Anneaux

David Harari

Agrégation, Orsay, 2019-2020

1. Généralités sur les anneaux

1.1. Définitions, premières propriétés

Définition 1.1 Un *anneau* $(A, +, .)$ est la donnée d'un ensemble A et de deux lois internes $+, .$ vérifiant :

1. $(A, +)$ est un groupe abélien.
2. La multiplication . est associative et possède un élément neutre (noté 1).
3. . est distributive par rapport à + : pour tous x, y, z dans A, on a $x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.

Si la multiplication est commutative, on dit que l'anneau A est *commutatif*. Noter qu'on a dans tout anneau $O.x = x.0 = 0$ pour tout x, où 0 est le neutre pour l'addition.

Exemples :

1. L'anneau nul $\{0\}$. Il est caractérisé par le fait que dans cet anneau, on a $0 = 1$.
2. $(\mathbf{Z}, +, .)$, $(\mathbf{Z}/n\mathbf{Z}, +, .)$ sont des anneaux commutatifs.
3. Un corps K est par définition un anneau *commutatif*, distinct de $\{0\}$, tel que tout élément non nul ait un inverse pour la multiplication.
4. Si A est un anneau *commutatif* [1], on dispose de l'*anneau des polynômes en n variables* $A[X_1, ..., X_n]$ qui est commutatif.

[1] On peut définir cet anneau de polynômes pour A non-commutatif, mais aucune des bonnes propriétés habituelles ne se conserve, donc on se limitera dans ce cours au cas commutatif.

5. Pour tout corps K, $(M_n(K), +, .)$ est un anneau, non commutatif si $n \geq 2$.

Définition 1.2 On appelle ensemble des éléments *inversibles* d'un anneau A l'ensemble des $x \in A$ tels qu'il existe $y \in A$ avec $xy = yx = 1$. C'est un groupe pour la multiplication, noté en général A^*.

Exemples :

1. $\mathbf{Z}^* = \{\pm 1\}$.
2. $(\mathbf{Z}/n\mathbf{Z})^*$ est l'ensemble des classes $\bar{m}$, avec m premier à n.
3. Dans un corps K, on a par définition $K^* = K \setminus \{0\}$.
4. Si K est un corps, $K[X_1, ..., X_n]^*$ est l'ensemble des polynômes constant non nul (qui est isomorphe au groupe multiplicatif K^*). Ceci reste vrai si on remplace K par un anneau *intègre* (voir plus loin) A, et K^* par son groupe des inversibles A^*.
5. Si K est un corps, on a $M_n(K)^* = \mathrm{GL}_n(K)$.

Définition 1.3 Un *homomorphisme* (ou morphisme) d'anneaux $f : A \to B$ est une application entre deux anneaux vérifiant :

1. $f(x + y) = f(x) + f(y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

On notera que l'application nulle n'est pas un morphisme d'anneaux car elle ne vérifie pas 3.

1.2. Idéaux, anneaux quotient

On supposera désormais tous les anneaux commutatifs, sauf mention expresse du contraire (la théorie des anneaux non commutatifs est intéressante, mais très différente, et elle n'a pas les mêmes applications).

Définition 1.4 Soit A un anneau. Un *sous-anneau* de A est un sous-groupe B de $(A, +)$, *contenant* 1, et stable pour la multiplication. Autrement dit,

cela signifie que B est un anneau pour les lois induites par A, avec le même neutre[2] pour la multiplication.

Cette notion n'est en pratique pas très intéressante, contrairement à la suivante :

Définition 1.5 Une partie I d'un anneau commutatif A est un *idéal* de A si elle vérifie :

1. I est un sous-groupe de A pour $+$.
2. Pour tout x de I et tout a de A, on a $ax \in I$.

En particulier un idéal de A contient 1 (ou encore un élément inversible de A) si et seulement s'il est égal à A. Noter aussi qu'un idéal de A n'est pas autre chose qu'un sous A-module de A.

