Soit $\mathcal{C}$ une chaîne non-vide dans $\mathcal{X}$. Alors $\bigcup \mathcal{C}$ est un idéal dans A contenant I majorant $\mathcal{C}$; puisque $1 \notin J$ pour tout $J \in \mathcal{C}$ on a $1 \notin \bigcup \mathcal{C}$ et $\bigcup \mathcal{C} \in \mathcal{X}$. Ainsi $\mathcal{X}$ est inductif et possède un élément maximal d'après le lemme de Zorn, c'est-à-dire un idéal propre maximal. □

Exemple 3.9. Soit A l'anneau des polynômes sur $\mathbb{Z}$ sans terme constant en variables $X, X^{1/2}, X^{1/4} \ldots, X^{1/2^n}, \ldots$, avec bien sur $\left(X^{1/2^{n+1}}\right)^2 = X^{1/2^n}$ pour tout $n \in \mathbb{N}$. Soit $I_n = (X^{1/2^n})$. Puisque $X^{1/2^k}$ divise $X^{1/2^n}$ pour $k > n$, on a $(X^{1/2^n}) \leq (X^{1/2^k})$ et les $(I_n : n \in \mathbb{N})$ forment une chaîne croissante. Or, $A = \bigcup_{n\in\mathbb{N}} I_n$. Si $I_0 \leq I \lhd A$ avec I maximal, alors A/I est un corps. Puisque $I < A$ et $\bigcup_{n\in\mathbb{N}} I_n = A$ il y a $n \in \mathbb{N}$ minimal tel que $I_n \not\leq I$; on note que $n > 0$. Soit $a \in I_n \setminus I$. Alors $a^2 \in I_{n-1} \leq I$. Comme I est maximal, il est premier, et $a \in I$, une contradiction. Donc I_0 n'est pas contenu dans un idéal maximal.

Définition 3.10. Soit A un anneau, et I et J deux idéaux.

1. La *somme* de I et J est l'idéal $I + J = \{a + b : a \in I,\ b \in J\}$.
2. Le *produit* de I et J est l'idéal $IJ = \langle ab : a \in I, b \in J\rangle_+$.

Remarque 3.11.
- Si I et J sont des idéaux à gauche/droite, $I + J$ aussi.
- Si I est un idéal à gauche et X un ensemble quelconque, $\langle ab : a \in I, b \in X\rangle_+$ est un idéal à gauche.
- Si J est un idéal à droite et X un ensemble quelconque, $\langle ab : a \in X, b \in J\rangle_+$ est un idéal à droite.
-
- Si I est un idéal à gauche et J un idéal à droite, $\langle ab : a \in I, b \in J\rangle_+$ est un idéal (bilatère).

Remarque 3.12. Pour deux *ensembles* $X, Y \subseteq A$ on avait défini XY comme l'*ensemble* $\{xy : x \in X, y \in Y\}$. Pour deux *idéaux* $I, J \trianglelefteq A$ on prend l'*idéal* engendré.

Définition 3.13. Soit A un anneau. Deux idéaux I et J sont *étrangers* (ou *premiers entre eux*) si $I + JA$.

Proposition 3.14. *Soit A un anneau unitaire, et I, J deux idéaux étrangers. Alors $IJ + JI = I \cap J$.*

Démonstration. Puisque I et J sont des idéaux, on a $IJ \leq I$, $IJ \leq J$, $JI \leq I$ et $JI \leq J$. Ainsi $IJ + JI \leq I \cap J$.
Réciproquement, puisque $A = I + J$ il y a $i \in I$ et $j \in J$ avec $i + j = 1$. Soit $a \in I \cap J$. Alors $a = (i + j)a = ia + ja \in IJ + JI$, d'où $I \cap J \leq IJ + JI$ et on a égalité. □

Théorème 3.15 (Théorème des restes chinois)**.** *Soit A un anneau unitaire, et $I_1, \ldots, I_n$ des idéaux deux-à-deux étrangers. Alors le morphisme d'anneaux*

$$\varphi : A/(I_1 \cap \cdots \cap I_n) \to A/I_1 \times \cdots A/I_n, \qquad x + (I_1 \cap \cdots \cap I_n) \mapsto (x + I_1, \ldots, x + I_n)$$

est un isomorphisme.

$\forall k \neq l \quad I_k + I_l = A$

I_1, I_2 idéaux de A étrangers si $I_1 + I_2 = A$

(par exemple, $n_1\mathbb{Z}$ et $n_2\mathbb{Z}$ étrangers $\Leftrightarrow n_1 \wedge n_2 = 1$
$(n_1, n_2 \in \mathbb{Z})$

Remarque. si I_1, I_2 étrangers alors $I_1 \cap I_2 = I_1 . I_2$

en effet : soient $x_1 \in I_1, x_2 \in I_2$ tels que $x_1 + x_2 = 1$

alors $x \in I_1 \cap I_2$, $x = x(x_1 + x_2)$

$= \underbrace{x x_1}_{\in I_1 I_2} + \underbrace{x x_2}_{\in I_1 I_2} \in I_1 I_2$

$\Rightarrow I_1 \cap I_2 \subset I_1 I_2$

donc $I_1 \cap I_2 = I_1 I_2$

démo : $A \longrightarrow A/I_1 \times \cdots \times A/I_n$

$a \longmapsto (a + I_1, \ldots, a + I_n)$

morphisme d'anneaux de noyau $I_1 \cap \ldots \cap I_n$

surjectif !

En effet Soient $a_1, \ldots, a_n \in A$

$\forall j$, soit $\widetilde{I_j} = \bigcap_{\substack{k=1 \\ k \neq j}}^{n} I_k = \prod_{\substack{k=1 \\ k \neq j}}^{n} I_k$

$\forall j$, $\widetilde{I_j} + I_j = A$

(en effet : $\forall k \neq j$, $\exists x_k \in I_k, y_k \in I_j$, $x_k + y_k = 1$

alors $1 = \prod_{k \neq j} (x_k + y_k) = \underbrace{\prod_{k \neq j} x_k}_{\in \widetilde{I}_j} + \underbrace{\cdots}_{\in I_j}$

Soient $\alpha_j \in \widetilde{I}_j$, $\beta_j \in I_j$ tq

$\alpha_j + \beta_j = 1 \Rightarrow \alpha_j \equiv 1 + I_j$.

Alors $a = \sum_{j=1}^{n} a_j \alpha_j \in A$

$\Rightarrow a \equiv a_1 \alpha_1 + I_1 \quad (j \geq 2 \Rightarrow \alpha_j \in \widetilde{I}_j \subset I_1)$

$\equiv a_1 + I_1$

de même $\forall j$, $a \equiv a_j + I_j$.

(6, 15, 10 premiers entiers dans leur ensemble mais pas deux à deux).

