Chapitre 5

Eléments d'algèbre commutative

Sauf mention du contraire, tous les anneaux et corps considérés dans ce chapitre sont supposés commutatifs.

5.1 Idéaux et quotients

5.1.1. Nous supposons connue la notion d'anneau (commutatif, d'après nos conventions), celle de corps, et celle de k-algèbre, où k est un corps, ainsi que celles de sous-anneau (resp. sous-k-algèbre) et d'homomorphisme d'anneaux (resp. de k-algèbres.) Un anneau A peut être réduit à $\{0\}$; c'est le cas si et seulement si l'on a $1 = 0$ dans A. En revanche, dans un corps on a toujours $1 \neq 0$. On rappelle qu'un *idéal* dans un anneau A est un sous-groupe abélien I de A tel que pour tous $a \in A$, $x \in I$ l'on ait $ax \in I$. Par exemple, le noyau d'un homomorphisme d'anneaux $\varphi : A \to A'$ est toujours un idéal. Un idéal I de A est dit *propre* si $I \neq A$; c'est le cas si et seulement si $1 \notin I$.

5.1.2 Proposition. — *Soit A un anneau, I un idéal de A. Alors il existe une unique structure d'anneau sur le groupe abélien quotient A/I telle que la surjection canonique $\pi : A \to A/I$ soit un homomorphisme d'anneaux. Si A est une k-algèbre, I est toujours un sous-k-espace vectoriel de A, et A/I est une k-algèbre pour la structure d'anneau définie ci-dessus et la structure d'espace vectoriel quotient.*

Démonstration. — Comme d'habitude : la formule $\pi(x)\pi(y) = \pi(xy)$ montre que si la structure d'anneau sur A/I existe, elle est unique. Pour que cette formule définisse bien une fonction de $A/I \times A/I$ vers A/I, il faut prouver que si $\pi(x) = \pi(x')$, $\pi(y) = \pi(y')$, alors $\pi(xy) = \pi(x'y')$; or c'est clair, puisque l'on a $x - x' \in I$, $y - y' \in I$, donc

$$\pi(xy) - \pi(x'y') = \pi((x - x')y + x'(y - y')) = 0$$

puisque $(x - x')y$ et $x'(y - y')$ appartiennent à I. Maintenant le fait que le produit soit associatif, commutatif, d'élément neutre $\pi(1)$, et distributif par rapport à l'addition, est immédiatement hérité des propriétés correspondantes pour A.

Si A est une k-algèbre, on peut en fait identifier k à un sous-anneau de A par l'application $\lambda \to \lambda.1$. Cela prouve que tout idéal de A est stable par multiplication par les

éléments de k, et est donc un sous-k-espace vectoriel ; ainsi A/I est muni d'une structure d'espace vectoriel quotient. Alors comme ci-dessus, la k-bilinéarité de la multiplication, qui exprime le fait que A/I est une k-algèbre, est héritée de la propriété correspondante pour A.

5.1.3 Remarque. — Dans les notations de la proposition, il est facile de voir que les applications $J \to J/I$, $J' \to \pi^{-1}(J')$ sont des bijections réciproques l'une de l'autre de l'ensemble des idéaux de A contenant I sur l'ensemble des idéaux de A/I. De plus ces bijections sont compatibles avec la relation d'inclusion.

En effet, la surjectivité de π implique que pour *tout* idéal J de A, $\pi(J)$ est un idéal de A/I ; si J contient I, on a $\pi(J) = J/I$ et il est immédiat de vérifier que $\pi^{-1}\pi(J) = J$. Réciproquement, pour tout idéal J' de A/I on voit que $\pi^{-1}(J')$ est un idéal de A contenant I ; et l'on vérifie aussitôt que $\pi\pi^{-1}(J') = J'$.