Exemples :

1. $\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps.
2. Les idéaux de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.
3. Si $f : A \to B$ est un morphisme entre deux anneaux commutatifs, l'image réciproque d'un idéal de B par f est un idéal de A. En particulier le *noyau* $\ker f = f^{-1}(0)$ est un idéal de A. Ceci implique qu'un morphisme de corps (=morphisme entre les anneaux sous-jacents) est toujours injectif.

Attention, l'image directe d'un idéal par un morphisme d'anneaux n'est pas toujours un idéal si on ne suppose pas le morphisme surjectif. Par exemple l'image de $\mathbf{Z}$ par l'inclusion $\mathbf{Z} \to \mathbf{Q}$ est $\mathbf{Z}$, qui n'est pas un idéal de $\mathbf{Q}$.

Proposition 1.6 *Soient A un anneau commutatif et I un idéal de A. Alors le groupe quotient A/I muni de la multiplication $\bar{a}\bar{b} := \overline{ab}$ est un anneau, appelé anneau quotient de A par I. La surjection canonique $p : A \to A/I$ est un morphisme d'anneaux, et l'élément unité de A/I est $\bar{1}$.*

[2]Attention, l'ensemble des matrices $A = (a_{ij}) \in M_2(K)$ dont tous les coefficients autres que a_{11} sont nuls est un anneau pour les lois $+$ et $\times$, mais ce n'est pas un sous-anneau de $M_2(K)$, car le neutre pour $\times$ n'est pas le même.

Vérification facile, comme dans le cas des espaces vectoriels quotients ou des groupes quotients.

On a alors immédiatement le théorème de factorisation habituel :

Theorème 1.7 *Soit $f : A \to B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A/\ker f \to B$ tel que $f = \tilde{f} \circ p$, où $p : A \to A/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injectif d'image* $\operatorname{Im} f$*, i.e. on a un isomorphisme d'anneaux $A/\ker f \simeq \operatorname{Im} f$.*

On vérifiera aussi facilement que si I est un idéal d'un anneau commutatif A, alors les idéaux de A/I sont les $p(J)$, où J est un idéal de A et $p : A \to A/I$ est la surjection canonique. De plus, le quotient $(A/I)/p(J)$ est isomorphe à $A/(I + J)$, où $I + J$ est l'idéal constitué des $i + j$ avec $i \in I$ et $j \in J$; une façon de le voir est de noter que comme dans le cas des groupes, $p(J)$ est aussi le sous A-module $(I + J)/I$ de A/I (il est d'ailleurs isomorphe au A-module $J/(I \cap J)$.

Exemples :

1. $\mathbf{Z}/n\mathbf{Z}$ est le quotient de $\mathbf{Z}$ par l'idéal $n\mathbf{Z}$.
2. L'application $P \mapsto P(i)$ est un morphisme d'anneaux surjectif de $\mathbf{R}[X]$ dans $\mathbf{C}$ dont le noyau est l'idéal $(X^2 + 1)$ engendré par le polynôme $X^2 + 1$ (pour le voir effectuer la division euclidienne par $X^2 + 1$). On a donc un isomorphisme d'anneaux $\mathbf{R}[X]/(X^2+1) \simeq \mathbf{C}$ et $\mathbf{R}[X]/(X^2+1)$ est un corps (on peut prendre cela pour définition de $\mathbf{C}$!).

1.3. Anneaux intègres

Définition 1.8 Un anneau commutatif A est dit *intègre* s'il est non nul, et si pour tous a, b de A, la condition $ab = 0$ implique $a = 0$ ou $b = 0$.

Exemples :

1. $\mathbf{Z}$ est intègre.
2. Pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier.
3. Tout corps est un anneau intègre (mais pas réciproquement, par exemple $\mathbf{Z}$ n'est pas un corps).
4. Tout sous-anneau d'un anneau intègre (par exemple d'un corps) est intègre.

