Anneaux et polynômes

David Harari

Agrégation, Orsay, 2017-2018

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*.

Exemples :

1. L'anneau nul $\{0\}$.
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.

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 $\bar{1}$.*

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

On a alors immédiatement le théorème de factorisation habituel :

[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.

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, A/J est isomorphe au quotient $(A/I)/p(J)$, comme dans le cas des groupes, et ce dernier quotient est aussi isomorphe à $A/(I+J)$, où $I+J$ est l'idéal constitué des $i+j$ avec $i \in I$ et $j \in J$.

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

2.1. Éléments irréductibles, anneaux factoriels

Dans tout ce paragraphe, A désigne un anneau commutatif intègre.

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 : 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 $A^* = \{\pm 1\}$.

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.

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 $p \in \mathcal{P}$.

c) 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). En particulier c'est le cas des anneaux *noethériens*, c'est-à-dire des anneaux vérifiant que tout idéal I est engendré par un nombre fini d'éléments de I, par exemple les anneaux principaux. De plus, si A est noethérien, on a aussi $A[X]$ noethérien (et donc par récurrence $A[X_1, ..., X_n]$ est noethérien); si A est noethérien, tout anneau quotient de A est noethérien (mais pas forcément tout sous-anneau). Voir les exercices.

Exemples :

1. $\mathbf{Z}$ est factoriel (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. Plus généralement, tout anneau principal est factoriel : l'existence de la décomposition est une propriété générale des anneaux noethériens. L'unicité se déduit immédiatement de la proposition 2.8 ci-dessous. La réciproque est fausse, par exemple pour $K[X_1, ..., X_n]$.

[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.

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 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 $2 - i\sqrt{5}$, $2 + i\sqrt{5}$.

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

Proposition 2.8 *Soit A un anneau intègre tel que tout élément non nul de A admette une décomposition en produit d'irréductibles*[4]*. 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.

□

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

Proposition 2.9 *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 $A \setminus \{0\}$.

2.2. Factorialité d'un anneau de polynômes

Dans ce paragraphe, A désigne un anneau factoriel .

Définition 2.10 Le *contenu* (noté $c(P)$) d'un polynôme $P \in A[X]$ est le p.g.c.d. de ses coefficients. P est dit *primitif* si $c(P) = 1$.

On notera que le contenu est défini à multiplication par un inversible de A près, par contre l'idéal qu'il engendre est bien défini. D'autre part, on a immédiatement $c(aP) = a.c(P)$ (mod. A^*) pour tout $a \in A$.

Lemme 2.11 (Gauss) *Pour tous P, Q de $A[X]$, on a $c(PQ) = c(P)c(Q)$ (toujours modulo A^*).*

Démonstration : Supposons d'abord P et Q primitifs et montrons que PQ est primitif. Sinon il existe un irréductible p de A qui divise tous les coefficients de PQ. Comme P et Q sont primitifs, chacun a au moins un coefficient non divisible par p. Soit a_{i_0} (resp. b_{j_0}) le coefficient de P (resp. Q) d'indice minimal non divisible par p. Alors le coefficient d'indice $i_0 + j_0$ de PQ est somme de termes divisibles par p et de $a_{i_0}b_{j_0}$ donc il n'est pas divisible par p car (p) est premier vu que A est factoriel. Ceci contredit le fait que tous les coefficients de PQ soient divisibles par p.

On se ramène à P, Q primitifs en appliquant le résultat précédent à $P/c(P)$, $Q/c(Q)$.

□

On en déduit l'important résultat suivant :

Theorème 2.12 *Soit A un anneau factoriel de corps des fractions K. Alors les irréductibles de $A[X]$ sont de deux types :*

i) Les polynômes $P = p$ constants avec p irréductible dans A.

ii) Les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $K[X]$.

En particulier, pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans $A[X]$ et dans l'anneau principal $K[X]$ (ce qui n'est pas du tout évident vu qu'il y a a priori plus de décompositions possibles dans $K[X]$). On fera attention avec les polynômes non primitifs : 2 est irréductible dans $\mathbf{Z}[X]$ mais pas dans $\mathbf{Q}[X]$ (il y est inversible) tandis que $2X$ est irréductible dans $\mathbf{Q}[X]$ mais pas dans $\mathbf{Z}[X]$.

Démonstration : Comme $A[X]^* = A^*$, il est clair qu'un polynôme constant $P = p$ est irréductible si et seulement si p est irréductible dans A (en effet si un polynôme constant non nul se décompose en produit de deux polynômes de $A[X]$, ces polynômes doivent être constants pour raison de degré).

Si d'autre part P est un polynôme primitif de degré ≥ 1 de $A[X]$ qui est irréductible dans $K[X]$, alors une écriture $P = QR$ avec Q, R dans $A[X]$ implique avec le lemme précédent que $c(Q)$ et $c(R)$ soient inversibles. Comme d'autre part l'un des polynômes Q, R est constant (parce que P est irréductible dans $K[X]$), c'est une constante inversible dans A (ou $A[X]$). Finalement P est bien irréductible dans $A[X]$ (il n'est pas inversible car de degré au moins 1).