Exemple. Résoudre (*) $\begin{cases} x \equiv 3\,[5] \\ x \equiv 2\,[6] \\ x \equiv 9\,[23] \end{cases}$

D'après le théorème, il existe une unique solution modulo $690 = 5 \times 6 \times 23$

Méthode.

$b_1 = 6 \times 23 = 138$ $\quad b_1^{-1} \equiv 2\,[5]$

$b_2 = 5 \times 23 = 115$ $\quad b_2^{-1} \equiv 1\,[6]$

$b_3 = 5 \times 6 = 30$ $\quad b_3^{-1} \equiv 10\,[23]$

On pose $x_0 = 3 \times 138 \times 2 + 2 \times 115 \times 1 + 9 \times 30 \times 10$

$\equiv 308\,[690]$

et (*) $\Leftrightarrow x \equiv 308\,[690]$

Ici : $I_1 = 5\mathbb{Z}$, $I_2 = 6\mathbb{Z}$, $I_3 = 23\mathbb{Z}$

$I_1 + I_2 = \mathbb{Z}$, $I_2 + I_3 = \mathbb{Z}$, $I_1 + I_3 = \mathbb{Z}$

$\mathbb{Z}/I_1 \cap I_2 \cap I_3 \simeq \mathbb{Z}/I_1 \times \mathbb{Z}/I_2 \times \mathbb{Z}/I_3$

$\mathbb{Z}/690\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$

$\overline{308} \longmapsto (\bar{3}, \bar{2}, \bar{9})$

Application.

Indicatrice d'Euler

$$\forall n \geq 1,\ \varphi(n) = |\{1 \leq k \leq n : k \wedge n = 1\}|$$

$$= |(\mathbb{Z}/n\mathbb{Z})^*|$$

Corollaire : $\forall m \wedge n = 1$ (premiers entre eux), $\varphi(mn) = \varphi(m)\varphi(n)$

démo : $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

iso. d'anneaux

$$\Rightarrow (\mathbb{Z}/mn\mathbb{Z})^* \simeq \underbrace{(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*}_{(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*}$$

iso de groupes

$$\Rightarrow |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^*| \times |(\mathbb{Z}/n\mathbb{Z})^*|$$

$$\varphi(mn) = \varphi(m)\,\varphi(n)$$

Exercice : a) $\forall p$ premier, $\forall \alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = \underbrace{p^\alpha}_{\text{}} - \underbrace{p^{\alpha-1}}_{\text{}}$

$(1 \leq k \leq p^\alpha,\ k \wedge p^\alpha \Leftrightarrow p \nmid k \Leftrightarrow k \notin \{p, 2p, \dots, p^{\alpha-1} \cdot p\})$

b) $\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3)\,\varphi(3) = 4 \cdot 2 = 8$

1, 5, 7, 11, 13, 17, 19, 23 (premiers à 24)

Ex. 1) Soit K corps $\quad P, Q \neq 0$

si $P \wedge Q = 1$ dans $K[X]$, alors

$$K[X]/(PQ) \simeq K[X]/(P) \times K[X]/(Q)$$

ex: $\mathbb{C}[X]/(X^2+1) \simeq \mathbb{C}[X]/(X+i) \times \mathbb{C}[X]/(X-i)$

$$\simeq \mathbb{C} \times \mathbb{C}$$

2) $\mathbb{Z}[i]/(5) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$\not\simeq \mathbb{Z}[i]/(2+i) \times \mathbb{Z}[i]/(2-i)$

Définition.

Démonstration. Par récurrence sur n, le cas $n = 1$ étant trivial. On suppose donc que $I_1, \dots, I_n, J$ sont deux-à-deux étrangers, et que $x + I \mapsto (x+, \dots, x + I_n)$ est un isomorphisme, où $I = I_1 \cap \cdots \cap I_n$. Puisque J est étranger à chaque I_k, il y a $i_k \in I_k$ et $j_k \in J$ avec $i_k + j_k = 1$. Alors $1 = \prod_{k=1}^{n}(i_k + j_k) \in i_1 i_2 \cdots i_n + J \subseteq I + J$. Donc I et J sont étrangers. On considère donc

$$A/(I_1 \cap \cdots \cap I_n \cap J) = A/(I \cap J) \to A/I \times A/J \to A/I_1 \times \cdots \times A/I_n \times A/J\,;$$

d'après l'hypothèse de récurrence il suffit de montrer que $\varphi : A/(I \cap J) \to A/I \times A/J$ est un isomorphisme. On est donc réduit au cas $n = 2$.
Il est clair que le morphisme est injectif. On considère $(x + I, y + J) \in A/I \times A/J$. Soient $i \in I$ et $j \in J$ tels que $i + j = 1$. On pose $z = iy + jx$. Alors

$$\begin{aligned} z + I &= iy + jx + I = ix + jx + I = (i + j)x + I = x + I, \quad \text{et} \\ z + J &= iy + jx + J = iy + jy + J = (i + j)y + J = y + J. \end{aligned}$$

Ceci montre la surjectivité. □

On note que si $z_0 \in A$ est une solution particulière du système de congruences $z \equiv a_k \mod I_k$ pour $k = 1, \dots, n$, alors l'ensemble des solutions est précisément $z_0 + (I_1 \cap \cdots \cap I_n)$.

Exemple 3.16. Soient $n_1, \dots, n_k \in \mathbb{Z}$ deux-à-deux premiers entre eux. Alors pour tout $a_1, \dots, a_k \in \mathbb{Z}$ il y a $x \in \mathbb{Z}$ tel que $x \equiv a_i \mod n_i$ pour $i = 1, \dots, k$.

Démonstration. Si n_i et n_j sont premiers entre eux, d'après la relation de Bézout il y a $u, v \in \mathbb{Z}$ avec $n_i u + n_j v = 1$. Donc $(n_i) + (n_j) = \mathbb{Z}$, et (n_i) et (n_j) sont étrangers. On conclut avec le théorème des restes chinois. □

Dans un anneau euclidien comme $\mathbb{Z}$ on calcule i et j à l'aide de l'algorithme d'Euclide.

4 Inversibilité, anneaux intègres

Définition 4.1. Soit A un anneau. Un élément $a \in A^*$ est un *diviseur de zéro à gauche* s'il y a $b \in A^*$ avec $ab = 0$. Dans ce cas, b est un *diviseur de zéro à droite*.
Un anneau commutatif sans diviseur de zéro est un anneau *intègre*. Attention : Parfois on demande en plus que l'anneau soit unitaire !
Si A est unitaire, un élément $a \in A$ est *inversible* s'il y a $b \in A$ avec $ab = ba = 1$.
L'ensemble des éléments inversibles est noté $A^\times$. C'est un groupe multiplicatif.
Un anneau commutatif dont tous les éléments non-nuls sont inversibles est un *corps*. Dans ce cas $A^\times = A^*$.

Remarque 4.2. Ne pas confondre $A^\times$ et $A^* = A \setminus \{0\}$.

