par récurrence on a facilement l'égalité pour tout k. Or $\mathbb{Q}$ est un corps donc par le théorème 69, pour tout k entier naturel, $Q_k = Q[X_k]$ est un anneau de Bézout. Soit $I = (f_1, ..., f_n)$ un idéal de type fini de Q^+. Alors il existe $k \in \mathbb{N}$ tel que $f_1, ..., f_n \in Q_k$. Q_k est de Bézout donc le pgcd de $f_1, ..., f_n$ existe, notons le d. De plus il existe $u_1, ..., u_n \in Q_k$ tels que $f_1u_1 + ... + f_nu_n = d$. Alors on a $d \in I$ donc $(d) \subset I$ dans Q^+. Et comme d est un diviseur commun de $f_1, ...f_n$ dans Q_k, d est un diviseur commun dans Q^+. Donc on a $I \subset (d)$. Au final Q^+ est bien de Bézout.
Montrons qu'il n'est pas factoriel. Supposons par l'absurde que X_1 est inversible dans Q^+ alors il existe $q \in Q^+$ non nul tel que $qX_1 = 1$. Or il existe $m \in \mathbb{N}$ tel que $q \in Q_m$ donc $qX_1 = 1$ dans Q_m. Donc $\deg(q) + 2^{m-1} = \deg(q) + \deg(X_1) = \deg(qX_1) = \deg(1) = 0$ or $\deg(q) \geq 0$ par définition ce qui est absurde. X_1 est un élément non nul non inversible de Q^+. Supposons par l'absurde que Q^+ est factoriel alors il existe $p_1, ..., p_n \in Q^+$ irréductibles dans Q^+ tels que $X_1 = p_1...p_n$. Par définition de Q^+, il existe $m \in \mathbb{N}$ tel que $p_1, ..., p_n \in Q_m$. Or dans Q_m, X_m est irréductible et $X_1 = X_m^{2^{m-1}}$. Comme $Q_m = \mathbb{Q}[X_m]$, Q_m est principal donc factoriel. Comme les $p_1, ..., p_n$ sont nécessairement irréductibles dans Q_m car sinon il ne le sont pas dans Q^+, on a deux décompositions en facteurs irréductibles de X_1, les deux décompositions sont donc unique à l'ordre et à associations près. Donc $n = 2^{m-1}$ et pour tout $k \in \{1, ..., 2^{m-1}\}$, il existe $q_k \in Q_m$ inversible tel que $p_k = q_kX_m$. Or comme les p_k sont irréductibles dans Q^+ ils le sont dans Q_{m+1}. Mais dans $Q_{m+1}, X_m = X_{m+1}^2$ avec X_{m+1} irréductible de Q_{m+1}. Donc les p_k ne sont pas irréductibles, ce qui est absurde.L'anneau Q^+ n'est donc pas factoriel. □

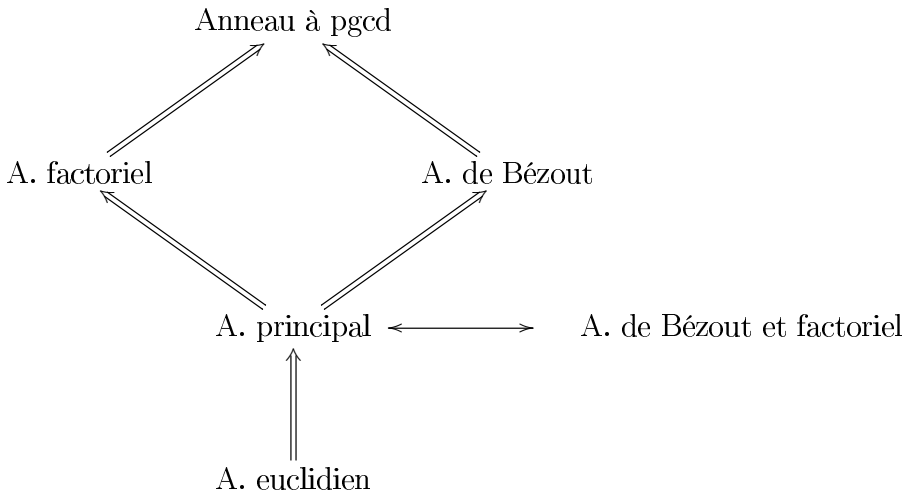
Remarque ∴ Cet anneau est donc aussi un exemple d'anneau de Bézout qui n'est pas principal (ni euclidien).

4.4.2 Un anneau à pgcd qui est ni de Bézout ni factoriel

Proposition 95. *$Q^+[X]$ l'anneau des polynômes en une indéterminé X sur Q^+ est à pgcd mais est ni factoriel ni de Bézout.*

Preuve. Comme Q^+ est de Bézout il est intègre à pgcd, donc $Q^+[X]$ aussi d'après le théorème 74. Q^+ n'est pas un corps car on a montré que $X_1 \neq 0$ n'est pas inversible. Donc le théorème 69 donne que $Q^+[X]$ n'est pas de Bézout. Enfin comme Q^+ n'est pas factoriel, le corollaire 78 donne que $Q^+[X]$ non plus. □

Conclusion Au final on a :



Avec $\Rightarrow$ qui signifie une inclusion stricte et $\leftrightarrow$ une égalité.

References

[1] Nicolas Bourbaki. *Algèbre commutative.* Eléments de mathématique. Berlin : Springer, 2006, cop. 2006., 2006.

[2] Daniel mathématicien) Perrin. *Cours d'algèbre.* CAPES-AGREG mathématiques. Paris : Ellipses, impr.1995, cop. 1996., 1995.

[3] Bruno Haible. Gauss' lemma without primes. page 4, 1994.

[4] A. N. Koryukin, A. M. Sebeldin, and A. L. Sylla. Rings with the greatest common divisor. *JOURNAL OF MATHEMATICAL SCIENCES -NEW YORK-*, 183(3):319 – 322, 2012.