Il reste à montrer qu'un polynôme P de degré ≥ 1 qui est irréductible dans $A[X]$ est primitif, et irréductible dans $K[X]$. Le fait que P soit primitif résulte de ce que $c(P)$ divise P dans $A[X]$ et ne lui est pas associé pour raison de degré. Il reste à montrer que P (qui n'est pas inversible dans $K[X]$) est irréductible dans $K[X]$. Or si $P = QR$ dans $K[X]$, on peut écrire $Q = Q_1/q$ et $R = R_1/r$ avec q, r dans A et Q_1, R_1 dans $A[X]$. Alors en posant $a = qr$, on obtient $aP = Q_1R_1$, et en passant aux contenus : $a = c(Q_1)c(R_1)$ (modulo A^*). Ainsi $P = u\frac{Q_1}{C(Q_1)}\frac{R_1}{C(R_1)}$ avec $u \in A^*$. Comme P est irréductible dans $A[X]$, l'un des polynômes $\frac{P_1}{C(P_1)}$, $\frac{Q_1}{C(Q_1)}$ de $A[X]$ est inversible, donc constant, et l'un des polynômes Q, R est constant ce qui achève la preuve.

□

On en déduit enfin

Theorème 2.13 *Si A est factoriel, $A[X]$ est factoriel.*

Démonstration : On doit d'abord démontrer qu'on a l'existence de la décomposition [5]. Quitte à écrire $P = c(P)P_1$ et à décomposer $c(P)$ en produit d'irréductibles dans A, on se ramène à P primitif. On décompose alors P (qu'on peut supposer non constant) dans l'anneau principal $K[X]$, soit $P = P_1...P_r$, ou encore $aP = Q_1...Q_r$ avec $Q_i \in A[X]$, $a \in A$, et Q_i irréductible dans $K[X]$. En passant aux contenus, on obtient $a = c(Q_1)...c(Q_r)$ (mod. A^*) et d'après le théorème précédent $P = u.\prod_{i=1}^{r} \frac{Q_i}{c(Q_i)}$ (avec $u \in A^*$) est une décomposition de P en produits d'irréductibles de $A[X]$, puisque chaque $\frac{Q_i}{c(Q_i)}$ est un polynôme primitif de $A[X]$ qui est irréductible dans $K[X]$ (il est le produit de Q_i par une constante de K^*).

Il suffit donc d'après la proposition 2.8 de montrer que si $P \in A[X]$ est irréductible, alors (P) est premier. Si $P = p$ est une constante irréductible de $A[X]$, alors p n'est pas inversible et si p divise un produit QR de deux polynômes de $A[X]$, alors il divise aussi le contenu $c(QR) = c(Q)c(R)$, donc il divise $c(Q)$ ou $c(R)$ vu que (p) est premier dans A (puisque A est factoriel). Ainsi la constante p divise bien Q ou R dans $A[X]$ (on aurait pu aussi remarquer que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$, qui est intègre vu que (p) est premier dans A).

Supposons donc P primitif de degré au moins 1, et donc irréductible dans $K[X]$ d'après le théorème précédent. Alors si P divise le produit QR de deux polynômes de $A[X]$, il divise Q ou R dans $K[X]$ vu que $K[X]$ est principal, par exemple Q. Il existe donc a dans A tel que $aQ = SP$ avec $S \in A[X]$. Alors $ac(Q) = c(S)$ (mod. A^*) car P est primitif, et a divise $c(S)$. En particulier $Q = (S/a)P$ avec S/a dans $A[X]$, i.e. P divise Q dans $A[X]$. C'est ce qu'on voulait montrer.

□

Corollaire 2.14 *Si A est factoriel, $A[X_1, ..., X_n]$ est factoriel.* [6]

Il est commode d'avoir un critère pratique d'irréductibilité dans les anneaux factoriels. Le résultat suivant est souvent utile :

Theorème 2.15 (Critère d'Eisenstein) *Soient A un anneau factoriel, P un polynôme non constant de $A[X]$, p irréductible dans A. On pose $P = \sum_{k=0}^{n} a_k X^k$ et on suppose :*

[5] Noter que A n'est pas forcément noethérien

[6] On a l'analogue avec une infinité d'indéterminées, c'est immédiat à partir du cas fini.

1. *p ne divise pas a_n.*

2. *p divise a_k pour $0 \leq k \leq n-1$.*

3. *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$ (donc aussi dans $A[X]$ s'il est primitif).

Pour une preuve, voir les exercices. Par exemple $X^{18} - 4X^7 - 2$ est irréductible dans $\mathbf{Q}[X]$, et $X^5 - XY^3 - Y$ est irréductible dans $\mathbf{C}[X, Y]$ (prendre $A = \mathbf{C}[Y]$ et $p = Y$).