Lemme 4.3. *1. Un élément inversible n'est pas diviseur de zéro.*

2. *Si a n'est pas diviseur de zéro à gauche et $ab = ac$, alors $b = c$ (et similairement à droite). En particulier un anneau intègre a simplification multiplicative.*

Démonstration. 1. Si $ab = 0$ et a est inversible, alors $b = a^{-1}ab = a^{-1}0 = 0$. Le raisonnement de l'autre coté est analogue.

2. Si $ab = ac$ alors $a(b - c) = 0$. Comme a n'est pas diviseur de zéro à gauche, $b - c = 0$ et $b = c$. □

Exemple 4.4. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z}$ est un idéal dans $\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire. Si $n = 0$ on a $n\mathbb{Z} = \{0\}$ et $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$. Si $n = 1$ on a $n\mathbb{Z} = \mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \cong \{0\}$, l'anneau trivial. On supposera donc $n \geq 2$.

Lemme 4.5. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier, pour $n \geq 2$.*

Démonstration. Supposons d'abord $n = k\ell$ composé, avec $1 < k, \ell < n$. Alors $k + n\mathbb{Z} \neq 0 + n\mathbb{Z}$, et $\ell + n\mathbb{Z} \neq 0 + n\mathbb{Z}$, mais

$$(k + n\mathbb{Z})(\ell + n\mathbb{Z}) = kl + n\mathbb{Z} = n + n\mathbb{Z} = 0 + n\mathbb{Z}.$$

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.
Réciproquement, supposons n premier. Alors pour tout $k \in \mathbb{Z}$ soit n divise k et $k + n\mathbb{Z} = 0 + n\mathbb{Z}$, soit k et n sont premiers entre eux. Dans ce cas, d'après le théorème de Bézout il y a des entiers relatifs $s, t \in \mathbb{Z}$ tels que $sk + tn = \text{pgcd}(k, n) = 1$. Alors

$$(s + n\mathbb{Z})(k + n\mathbb{Z}) = (sk + n\mathbb{Z}) = 1 - kn + n\mathbb{Z} = 1 + n\mathbb{Z}.$$

Ainsi tout $k + \mathbb{Z}$ non-nul est inversible, et $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

C'est un cas particulier d'un théorème plus général.

Proposition 4.6. *Un anneau intègre fini est un corps.*

Démonstration. Soit $a \in A^*$. Alors l'application $\lambda_a : x \mapsto ax$ est injective : Si $ax = ax'$, alors d'après lemme 4.3.2 on a $x = x'$. Or, A est fini, et toute application $A \to A$ injective est surjective. Par surjectivité de λ_a il y a un élément $e \in A$ avec $ae = a$. Si $b \in A$ est quelconque, alors $ab = aeb$, d'où $b = eb$ encore par lemme 4.3.2. Ainsi e est une unité multiplicative.
Encore par surjectivité de λ_a il y a $a' \in A$ avec $aa' = e$. Donc a possède un inverse multiplicatif $a^{-1} = a'$, et A est un corps. □

En fait, le Théorème de Wedderburn asserte qu'on a pas besoin de supposer la commutativité : Tout anneau fini sans diviseur de zéro est un corps.

On va maintenant généraliser la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$ à un anneau intègre quelconque.

On pose $\forall a, a' \in A, \forall b, b' \in A\setminus\{0\}$,

$(a,b) \sim (a',b')$ si $ab' = a'b$

$\sim$ relation d'équivalence sur $A \times A\setminus\{0\}$

On pose $K = A \times A\setminus\{0\} / \sim$

on note $\forall a \in A, \forall b \in A\setminus\{0\}$, $\frac{a}{b}$ = classe de (a,b)

En particulier, $\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b$.

K est un corps pour : $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$

$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$

De plus $\begin{array}{ccc} A & \longrightarrow & K \\ a & \longmapsto & \frac{a}{1} \end{array}$ injective

Exemples. si $A = \mathbb{Z}$, $K = \mathbb{Q}$

si $A = \mathbb{D}$ (décimaux), $K = \mathbb{Q}$

si $A = \mathbb{R}[X]$, $K = \mathbb{R}(X)$

si $A = \mathbb{R}[X,Y]$, $K = \mathbb{R}(X,Y)$

si $A = \mathbb{Z}[i]$, $K = \mathbb{Q}[i] = \{a+ib : a,b \in \mathbb{Q}\}$

Théorème 4.7 (Corps des fractions)**.** *Soit A un anneau intègre. Alors il y a un unique (à isomorphisme près) plus petit corps K contenant A. Tout élément de K s'écrit de la forme ab^{-1} avec $a, b \in A$ (inverse et produit calculé dans K). C'est le* corps des fractions *de A. Si $f : A \to L$ est un morphisme d'anneaux avec L un corps, il se prolonge en morphisme $\bar{f} : K \to L$.*

Démonstration. On imagine que A se plonge dans un corps K. Alors K contient tous les éléments de la forme ab^{-1} avec $a \in A$ et $b \in A^*$. On note que la collection de tels quotients est clos par addition, soustraction, multiplication et réciproque, c'est donc un sous-corps. Par minimalité $K = \{ab^{-1} : a \in A,\ b \in A^*\}$. On va coder l'élément ab^{-1} par la paire (a, b). Or, ce codage n'est pas unique ; on appellera paires qui donnent le même quotient $\sim$-équivalents : $(a, b) \sim (a'b') \Leftrightarrow ab^{-1} = a'b'^{-1} \Leftrightarrow ab' = a'b$.
Pour ce faire, on n'a pas besoin de l'existence *à priori* de K — on le construira. Sur $A \times A^*$ on définit une relation d'équivalence par $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$. On note que $(a, b) \sim (ac, bc)$ pour $c \neq 0$, et que $\sim$ est réflexif et symétrique. On vérifie la transitivité : si $(a, b) \sim (a', b') \sim (a'', b'')$, alors $ab' = a'b$ et $a'b'' = a''b'$, d'où $ab'b'' = a'bb'' = a''bb'$ et $ab'' = a''b$ par simplification, ce qui donne $(a, b) \sim (a'', b'')$. Ainsi $\sim$ est une relation d'équivalence, dont on note la classe de (a, b) par $[a, b]$.
On *pose* $K = (A \times A^*)/\sim$, et définit une addition $\oplus$ et une multiplication $\otimes$ sur K par les formules qu'on connaît des quotients ab^{-1} :

$$[a, b] \oplus [a', b'] = [ab' + a'b, bb'] \qquad \text{et} \qquad [a, b] \otimes [a', b'] = [aa', bb'].$$