5.1.4. *Sous-anneaux et idéaux engendrés.* Soit A un anneau, S une partie de A. Alors il existe un unique plus petit sous-anneau de A contenant S ; c'est le sous-groupe abélien de A engendré par les produits finis $x_1 \dots x_s$, $s \in \mathbf{N}$, $x_1, \dots, x_s \in S$ (on rappelle que comme d'habitude le produit vide, correspondant à $s = 0$, est égal par convention à 1) — nous laisserons au lecteur le soin de vérifier que ceci est bien un sous-anneau de A avec la propriété voulue. Si A est une k-algèbre, on définit de même la sous-k-algèbre engendrée par S ; il suffit de remplacer le sous-groupe abélien ci-dessus par le sous-k-espace vectoriel engendré par les produits finis d'éléments de S.

De même, il existe un unique plus petit idéal de A contenant S ; c'est l'ensemble des sommes finies $a_1x_1 + \ldots + a_sx_s$, où les a_j appartiennent à A et les x_j appartiennent à S.

Dans le cas particulier où $S = \{x\}$ est réduit à un seul élément, le sous-anneau (resp. la sous-k-algèbre) engendré par S est simplement l'ensemble des combinaisons linéaires à coefficients dans $\mathbf{Z}$ (resp. dans k) des x^j, $j \in \mathbf{N}$; l'idéal engendré par S est l'ensemble des ax, $a \in A$. On note Ax cet idéal ; un idéal engendré par un seul élément sera dit *principal*. Plus généralement, si $S = \{x_1, \dots, x_m\}$ est fini, on pourra noter $Ax_1 + \ldots + Ax_m$ l'idéal engendré par S (attention, il ne s'agit pas d'une somme directe en général !)

5.1.5. On rappelle qu'un élément b dans un anneau A est dit *diviseur de zéro*, s'il existe $a \neq 0$ dans A tel que $ab = 0$. Par ailleurs, un élément a est dit *inversible*, s'il existe $b \in A$ tel que $ab = 1$; b est alors unique et sera noté a^{-1}.

On dit qu'un élément $a \neq 0 \in A$ est *simplifiable*, s'il n'est pas diviseur de zéro ; la terminologie vient du fait que si $ax = ay$, alors $x = y$ (puisque $a(x - y) = 0$ implique $x - y = 0$.) Pour tout anneau A, notons $A^\bullet$ l'ensemble des éléments simplifiables de A, et $A^\times$ le groupe des éléments inversibles de A. Alors on vérifie facilement (exercice) que $A^\bullet$ est stable par multiplication, et bien sûr $A^\times \subset A^\bullet$.

5.2 Idéaux premiers et idéaux maximaux

5.2.1 Définition. — Soit A un anneau.

(a) On dit que A est *intègre*, si $1 \neq 0$ dans A, et si $A^\bullet = A\backslash\{0\}$ (*i.e.*, 0 est le seul diviseur de zéro dans A.)
(b) Un idéal P de A est dit *premier*, si A/P est intègre.
(c) Un idéal M de A est dit *maximal*, si A/M est un corps.

5.2.2 Remarque. — Puisqu'un corps est toujours intègre, il est clair que tout idéal maximal est premier ; la réciproque est bien sûr fausse : soit A un anneau intègre qui n'est pas un corps, par exemple $A = \mathbf{Z}$; alors l'idéal $\{0\}$ est premier, puisque $A/\{0\} = A$ est intègre, mais n'est pas maximal.

5.2.3 Proposition. — *Soit $\varphi : A \to B$ un homomorphismes d'anneaux. Alors pour tout idéal premier Q de B, $\varphi^{-1}(Q)$ est un idéal premier de A.*

Démonstration. — C'est immédiat : on peut reformuler la définition en disant qu'un idéal P de A est premier si et seulement si pour tous $x, y \in A$, $xy \in P$ entraîne $x \in P$ ou $y \in P$. Or $xy \in \varphi^{-1}(Q)$ équivaut à $\varphi(xy) = \varphi(x)\varphi(y) \in Q$, donc $\varphi(x) \in Q$ ou $\varphi(y) \in Q$.