5. Si A est intègre, les anneaux $A[X]$, $A[X_1, ..., X_n]$ sont intègres (et réciproquement).

On rappelle le résultat classique suivant :

Proposition 1.9 *Soit A un anneau intègre; alors il existe un corps K et un homomorphisme injectif $i : A \to K$ tel que pour tout morphisme injectif d'anneaux de A vers un corps K', il existe un unique morphisme de corps $j : K \to K'$ tel que $f = j \circ i$. K est unique à isomorphisme près, et s'appelle le corps des fractions de A. On le note* $\operatorname{Frac} A$.

Cela signifie donc que K est le "plus petit corps" contenant A, tout élément de K s'écrit x/y avec $x \in A$ et $y \in A$ non nul; ainsi un anneau est intègre si et seulement s'il est sous-anneau d'un corps. Par exemple $\operatorname{Frac} \mathbf{Z} = \mathbf{Q}$, et $\operatorname{Frac}(K[X]) = K(X)$ (le corps des fractions rationnelles en une indéterminée). Noter que l'anneau nul n'a pas de corps des fractions (ce qui justifie qu'il ne soit pas intègre par convention). Pour construire $K = \operatorname{Frac} A$, on considère les couples (a, b) avec $a \in A$ et $b \in A \setminus \{0\}$, et on définit ensemblistement K comme le quotient de l'ensemble de ces couples par la relation d'équivalence : $(a, b) \sim (c, d)$ ssi $ad = bc$. On vérifie alors que K, muni des lois

$$(a, b)(c, d) := (ac, bd); \quad (a, b) + (c, d) = (ad + bc, bd),$$

est un corps (dans lequel (a, b) correspond à a/b) qui vérifie les propriétés voulues.

Définition 1.10 Un anneau commutatif A est dit *principal* s'il est intègre et si tous ses idéaux sont *principaux*, i.e. de la forme $(a) = aA$ avec $a \in A$.

Par exemple $\mathbf{Z}$ et $K[X]$ (quand K est un corps) sont principaux. Si $n \in \mathbf{N}^*$ n'est pas premier, alors $\mathbf{Z}/n\mathbf{Z}$ n'est pas un anneau principal (bien que tous ses idéaux soient principaux) car il n'est pas intègre.

Définition 1.11 Un idéal I de A est dit *premier* si A/I est intègre. De manière équivalente cela signifie : $A \neq I$, et la condition $ab \in I$ implique $a \in I$ ou $b \in I$.

Exemples :

1. Les idéaux premiers de $\mathbf{Z}$ sont $\{0\}$ et les $n\mathbf{Z}$ pour n premier.
2. Un anneau A est intègre si et seulement si $\{0\}$ est premier.
3. Les idéaux (X_1) et (X_1, X_2) sont tous deux premiers dans $K[X_1, X_2]$.

□

2. Divisibilité dans les anneaux intègres

Dans tout cette section, A désigne un anneau commutatif, supposé intègre sauf mention explicite du contraire.

2.1. Éléments irréductibles

Définition 2.1 Soient a, b dans A. On dit que a *divise* b et on écrit $a \mid b$ s'il existe $c \in A$ tel que $b = ac$. En termes d'idéaux, c'est équivalent à $(a) \supset (b)$.

En particulier 0 ne divise que lui-même, et un élément de A^* divise tous les éléments de A.

Proposition 2.2 *Soient a, b dans A. Alors ($a \mid b$ et $b \mid a$) si et seulement s'il existe $u \in A^*$ tel que $a = ub$. On dit alors que a et b sont associés.*

Démonstration : On peut supposer a et b non nuls (sinon le résultat est trivial). Si $a = ub$ avec $u \in A^*$, alors $b \mid a$ et $b = u^{-1}a$ donc $a \mid b$. En sens inverse si $a = bc$ et $b = ad$ avec c, d dans A, alors $a = adc$ donc $dc = 1$ par intégrité de A, soit $c \in A^*$.