Il faut vérifier que la somme et le produit ne dépendent pas du choix des représentants. Par symétrie il suffit de vérifier sur la gauche. Soit donc $[a, b] = [a'', b'']$, et donc $ab'' = a''b$. Alors $[a'', b''] \oplus [a', b'] = [a''b' + a'b'', b''b']$ et $[a'', b''] \otimes [a', b'] = [a''a', b''b']$. Or,

$$[ab' + a'b, bb'] = [ab'b'' + a'bb'', bb'b''] = [a''b'b + a'bb'', bb'b''] = [a''b' + a'b'', b''b'] \text{ et}$$
$$[aa', bb'] = [aa'b'', bb'b''] = [a''a'b, bb'b''] = [a''a', b''b'].$$

Donc $\oplus$ et $\otimes$ sont bien définis.
On fixe $c \in A^*$ et pose $0 = [0, c]$ et $1 = [c, c]$. Ces classes ne dépendent pas du choix de c. Pour $[a, b] \in K$ on pose $-[a, b] = [-a, b]$, et si $a \neq 0$ on pose $[a, b]^{-1} = [b, a]$. On vérifie facilement que ceci ne dépend pas du choix des représentants. Alors

$$[a, b] \oplus [0, c] = [ac + 0b, bc] = [a, b] \qquad \text{et} \qquad [a, b] \otimes [c, c] = [ac, bc] = [a, b],$$

et donc

$$[a, b] \oplus (-[a, b]) = [a, b] \oplus [-a, b] = [ab - ab, bb] = [0, bb] = 0, \text{ et}$$
$$[a, b] \otimes [a, b]^{-1} = [a, b] \otimes [b, a] = [ab, ab] = 1.$$

Il est évident de la définition que $\oplus$ et $\otimes$ sont commutatifs. On vérifie l'associativité :

$$\begin{aligned}([a, b] \oplus [a', b']) \oplus [a'', b''] &= [ab' + a'b, bb'] \oplus [a'', b''] = [ab'b'' + a'bb'' + a''bb', bb'b''] \\ &= [a, b] \oplus [a'b'' + a''b', b'b''] = [a, b] \oplus ([a', b'] \oplus [a'', b'']), \text{ et} \\ ([a, b] \otimes [a', b']) \otimes [a'', b''] &= [aa', bb'] \otimes [[a'', b''] = [aa'a'', bb'b''] = [a, b] \otimes [a'a'', b'b''] \\ &= [a, b] \otimes ([a', b'] \otimes [a'', b''])\end{aligned}$$

et la distributivité :

$$\begin{aligned}([a,b]+[a',b'])\otimes[a'',b''] &= [ab'+a'b,bb']\otimes[a'',b''] = [aa''b'+a'a''b,bb'b''] \\ &= [aa''b'b''+a'a''bb'',bb'b''b''] = [aa'',bb'']\oplus[a'a'',b'b''] \\ &= [a,b]\otimes[a'',b'']\oplus[a',b']\otimes[a'',b''].\end{aligned}$$

Ainsi $(K,0,1,\oplus,\otimes)$ est bien un corps.
On considère $f : A \to K$ défini par $a \mapsto [ac,c]$ (on note que $f(a)$ ne dépend pas de c). Si $f(a) = f(a')$ alors $[ac,c] = [a'c,c]$, soit $ac^2 = a'c^2$ et $a = a'$; ainsi f est injectif. On a $f(0) = [0c,c] = 0$, $f(1) = [1c,c] = 1$ (si A est unitaire), et f préserve l'addition et la multiplication :

$$\begin{aligned}f(a+b) = [(a+b)c,c] = [acc+bcc,cc] = [ac,c]+[bc,c] = f(a)\oplus f(b),\ \text{et} \\ f(ab) = [abc,c] = [acbc,cc] = [ac,c]\otimes[bc,c] = f(a)\otimes f(b).\end{aligned}$$

Ainsi f plonge A dans K, et tout élément $[a,b] \in K$ est de la forme

$$f(a)\otimes f(b)^{-1} = [ac,c]\otimes[bc,c]^{-1} = [ac,c][c,bc] = [ac^2,bc^2] = [a,b].$$

On identifie donc A avec son image dans K.
Si L est un autre corps et $g : A \to L$ est un plongement, on prolonge g sur K par $g : [a,b] \mapsto g(a)g(b)^{-1}$; on vérifie que $\bar{g}$ ne dépend pas des choix des représentants, que $\bar{g}(0) = 0$ et que $\bar{g}$ prolonge g et préserve l'addition et la multiplication. Ainsi $\bar{g}$ est un homomorphisme de K dans L. Or, $\ker\bar{g}$ est un idéal de K qui ne peut pas être K entier puisque $\ker\bar{g}\cap A = \{0\}$. Mais un idéal d'un corps est soit (0) soit le corps entier. Ainsi $\ker\bar{g} = (0)$ et $\bar{g}$ est injectif, ce qui montre que K est minimal et unique. □

5 Divisibilité, anneaux principaux

Définition 5.1. Soit A un anneau intègre unitaire.

- Soient $a,b \in A$. On dit que a *divise* b, noté $a \mid b$, s'il y a $c \in A$ avec $ac = b$.
- Un élément a est *irréductible* si pour tous $b,c \in A$, si $a = bc$ alors b ou c est inversible.
- Un élément $a \in A$ est premier si pour tous $b,c \in A$, si $p \mid bc$ alors $p \mid b$ ou $p \mid c$.

Ceci généralise les notions bien connues de $\mathbb{Z}$ et $\mathbb{R}[X]$.

Exemple 5.2. Soit $A = \mathbb{Z}[i\sqrt{5}] = \{a+ib\sqrt{5} : a,b \in \mathbb{Z}\}$, un sous-anneau de $\mathbb{C}$. On a

$$6 = 2\times 3 = (1+i\sqrt{5})\,(1-i\sqrt{5}).$$

Pour tout $a \in A$ on a $|a|^2 \in \mathbb{N}$. On en déduit que $|a| = 1$ pour tout $a \in A$ inversible. Si $z = a+i\sqrt{5}b \in Z[i\sqrt{5}]$ avec $|z|^2 < 5$, on a $b = 0$ et $z \in \mathbb{Z}$. En particulier les seuls éléments z avec $|z|^2 = 1$ sont ± 1, et il n'y a pas d'élément z avec $|z|^2 \in \{2,3\}$.
Si $zz' = 1 \pm i\sqrt{5}$, alors $|z|^2|z'|^2 = 6$; si $zz' = 2$, alors $|z|^2|z'|^2 = 4$, et si $zz' = 3$, alors $|z|^2|z'|^2 = 9$. Dans tous les cas $|z|^2 \leq 3$ ou $|z'|^2 \leq 3$, donc vaut 1, et $1 \pm i\sqrt{5}$, 2 et 3 sont tous irréductibles. Il n'y a donc pas factorisation unique en irréductibles dans A.