5.2.4. La proposition suivante explique le mot "maximal" dans la déf. 5.2.1 :

Proposition. — *Soit A un anneau, I un idéal de A. Alors I et maximal si et seulement si il est propre, et maximal pour l'inclusion dans l'ensemble des idéaux propres de A.*
Démonstration. — Puisque dans un corps on a $0 \neq 1$, tout idéal maximal M de A est propre. Si J est un idéal de A contenant M, d'après la remarque 5.1.3, J/M est un idéal du corps $K = A/M$. Or si J/M contient un élément $x \neq 0$, il contient aussi $x^{-1}x = 1$, donc $J/M = K$, et $J = \pi^{-1}(J/M) = A$. Donc si J est propre, on doit avoir $J/M = \{0\}$, donc $J = M$, ce qui montre que M est maximal pour l'inclusion dans l'ensemble des idéaux propres de A.

Réciproquement, soit I un idéal propre maximal pour l'inclusion, et soit $x \in A$, $x \notin I$. Alors l'idéal $I + Ax$ contient strictement I, donc est égal à A. En particulier il existe $a \in A$ et $y \in I$ tels que $y + ax = 1$; alors $\pi(y + ax) = \pi(a)\pi(x) = 1$ dans l'anneau A/I, ce qui montre que $\pi(x)$ est inversible. Comme ceci est vrai pour tout x tel que $\pi(x) \neq 0$, A/I est bien un corps.

5.2.5 Théorème. — (Krull) *Soit A un anneau. Alors tout idéal propre de A est contenu dans un idéal maximal.*

Démonstration. — On utilise le lemme de Zorn. Soit I un idéal propre de A, et soit $\mathcal{F}$ l'ensemble des idéaux propres de A contenant I, ordonné par inclusion. Montrons que $\mathcal{F}$ est inductif. Soit $(J_\lambda)_{\lambda\in\Lambda}$ une famille totalement ordonnée d'éléments de $\mathcal{F}$, et posons $J = \cup_{\lambda\in\Lambda} I_\lambda$. Alors on voit facilement que J est un idéal de A contenant I, et de plus J est propre, car si $1 \in J$ on aurait déjà $1 \in J_\lambda$ pour un certain $\lambda \in \Lambda$, ce qui contredit le fait que J_λ est propre. D'après le lemme de Zorn, $\mathcal{F}$ contient donc un élément maximal M, qui est l'idéal maximal cherché (car on voit aussitôt que M est aussi un élément maximal dans l'ensemble de *tous* les idéaux propres de A, et on applique la prop. 5.2.4.)

5.3 Corps de fractions et localisation

5.3.1. Il est clair que tout sous-anneau d'un anneau intègre est encore intègre ; en particulier tout sous-anneau d'un *corps* est un anneau intègre. Nous nous proposons de prouver la réciproque : tout anneau intègre peut être plongé dans un corps, et même, il existe à isomorphisme près un unique corps K contenant A et qui soit "le plus petit possible", en un sens à préciser.

5.3.2. Puisque A est intègre, on a $A^\bullet = A\backslash\{0\}$. Soient $a, b \in A^\bullet$. On dit que a *divise* b, et l'on note $a|b$, s'il existe $c \in A^\bullet$ tel que $b = ac$. La relation "a divise b" est réflexive et transitive, mais non antisymétrique en général : on peut avoir $a|b$ et $b|a$ sans que $a = b$; si $a|b$ et $b|a$ on dit que a et b sont *associés*. On dit qu'un diviseur de $a \in A^\bullet$ est *trivial*, s'il est de la forme $u \in A^\times$ ou de la forme ua, $u \in A^\times$. On dit qu'un élément $p \in A^\bullet$ est *irréductible*, s'il n'est pas inversible et s'il ne possède pas de diviseurs non-triviaux.

Pour tout $a \in A^\bullet$, notons simplement (a) l'idéal principal Aa.