□

La relation "être associé" est d'équivalence sur A ou $A \setminus \{0\}$; en termes d'idéaux, a est associé à b si et seulement si $(a) = (b)$.

Définition 2.3 On dit qu'un élément p de $A \setminus \{0\}$ est *irréductible* s'il vérifie les deux propriétés suivantes :

1. p n'est *pas* inversible dans A.
2. La condition $p = ab$ avec a, b dans A implique que a ou b soit inversible.

La deuxième condition signifie que les seuls diviseurs de p sont ses associés et les inversibles de A. On fera bien attention au fait que par convention, les éléments de A^* ne sont pas irréductibles.

Exemple 2.4 a) Les irréductibles de $\mathbf{Z}$ sont les $\pm p$ avec p nombre premier.

b) Les éléments irréductibles de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

c) Un corps n'a pas d'éléments irréductibles.

d) L'anneau $A = \mathbf{Z}[i\sqrt{5}] = \mathbf{Z}[T]/(T^2 + 5)$, qui est aussi le sous-anneau de $\mathbf{C}$ constitué des $a + bi\sqrt{5}$ avec $a, b \in \mathbf{Z}$, est intègre. Si $z = a + bi\sqrt{5} \in A$,

posons $N(z) = |z|^2 = a^2 + 5b^2$. On observe que $N(z) \in \mathbf{N}$ et que $N(zz') = N(z)N(z')$. En particulier, si $z \in A^*$, alors l'égalité $N(z)N(z') = 1$ implique $N(z) = 1$, ce qui implique que $z = 1$ ou $z = -1$ puisque $N(z) = a^2 + 5b^2$. Comme 1 et -1 sont évidemment inversibles, on a $A^* = \{\pm 1\}$. Un exemple d'irréductible de A est 3, car si $3 = zz'$ avec z, z' dans A, alors $9 = N(3) = N(z)N(z')$, ce qui implique que $N(z) = 1$ vu que $N(z)$ divise 9 et ne peut pas valoir 3 (parce que l'équation $a^2 + 5b^2 = 3$ n'a pas de solutions avec a, b entiers); or $N(z) = 1$ implique comme on l'a vu que $z \in \{\pm 1\}$. On vérifie de même que $2 - i\sqrt{5}$ et $2 + i\sqrt{5}$ sont irréductibles, et aucun des deux n'est associé à 3 puisque $A^* = \{\pm 1\}$.

2.2. Anneaux factoriels

Définition 2.5 On dit que deux éléments a et b de A sont *premiers entre eux* si leurs seuls diviseurs communs sont les éléments de A^*.

On a l'analogue du théorème de Bezout quand A est *principal* :

Proposition 2.6 *Soit A un anneau principal. Deux éléments a et b de A sont premiers entre eux si et seulement s'il existe u, v dans A tels que $ua + vb = 1$ (i.e. si $A = (a, b) = aA + bA$, idéal engendré par a et b).*

Plus généralement, dans tout anneau principal, on peut définir un p.g.c.d. (unique à multiplication par un inversible près) de deux éléments a et b comme un générateur de l'idéal (a, b).

Démonstration : Si $1 = ua + bv$, alors tout diviseur commun de a et b divise 1, donc est inversible (cette implication est vraie dans tout anneau commutatif). En sens inverse, si a et b sont premiers entre eux, alors l'idéal (a, b) s'écrit (d) avec $d \in A$ car A est principal. En particulier d divise a et b, donc est inversible donc $(d) = A$.

□

Notons que dans l'anneau $A = K[X, Y]$, les polynômes X et Y sont premiers entre eux mais ne satisfont pas $A = (X, Y)$ (par exemple parce que tout polynôme de (X, Y) s'annule en $(0, 0)$). Ainsi $K[X, Y]$ n'est pas principal.