Proposition 5.3. *Soit A un anneau intègre unitaire. Alors tout élément premier est irréductible.*

Démonstration. Soit $a \in A$ premier, et $b, c \in A$ avec $a = bc$. Puisque A est unitaire, $a \mid bc$; comme a est premier, on a $a \mid b$ ou $a \mid c$. Par symétrie on peut supposer $a \mid b$, et il y a $d \in A$ avec $ad = b$. Donc $bcd = ad = b$ et $cd = 1$ d'après le lemme 4.3. Ainsi c est inversible. Ceci montre que a est irréductible. □

Remarque 5.4. La réciproque est fausse : Dans l'exemple 5.2 on a que 2 est irréductible et divise $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, mais ne divise aucun des deux facteurs.

Définition 5.5. Soit A un anneau intègre unitaire. Deux éléments $a, b \in A$ sont *associés* s'il y a $c \in A$ inversible avec $a = cb$.

C'est une relation d'équivalence.

Lemme 5.6. *Soit A un anneau intègre unitaire, et $a, b \in A$. Deux éléments $a, b \in A$ sont associés si et seulement si $(a) = (b)$.*

Démonstration. S'il y a $c \in A$ inversible avec $ac = b$, alors $bc^{-1} = a$. Donc $b \in (a)$ et $a \in (b)$, d'où $(a) = (b)$.
Réciproquement, supposons $(a) = (b)$. Puisque $b \in (a) = aA$, il y a $c \in A$ avec $ac = b$. De même, il y a $d \in A$ avec $bd = a$. Donc $a = bd = acd$. Alors soit $a = 0$, soit $a \neq 0$ et $cd = 1$. Dans le premier cas $(b) = (0)$ implique $b = 0 = a \cdot 1$; dans le deuxième cas c est inversible avec $ac = b$. □

Proposition 5.7. *Soit A un anneau intègre unitaire, et $a \in A^*$.*

1. *L'élément a est premier si et seulement si l'idéal (a) est premier.*
2. *L'élément a est irréductible si et seulement s'il n'existe pas de $b \in A$ avec $(a) < (b) < A$.*

Démonstration.

1. Soit (a) premier, et $b, c \in A$ avec $a \mid bc$. Donc $bc \in (a)$; puisque (a) est premier, soit $b \in (a)$ et $a \mid b$, soit $c \in (a)$ et $a \mid c$. Ainsi a est premier.
   Réciproquement, soit a premier, et soient $b, c \in A$ avec $bc \in (a)$. Puisque (a) est premier, soit $b \in (a)$ et $a \mid b$, soit $c \in (a)$ et $a \mid c$. Ainsi a est premier.
2. Soit a irréductible, et $b \in A$ avec $(a) \leq (b) \trianglelefteq A$. Donc $a \in (b)$ et il y a $c \in A$ avec $a = bc$. Si b est inversible, alors $(b) = A$; si c est inversible, alors $(a) = (b)$.
   Réciproquement, supposons qu'il n'existe aucun $b \in A$ avec $(a) < (b) < A$. Soient $c, d \in A$ avec $a = cd$. Alors $(a) \leq (c) \leq A$. Si $(c) = A$ alors c est inversible ; si $(c) = (a)$ alors a et c sont associés et d est inversible. Ainsi a est irréductible. □

Définition 5.8. Un idéal I dans un anneau A est *principal* s'il est engendré par un seul élément : il y a $a \in A$ avec $I = (a)$.
Un anneau intègre unitaire A est *principal* si tout idéal dans A est principal.

Exemple 5.9. On va voir plus bas des exemples d'anneaux principaux. On note que $\mathbb{Z}[X]$ n'est pas principal.

Proposition 5.10. *Soit A un anneau principal, et $a \in A^*$. Sont équivalents :*

1. *a est premier.*
2. *a est irréductible.*
3. *aA est premier.*
4. *aA est maximal.*

Démonstration. On sait déjà que 4.⇒3.⇒1.⇒2. Enfin, 2.⇒4. découle de la proposition 5.7.2, sachant que tout idéal est principal. □

Définition 5.11. Un anneau intègre unitaire est *euclidien* s'il y a une fonction $N : A \setminus \{0\} \to \mathbb{N}$ telle que

1. On a $N(ab) \geq N(a)$ pour tout $a, b \in A \setminus \{0\}$.
2. Pour tout $a, b \in A$ avec $b \neq 0$ il y a $q, r \in A$ avec $a = bq + r$ et soit $r = 0$, soit $N(r) < N(b)$.

La fonction N est la *norme euclidienne*.

Exemple 5.12.
- $\mathbb{Z}$ avec la norme $N(z) = |z|$.
- $K[X]$ avec la norme $N(P) = \deg(P)$.
- Les entiers de Gauss $\mathbb{Z}[i]$ avec la norme $N(x + iy) = x^2 + y^2$.
  Pour vérifier la condition 2., on considère $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. Les points de $\mathbb{Z}[i]$ forment un réseau rectangulaire de distance horizontale et verticale 1. Pour tout point $z \in \mathbb{C}$ on trouve donc un point de $\mathbb{Z}[i]$ de distance au plus $\sqrt{2}/2$ de z (avec égalité si z est le milieu d'un carré unitaire dont les coins sont dans $\mathbb{Z}[i]$). En particulier il y a $q \in \mathbb{Z}[i]$ avec $|\frac{a}{b} - q| \leq \frac{\sqrt{2}}{2}$. On pose $r = a - bq$. Alors soit $r = 0$, soit
  $$N(r) = |r|^2 = |a - bq| \leq \frac{1}{2} |b|^2 < |b|^2 = N(b).$$

Lemme 5.13. *Soit A un anneau euclidien. Alors $N(1) = \min \mathrm{im}(N)$ est la valeur minimale de la norme. Un élément $a \in A$ est inversible si et seulement si $N(a) = N(1)$.*

Démonstration. Pour $b \in A^*$ on a $N(b) = N(1 \cdot b) \geq N(1)$.
Si a est inversible, disons $c \in A$ satisfait $ac = 1$, alors $N(1) = N(ac) \geq N(a) \geq N(1)$ et on a égalité. Réciproquement, si $N(a) = N(1)$, alors $a \neq 0$ et il y a $q, r \in A$ avec $1 = aq + r$ et soit $N(r) < N(1)$ ou $r = 0$. Le premier cas est impossible. Donc $r = 0$ et $aq = 1$, ce qui veut dire que a est inversible. □

Théorème 5.14. *Un anneau euclidien est principal.*

Démonstration. Soit $(0) \neq I \trianglelefteq A$. On choisit $0 \neq a \in I$ avec $N(a)$ minimal possible. Alors pour tout $b \in I$ il y a $q, r \in A$ avec $b = aq + r$, et soit $r = 0$, soit $N(r) < N(a)$. Or, $r = b - aq \in I$, d'où $N(r) \geq N(a)$ par minimalité. Donc $r = 0$ et $b = aq \in (a)$. Ainsi $I = (a)$ est principal. □

Exemple 5.15. L'anneau $\mathbb{Z}[\frac{1+\sqrt{19}}{2}]$ est principal, mais pas euclidien.