Remarque : Rappelons au passage que tout anneau *euclidien* comme $\mathbf{Z}$, $K[X]$ (si K est un corps), ou encore $\mathbf{Z}[i]$, est principal. Un anneau intègre A est euclidien s'il existe une application $v : A \setminus \{0\} \to \mathbf{N}$ ("stathme euclidien")

vérifiant la propriété suivante : pour tous $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ (pas forcément uniques) avec $a = bq + r$ et : $v(r) < v(b)$ ou $r = 0$. Il existe des anneaux principaux non euclidiens (cf. par exemple le livre de D. Perrin pour l'exemple de $\mathbf{Z}[\frac{1+i\sqrt{19}}{2}]$).

On aimerait quand même avoir une théorie de la divisibilité raisonnable pour des anneaux plus généraux que les anneaux principaux. C'est ce qui motive l'introduction de la notion d'anneau factoriel.

Définition 2.7 Un anneau commutatif A est dit *factoriel* s'il vérifie les trois propriétés suivantes :

1. A est intègre.
2. Tout élément non nul a de A s'écrit comme produit
$$a = up_1...p_r \tag{1}$$
avec $u \in A^*$ et les p_i irréductibles [3].
3. Il y a unicité de cette décomposition au sens suivant : si $a = vq_1...q_s$ en est une autre, alors $r = s$ et il existe une permutation σ de $\{1, ..., r\}$ telle que pour tout i de $\{1, ..., r\}$, les éléments p_i et $q_{\sigma(i)}$ soient associés.

Remarques : a) Comme pour principal, on n'oubliera pas la condition d'intégrité de A.

b) Une autre formulation, souvent plus commode, de l'unicité, est la suivante : fixons un *système de représentants irréductibles* $\mathcal{P}$ de A, i.e. un ensemble d'éléments irréductibles tels que tout irréductible de A soit associé à un et un seul élément de $\mathcal{P}$. Alors tout élément non nul a de A s'écrit d'une manière unique $a = u \prod_{p \in \mathcal{P}} p^{n_p}$ avec $u \in A^*$, et $(n_p)_{p \in \mathcal{P}}$ famille presque nulle d'entiers naturels. On note alors $n_p = v_p(a)$. Avec cette notation, on a : a divise b si et seulement si $v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{P}$.

Il se trouve que la plupart des anneaux intègres que l'on rencontre en algèbre ont la propriété d'existence de la décomposition (la propriété forte est l'unicité). Plus précisément, ceci est lié à la notion suivante :

Proposition 2.8 *Soit A un anneau commutatif (pas forcément intègre). Les trois propriétés suivantes sont équivalentes :*

[3] Si a n'est pas inversible, le produit des p_i qui apparaît n'est pas un produit vide, et on peut remplacer up_1 par p_1, donc se passer de l'unité u dans la décomposition.

i) Pour tout idéal I de A, il existe un nombre fini $x_1, ..., x_n$ d'éléments de I tels que $I = \{\sum_{i=1}^{n} a_i b_i, a_i \in A\}$ (autrement dit : tout idéal de A est engendré par un nombre fini d'éléments).

ii) Toute suite croissante $I_1 \subset I_2 \subset ...I_n \subset ...$ d'idéaux est stationnaire (autrement dit : il existe un indice k tel que $I_n = I_k$ pour tout $n \geq k$).

iii) Toute famille non vide E d'idéaux de A possède un élément maximal (i.e. un élément I de E tel que si J est dans E et $J \supset I$, alors $J = I$).

On dit que A est noethérien s'il vérifie ces propriétés.

Démonstration : 1. implique 2. : soit (I_n) une telle suite, alors la réunion I des I_n est encore un idéal car la famille (I_n) est totalement ordonnée pour l'inclusion. Soient $x_1, ..., x_r$ des éléments de I qui l'engendrent, alors chaque x_i est dans l'un des I_n, donc il existe n_0 (le plus grand des indices correspondants) tel que I_{n_0} les contienne tous. Alors $I = I_{n_0}$ et la suite (I_n) stationne à I_{n_0}.

2. implique 3. : si une famille non vide d'idéaux de A n'a pas d'élément maximal, on construit par récurrence une suite infinie strictement croissante d'idéaux de A, ce qui contredit 2.

3. implique 1. : soit I un idéal de A, alors la famille E des idéaux $J \subset I$ qui sont engendrés par un nombre fini d'éléments est non vide (elle contient $\{0\}$). Soit J_0 un élément maximal de E, alors pour tout x de I, l'idéal $J_0 + xA$ est aussi dans E, donc $J_0 + xA = J_0$ par maximalité. Ceci signifie que $x \in J_0$ Finalement $I = J_0$ et I est engendré par un nombre fini d'éléments.

□

Par exemple via la propriété i), il est clair que tout anneau principal est noethérien et le quotient d'un anneau noethérien par tout idéal reste un anneau noethérien. Il se trouve (voir exercices) que si A est noethérien, on a aussi $A[X]$ noethérien et donc par récurrence $A[X_1, ..., X_n]$ est noethérien, ce qui implique que la plupart des anneaux qu'on rencontre (qui apparaissent comme quotients d'un anneau de polynômes sur un corps ou sur $\mathbf{Z}$) sont noethériens.

Proposition 2.9 *Soit A un anneau intègre noethérien. Alors tout élément non nul a de A admet une décomposition en produit d'irréductibles.*[4]

[4]C'est ici un léger abus de langage pour dire que tout élément non nul admet une décomposition du type (1), i.e. est produit d'un inversible par un produit d'irréductibles.

Démonstration : Soit F l'ensemble des idéaux de A de la forme xA avec x ne s'écrivant pas comme produit d'irréductibles (en particulier, un tel x n'est pas inversible). Si F n'était pas vide, il admettrait un élément maximal $(a) = aA$. En particulier a n'est alors pas irréductible, donc comme il n'est pas inversible il s'écrit $a = bc$ avec b, c dans A non associés à a. Mais alors les idéaux (b) et (c) contiennent strictement (a), donc par maximalité b et c se décomposent en produit d'irréductibles, ce qui contredit le fait que a ne s'écrit pas comme produit d'irréductibles.

□

La proposition suivante donne un critère pour qu'un anneau soit factoriel quand on connaît déjà l'existence de la décomposition en irréductibles.

Proposition 2.10 *Soit A un anneau intègre tel que tout élément non nul de A admette une décomposition en produit d'irréductibles, par exemple un anneau noethérien. Alors les propriétés suivantes sont équivalentes :*

1. *A est factoriel.*
2. *Si $p \in A$ est irréductible, alors l'idéal (p) est premier.*
3. *Soient a, b, c dans $A \setminus \{0\}$. Si a divise bc et est premier avec b, alors a divise c ("lemme de Gauss").*

Démonstration : 3. implique 2. : déjà $(p) \neq A$ car p n'est pas inversible puisqu'irréductible. Si maintenant p divise ab et ne divise pas a, alors p est premier avec a puisque p est irréductible (donc un diviseur commun non inversible de a et p serait associé à p, et p diviserait a), d'où p divise b d'après 3. Ainsi (p) est premier.

2. implique 1. : Soit $\mathcal{P}$ un système de représentants irréductibles. Si $u \prod_{p \in \mathcal{P}} p^{m_p} = v \prod_{p \in \mathcal{P}} p^{n_p}$ sont deux décompositions, alors la condition $m_q > n_q$ pour un certain q de $\mathcal{P}$ impliquerait que q divise $\prod_{p \in \mathcal{P}, p \neq q} p^{n_p}$, donc l'un des facteurs d'après 2. Mais q ne peut diviser p pour $p \in \mathcal{P}$ distinct de q car $\mathcal{P}$ est un système de représentants irréductibles. Ainsi $m_p = n_p$ pour tout $p \in \mathcal{P}$, puis $u = v$ par intégrité de A.