Si on peut deviner la norme, il est généralement facile de montrer qu'un anneau est euclidien. Sinon, il est souvent plus facile de montrer qu'un anneau est principal.

Définition 5.16. Soit A un anneau principal, et $a_1, \dots, a_n \in A$ non-nuls.

— Un élément $\delta \in A$ tel que $(\delta) = (a_1, \dots, a_n)$ est un pgcd de $A_1, \dots, a_n$. On le note $\delta = \text{pgcd}(a_1, \dots, a_n) = a_1 \wedge \cdots \wedge a_n$. D'après le lemme 5.6 un pgcd est déterminé à un facteur inversible près.

— Un élément $\Delta \in A$ tel que $(\Delta) = (a_1) \cap \cdots \cap (a_n)$ est un ppcm de $_1, \dots, a_n$. Il est noté $\delta = \text{ppcm}(a_1, \dots, a_n) = a_1 \vee \cdots \vee a_n$, et déterminé à facteur inversible près.

Remarque 5.17. Dans $\mathbb{Z}$ et $K[X]$ on peut éliminer l'ambiguïté dans le définition du pgcd et du ppcm en demandant qu'il soit positif (dans $\mathbb{Z}$) ou unitaire (dans $K[X]$). En général il n'y a pas de choix canonique.

Théorème 5.18 (Relation de Bézout)**.** *Soit $\delta = a_1 \wedge \cdots \wedge a_n$. Alors il y a $c_1, \dots, c_n \in A$ avec $\delta = c_1 a_1 + \cdots + c_n a_n$.*

Démonstration. On a $\delta \in (a_1, \dots, a_n) = a_1 A + \cdots + a_n A$. □

Remarque 5.19. Les éléments $c_1, \dots, c_n$ sont des *coefficients de Bézout.*

Définition 5.20. Les éléments $a_1, \dots, a_n$ sont *premiers entre eux* si $a_1 \wedge \cdots \wedge a_n = 1$.

Corollaire 5.21 (Théorème de Bézout)**.** Soit A principal. Les éléments $a_1, \dots, a_n$ sont premiers entre eux si et seulement s'il y a $c_1, \dots, c_n \in A$ avec $a_1 c_1 + \cdots + a_n c_n = 1$.

Démonstration. L'existence est la relation de Bézout. Réciproquement, $a_1 \wedge \cdots \wedge a_n$ doit diviser $a_1 c_1 + \cdots + a_n c_n$ et est donc associé à 1. □

Théorème 5.22 (Lemme de Gauss)**.** *Soient a, b, c non-nuls. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.*

Démonstration. Puisque $a \wedge b = 1$ il y a $u, v \in A$ avec $au + bv = 1$. Alors $c = acu + bcv$. Or, $a \mid acu$ et $a \mid bcv$, donc $a \mid acu + bcv = c$. □

Théorème 5.23. *Soit $\delta = a_1 \wedge \cdots \wedge a_n$ et $\Delta = a_1 \vee \cdots \vee a_n$.*

1. *Pour un élément $b \in A$ on a $b \mid \delta$ si et seulement si $b \mid a_i$ pour $i = 1, \dots, n$.*
2. *Pour un élément $b \in A$ on a $\Delta \mid b$ si et seulement si $a_i \mid b$ pour $i = 1, \dots, n$.*

Démonstration. 1. D'après Bézout il y a $c_1, \dots, c_n \in A$ avec $\delta = c_1 a_1 + \cdots + c_n a_n$. Donc si $b \mid a_i$ pour $i = 1, \dots, n$ alors $b \mid c_1 a_1 + \cdots + c_n a_n = \delta$.
Réciproquement, $a_i \in (\delta)$ pour $i = 1, \dots, n$, donc il y a $d_i \in A$ avec $a_i = \delta d_i$. Donc si $b \mid \delta$, alors $b \mid \delta d_i = a_i$.

2. On a $\Delta \in (a_i)$ pour $i = 1, \dots, n$, et il y a $c_i \in A$ avec $\Delta = a_i c_i$. Donc si $\Delta \mid b$, alors $a_i \mid b$ pour $i = 1, \dots, n$.
   Réciproquement, si $a_i \mid b$ alors $b \in (a_i)$ pour $i = 1, \dots, n$, et donc $b \in (a_1) \cap \cdots \cap (a_n) = (\Delta)$. Ainsi $\Delta \mid b$. □

Remarque 5.24. Puisque $a \mid b$ si et seulement $ca \mid cb$, on a $ca_1 \wedge \cdots \wedge ca_n = c\,(a_1 \wedge \cdots \wedge a_n)$ et $ca_1 \vee \cdots \vee ca_n = c\,(a_1 \vee \cdots \vee a_n)$.

Théorème 5.25. *Soit A un anneau principal, et $a, b \in A^*$. Alors $(a \wedge b)\,(a \vee b) = (ab)$. Autrement dit, si $\delta = a \wedge b$ et $\Delta = a \vee b$, alors il y a $u \in A$ inversible avec $\delta\Delta = uab$.*

Démonstration. Soient $a', b' \in A$ avec $a = a'\,(a \wedge b)$ et $b = b'\,(a \wedge b)$. Alors $a' \wedge b' = 1$, et il suffit de montrer que $(a' \vee b') = (a'b')$.
Soient $u, v \in A$ avec $a'u + b'v = 1$. Puisque $a' \mid a' \vee b'$ il y a $c \in A$ avec $a'c = a' \vee b'$. Alors $c = a'cu + b'cv$. Or, $b' \mid b'cv$ et $b' \mid (a' \vee b') = a'cu$, ce qui donne $b' \mid a'cu + b'cv = c$, et il y a $c' \in A$ avec $b'c' = c$. Ainsi $a' \vee b' = a'c = a'b'c'$ et $a' \vee b' \in (a'b')$. Donc $(a' \vee b') \leq (a'b')$.
Réciproquement, $a'b' \in (a') \cap (b')$, d'où $(a'b') \leq (a') \cap (b') = (a' \vee b')$ ce qui donne l'égalité. □

Dans un anneau euclidien, on calcule le pgcd à l'aide de l'*algorithme d'Euclide*. Soient $a_0, a_1 \in A^*$. Alors on trouve $q_1, a_2 \in A$ avec $a_0 = a_1 q_1 + a_2$ et $a_2 = 0$ ou $N(a_2) < N(b)$. Puisque $(a_0, a_1) = (a_1, a_2)$, on a $a_0 \wedge a_1 = a_1 \wedge a_2$. Si $a_2 = 0$ an a $a_1 \mid a_0$ et $(a, b) = (a_0, a_1) = (a_1)$, d'où $a \wedge b = a_1$. Si $a_2 \neq 0$ on itère avec a_1, a_2. Puisque la suite d'entiers $(N(a_i))_{i>0}$ décroît strictement, l'algorithme s'arrête. Pour calculer des coefficents de Bézout, on calcule $u_n, v_n \in A$ tel que $a_n = u_n a + v_n b$. On pose $u_0 = v_1 = 1$ et $u_1 = v_0 = 0$. Si $a_{n-1} = u_{n-1}a + v_{n-1}b$ et $a_n = u_n a + v_n b$, on obtient

$$\begin{aligned} a_{n+1} &= a_{n-1} - a_n q_n \\ &= u_{n-1}a + v_{n-1}b - (u_n a + v_n b)q_n \\ &= (u_{n-1} - q_n u_n)a + (v_{n-1} - q_n v_n)b. \end{aligned}$$

Ainsi $u_{n+1} = u_{n-1} - q_n u_n$ et $v_{n+1} = v_{n-1} - q_n v_n$. On itère.

Exemple 5.26. Calculer $597 \wedge 322$, ainsi que des coefficients de Bézout.

n	a_{n-1}	=	a_n	×	q_n	+	a_{n+1}	u_n	v_n
0			597				322	1	0
1	597	=	322	×	1	+	275	0	1
2	322	=	275	×	1	+	47	1	−1
3	275	=	47	×	5	+	40	−1	2
4	47	=	40	×	1	+	7	6	−11
5	40	=	7	×	5	+	5	−7	13
6	7	=	5	×	1	+	2	41	−76
7	5	=	2	×	2	+	1	−48	89
8	2	=	1	×	2	+	0	137	−254

Ainsi $597 \wedge 322 = 1 = 597 \times 137 - 322 \times 254$.

Définition 5.27. Un anneau est *noetherien* s'il n'y a pas de chaîne $I_0 < I_1 < I_2 < \cdots$ infinie strictement croissante d'idéaux à gauche ou à droite.

Proposition 5.28. *Un anneau est noethérien si et seulement si tout idéal (à gauche) ou (à droite) est finiment engendré (c'est-à-dire engendré par un nombre fini d'éléments).*

Démonstration. Supposons que A est noethérien, mais que $I \trianglelefteq A$ est un idéal à gauche qui n'est pas finiment engendré. Supposons qu'on a trouvé $a_1, \ldots, a_n \in I$ tel que $(a_1) < (a_1, a_2) < \cdots < (a_1, \ldots, a_n)$ (pour $n = 0$ l'hypothèse est vide). Puisque I n'est pas finiment engendré, on a $(a_1, \ldots, a_n) < I$ et il y a $a_{n+1} \in I \setminus (a_1, \ldots, a_n)$. Alors $(a_1, \ldots, a_n) < (a_1, \ldots, a_n, a_{n+1})$. Ainsi on trouve une chaîne infinie strictement croissante d'idéaux à gauches, une contradiction. Donc tout idéal à gauche de A est finiment engendré. Par symétrie, tout idéal à droite est aussi finiment engendré.
Réciproquement, supposons que tout idéal à gauche ou à droite est finiment engendré Soit $I_0 < I_1 < \cdots \trianglelefteq A$ est une chaîne infinie strictement croissante d'idéaux à gauche. Alors $I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal à gauche dans A, donc engendré par un nombre fini d'éléments $a_1, \ldots, a_k \in I$. Or, $I = \bigcup_{n\in\mathbb{N}} I_n$; il y a donc $n_0 \in \mathbb{N}$ tel que $a_1, \ldots, a_k \in I_{n_0}$. Alors $I = (a_1, \ldots, a_k) \leq I_{n_0} < I_{n_0+1} \leq I$, une contradiction. Par symétrie, il n'y a pas de chaîne infinie strictement croissante d'idéaux à droite non plus, et A est noethérien. □

Corollaire 5.29. Un anneau principal est noethérien. □

Contre-exemple. $A = \left\{a_0 + a_1 X + \cdots + \frac{a_d}{d!} X^d : d \in \mathbb{N},\ a_i \in \mathbb{Z}\right\} \subset \mathbb{Q}[X]$ Sous-anneau non noethérien.

6 Anneaux factoriels

$(X, \frac{X^2}{2!}, \ldots, \frac{X^n}{n!}, \ldots)$ n'est pas de type fini (exo)

Définition 6.1. Un anneau intègre unitaire est *factoriel* si tout élément $a \in A^*$ non-inversible se factorise comme produit d'éléments irréductibles, et que cette factorisation est unique à association et permutation près.

Cela veut dire que si $a \in A^*$ est non-inversible il y a n unique, des irréductibles $p_1, \ldots, p_n \in A$ tel que $a = p_1 p_2 \cdots p_n$, et si $q_1, \ldots, q_m \in A$ sont irréductibles avec $a = q_1 q_2 \cdots q_m$ alors $n = m$ et il y a une permutation σ de $[\![1, n]\!]$ tel que p_i et $q_{\sigma(i)}$ sont associés pour tout $i = 1, \ldots, n$.

Exemple 6.2. $\mathbb{Z}[X]$ est un anneau factoriel qui n'est pas principal.
(par ex. L'idéal $(2, X)$ n'est pas principal)
La démonstration se fera dans le prochain chapitre.

Lemme 6.3. *Dans un anneau intègre unitaire noethérien, tout élément non-nul non-inversible se factorise comme produit d'éléments irréductibles.*

Démonstration. Soit $a \in A^*$ non-inversible, et supposons que a_0 ne se factorise pas comme produit d'éléments irréductibles. En particulier a_0 n'est pas irréductible, et il y a $b, c \in A$ non-inversibles avec $a = bc$. Alors a est associé ni à b ni à c. Donc soit a soit b ne se factorise pas comme produit d'irréductibles, et il y a $a_1 \in \{b, c\}$ avec $(a_0) < (a_1)$

Contre-exemple.

L'anneau $\mathbb{Z}[i\sqrt{5}] = \{a+ib\sqrt{5} / a,b \in \mathbb{Z}\}$

n'est pas factoriel car

$$6 = \underbrace{2}_{\text{irréductibles}} \cdot \underbrace{3}_{\text{irréductibles}} = \underbrace{(1+i\sqrt{5})}_{\text{irréductibles}} \underbrace{(1-i\sqrt{5})}_{\text{irréductibles}}$$

Pause.

euclidien $\Rightarrow$ principal $\Rightarrow$ factoriel

$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ $\mathbb{Z}[X]$

(on ne peut pas avoir égalité, car sinon a_0 et a_1 seraient associés). On itère avec a_1 à la place de a_0, et on obtient une chaîne infinie strictement croissante d'idéaux, ce qui contredit la noethérianité. □

Proposition 6.4. *Dans un anneau factoriel, un élément est irréductible si et seulement s'il est premier.*