1. implique 3. : on décompose a, b, c comme ci-dessus. Alors pour tout p de $\mathcal{P}$, $v_p(a) \leq v_p(b) + v_p(c)$ (car a divise bc) et $v_p(b) > 0$ implique $v_p(a) = 0$ (car a est premier avec b). Finalement on a $v_p(a) \leq v_p(c)$ aussi bien quand $v_p(b) = 0$ que quand $v_p(b) > 0$. Ainsi a divise c.

□

Theorème 2.11 *Tout anneau principal A est factoriel.*

Démonstration : Comme A est noethérien, on connaît déjà l'existence de la décomposition en irréductibles par la proposition 2.9. Il suffit donc de montrer (en utilisant la caractérisation 2. de la proposition 2.10) que si $p \in A$ est irréductible et si p divise xy avec $x, y \in A$, alors p divise x ou y. Supposons donc que p ne divise ni x ni y. Comme p est irréductible, ceci implique que p est premier avec x et avec y. Comme A est principal, il existe (Bezout) des éléments $a, b, c, d \in A$ avec $ap + bx = 1$ et $cp + dy = 1$. En multipliant, on obtient $(acp + ady + bcx)p + (bd)xy = 1$, ce qui montre que p et (xy) sont premiers entre eux. En particulier, p ne divise pas (xy).

□

Exemples :

1. $\mathbf{Z}$ est factoriel (on peut prendre pour $\mathcal{P}$ l'ensemble des nombres premiers).

2. $K[X]$ est factoriel (on peut prendre pour $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires).

3. Il y a des anneaux factoriels non principaux, même noethériens, par exemple $K[X_1, ..., X_n]$. Aussi, l'anneau $K[(X_n)_{n \in \mathbf{N}^*}]$ est factoriel (ces résultats seront vus dans le cours sur les anneaux de polynômes) mais pas noethérien.

4. L'anneau $A = \mathbf{Z}[i\sqrt{5}] = \mathbf{Z}[T]/(T^2 + 5)$, qui est aussi le sous-anneau de $\mathbf{C}$ constitué des $a + bi\sqrt{5}$ avec $a, b \in \mathbf{Z}$, est intègre et noethérien mais n'est pas factoriel (cf. exemple 2.4, d). En effet $A^* = \{\pm 1\}$, et on a deux décompositions

$$9 = 3 \times 3 = (2 - i\sqrt{5})(2 + i\sqrt{5})$$

dans A, alors que 3 est irréductible, mais n'est associé à aucun des irréductibles $2 - i\sqrt{5}$, $2 + i\sqrt{5}$.

5. Un sous-anneau d'un anneau factoriel (resp. noethérien) ne le reste pas forcément, puisque tout anneau intègre est un sous anneau de son corps des fractions, lequel est évidemment un anneau principal.

Proposition 2.12 *Si A est un anneau factoriel, alors deux éléments non nuls a et b de A (et plus généralement toute famille d'éléments de $A \setminus \{0\}$) ont un pgcd, bien défini à association près.*

Rappelons qu'un pgcd (plus grand commun diviseur) de a et b est un diviseur commun d de a et b, tel que tout autre diviseur commun divise d; "grand" fait réference à la relation d'ordre partiel "divise" sur l'ensemble quotient de $A \setminus \{0\}$ par la relation d'association.

La proposition est immédiate en décomposant a et b suivant un système de représentants $\mathcal{P}$, un pgcd étant $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$ (et de même pour une famille quelconque d'éléments de $A \setminus \{0\}$). On étend immédiatement ceci a une famille d'éléments de A, le pgcd étant alors le même que celui de la famille à laquelle on a éventuellement enlevé 0 (le pgcd de la famille vide, ou encore de la famille réduite à 0, est 0). Notons que deux éléments de A sont premiers entre eux si et seulement si leur pgcd est 1.

On a de même un ppcm de a et b (plus petit commun multiple) en prenant $\prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$, notion qu'on peut étendre à une famille *finie* d'éléments de $A \setminus \{0\}$.