Démonstration. On sait déjà que premier implique irréductible dans un anneau intègre unitaire. Soit $p \in A$ irréductible, et $b, c \in A$ tel que $p \mid bc$. Il y a donc $a \in A$ avec $ap = bc$. Soient $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$ et $c = r_1 \cdots r_k$ les factorisations de a, b et c en facteurs irréductibles. Alors $pp_1 \cdots p_n = q_1 \cdots q_m r_1 \cdots r_k$ sont deux factorisations de $ap = bc$ en facteurs irréductibles. Par unicité il y a soit $i \in [\![1, m]\!]$ avec p associé à q_i, et $p \mid b$, soit $j \in [\![1, k]\!]$ avec p associé à r_j, et $p \mid c$. Ainsi p est premier. □

Proposition 6.5. *Un anneau intègre unitaire A est factoriel si et seulement si tout élément $a \in A^*$ non-inversible se factorise comme produit d'éléments premiers.*

Démonstration. Soit A factoriel. Alors tout élément non-nul non-inversible se factorise comme produit d'éléments irréductibles, qui sont premiers d'après la proposition 6.4. Réciproquement, supposons que tout élément $a \in A^*$ non-inversible se factorise comme produit d'éléments premiers. Puisque un élément premier est irréductible, a se factorise comme produit d'éléments irréductibles. Supposons donc que

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

pour des éléments premiers $p_1, \ldots, p_n$ et des éléments irréductibles $q_1, \ldots, q_m$. On fait une récurrence sur n.
Initialisation. Si $n = 1$, alors $a = p_1 = q_1 \cdots q_m$. Puisque p_1 est premier, il y a $i \in [\![1, m]\!]$ tel que p_1 divise q_i. Il y a donc $b \in A$ avec $p_1 b = q_i$. Donc $p_1 = b^{-1} q_i = q_1 \cdots q_m$. Par simplification on a $b^{-1} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m$, ce qui implique que q_j est inversible pour $j \neq i$. Or, un élément irréductible n'est pas inversible. On a donc $m = 1$ et $p_1 = q_1 = a$.
Hypothèse. On suppose qu'un produit de $n - 1$ éléments premiers a une unique factorisation en irréductibles.
Hérédité. On a $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ comme ci-dessus. Alors $p_n \mid q_1 q_2 \cdots q_m$; puisque p_n est premier il y a $i \in [\![1, n]\!]$ tel que $p_n \mid q_i$, et il y a $b \in A$ avec $p_n b = q_i$; puisque q_i est irréductible et p_1 non-inversible, b est inversible et p_n est associé à q_i ; quitte à permuter les q_i on peut supposer $i = m$. Alors $p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1} b^{-1}$ avec $q_1, \ldots, q_{m-2}, q_{m-1} b^{-1}$ irréductibles. Par hypothèse de récurrence $n - 1 = m - 1$ et il y a une permutation σ de $[\![1, n-1]\!]$ tel que p_i est associé à $q_{\sigma(i)}$ pour $i = 1, \ldots, n-1$ (être associé à q_{m-1} est la même chose qu'être associé à $q_{m-1} b^{-1}$). Donc la factorisation de a en éléments irréductibles est unique. □

Corollaire 6.6. Un anneau principal est factoriel.

Démonstration. Un anneau principal est euclidien, et chaque élément non-nul non-inversible s'écrit donc comme produit d'irréductibles. Or, dans un anneau principal un élément irréductible est premier. On termine avec la proposition 6.5. □

Soit A un anneau factoriel, et $\mathcal{P}$ un système de représentants pour les classes d'association des éléments premiers. Cela signifie que tout élément premier est associé à un unique élément de $\mathcal{P}$.

Lemme 6.7. *Tout $a \in A^*$ s'écrit de manière unique comme $a = u\prod_{p\in\mathcal{P}} p^{n_p}$, avec u inversible et $n_p \in \mathbb{N}$ pour tout $p \in \mathcal{P}$, et tous nuls sauf un nombre fini.*

Démonstration. On considère une factorisation $a = q_1 \cdots q_n$ de a en facteurs premiers. Alors pour tout $i \in [\![1, n]\!]$ il y a $p_i \in \mathcal{P}$ associé à q_i, et donc $u_i \in A^\times$ avec $q_i = p_i u_i$. Ainsi $a = u_1 \cdots u_n p_1 \cdots p_n$; on pose $u = u_1 \cdots u_n$ et regroupe les p_i identiques, ce qui nous donne la factorisation $a = u\prod_{p\in\mathcal{P}} p^{n_p}$ souhaité. L'unicité suit de la factorisation unique. □

Proposition 6.8. *Soit $a = u\prod_{p\in\mathcal{P}} p^{n_p}$ et $b = v\prod_{p\in\mathcal{P}} p^{m_p}$ avec $u, v \in A^\times$. Alors $a \mid b$ si et seulement si $n_p \leq m_p$ pour tout $p \in \mathcal{P}$.*

Démonstration. Si $n_p \leq m_p$ pour tout $p \in \mathcal{P}$, alors $c = \prod_{p\in\mathcal{P}} p^{m_p - n_p} \in A$, et $b = vu^{-1}ac$. Donc $a \mid b$.
Réciproquement, supposons que $a \mid b$. Alors il y a $c \in A$ tel que $ac = b$. Soit $c = w\prod_{p\in\mathcal{P}} p^{k_p}$ la factorisation de c, avec $w \in A^\times$. Donc

$$v\prod_{p\in\mathcal{P}} p^{m_p} = b = ac = u\prod_{p\in\mathcal{P}} p^{n_p}\, w\prod_{p\in\mathcal{P}} p^{k_p} = uw\prod_{p\in\mathcal{P}} p^{n_p+k_p} ;$$

l'unicité donne $v = uw$ et $m_p = n_p + k_p \geq n_p$ pour tout $p \in \mathcal{P}$. □

Définition 6.9. Soit $a = u\prod_{p\in\mathcal{P}} p^{n_p}$ et $b = v\prod_{p\in\mathcal{P}} p^{m_p}$ avec $u, v \in A^\times$. Soit $k_p = \min\{n_p, m_p\}$ et $\ell_p = \max\{n_p, m_p\}$. On pose

$$\operatorname{pgcd}(a, b) = a \wedge b = \prod_{p\in\mathcal{P}} p^{k_p} \quad \text{et} \quad \operatorname{ppcm}\{a, b\} = a \vee b = \prod_{p\in\mathcal{P}} p^{\ell_p}.$$

Lemme 6.10. *Soient $a, b, c \in A^\times$. Alors*

$$c \mid a \text{ et } c \mid b \Leftrightarrow c \mid a \wedge b,$$
$$a \mid c \text{ et } b \mid c \Leftrightarrow a \vee b \mid c.$$

De plus, $(a \wedge b)\,(a \vee b)$ est associé à ab.

Démonstration. Les équivalences sont conséquence de la proposition 6.8. Le dernier énoncé est un simple calcul, en utilisant $\min\{m, n\} + \max\{m, n\} = m + n$. □

Un anneau factoriel permet donc un plus grand commun diviseur et un plus petit commun multiple, avec les propriétés habituels. Cependant, il satisfait une identité de Bézout si et seulement s'il est principal.