5.3.3 Proposition. — *Soient $a, b \in A^\bullet$.*
(a) *On a $a|b$ si et seulement si $(b) \subset (a)$; en particulier a et b sont associés si et seulement si $(a) = (b)$.*
(b) *Les éléments a et b sont associés si et seulement si il existe $u \in A^\times$ tel que $b = ua$.*

Démonstration. — Clairement, si $a|b$ on a $b \in (a)$, donc $(b) \subset (a)$; réciproquement, si $(b) \subset (a)$ on a $b \in (a)$, donc il existe $c \in A$, nécessairement non nul, tel que $b = ac$. Ceci prouve *(a)*. S'il existe $u \in A^\times$ tel que $b = ua$, on a $a|b$ et $a = u^{-1}b$ donc $b|a$; réciproquement, si $b = ac$ et $a = bd$, on a $a = acd$ donc $cd = 1$, ce qui prouve que c et d sont inversibles.

5.3.4 Remarque. — Il résulte de la proprosition ci-dessus que la relation "a est associé à b" est une relation d'équivalence sur $A^\bullet$, et ce pour deux raisons : d'une part a et b sont associés si et seulement si ils ont même image par l'application $a \to (a)$ de $A^\bullet$ vers l'ensemble des idéaux principaux de A, ce qui est notre procédé canonique pour définir des relations d'équivalence ; d'autre part, a et b sont associés si et seulement si ils sont dans la même orbite pour l'action du groupe $A^\times$ sur $A^\bullet$. On parlera donc de classes d'association d'éléments de $A^\bullet$.

5.3.5. Pour comprendre la consturction du corps de fractions de A, le mieux est de supposer d'abord le problème résolu, *i.e.* de supposer A plongé dans un corps L. Alors l'ensemble L' des éléments de L de la forme a/s, $a \in A$, $s \in A^\bullet$, est un sous-corps de L (exercice) ; en fait on voit facilement que c'est le plus petit sous-corps de L contenant A. On voit que $a/s = b/t$ dans L si et seulement si $at = bs$ dans A ; pour chaque $s \in A^\bullet$ fixé, l'ensemble des a/s, $a \in A$, est un sous-groupe additif de L' contenant A, et L' est la réunion de ces sous-groupes lorsque s varie. Nous allons utiliser ces remarques pour faire la construction de L' "dans l'abstrait".

5.3.6. Soit E l'ensemble $A \times A^\bullet$, et considérons sur E la relation $\sim$ définie par $(a, s) \sim (b, t)$ si et seulement si $at = bs$ dans A. Alors $\sim$ est une relation d'équivalence : en effet si $(a, s) \sim (b, t)$ et $(b, t) \sim (c, u)$, on a $at = bs$, $bu = ct$, et en multipliant la première

égalité par u et la deuxième par s, on obtient $but = atu = cts$, donc en simplifiant par t, $au = cs$. On note K l'ensemble quotient $E/\sim$, et l'on note $(a,s) \to a/s$ la surjection canonique de E vers K.

Pour chaque $s \in A^\bullet$ fixé, l'application $a \to a/s$ est injective de A vers K ; on note A/s son image, et on la munit de la structure de groupe résultant de son identification avec A. On identifie $A/1$ avec A. Remarquons que $A/s \subset A/t$ si et seulement si s divise t : en effet si $A/s \subset A/t$ il existe $c \in A$ tel que $1/s = c/t$, donc $t = cs$; si $t = cs$ on a $at = acs$ pour tout $a \in A$, donc $a/s = ac/t$, ce qui montre bien que $A/s \subset A/t$. Cette inclusion respecte la structure de groupe : en effet dans l'identification de A/s et A/t avec A, avec $t = cs$, l'inclusion se traduit par l'application $a \to ac$ (*i.e.*, l'élément de K identifié à a dans A/s est celui qui est identifié à ac dans A/t.) C'est donc bien un homomorphisme de groupes. En particulier $A/s = A/t$ si et seulement si s et t sont associés, et la structure de groupe sur A/s ne dépend pas du choix de s dans sa classe d'association.

5.3.7. Remarquons maintenant que pour $s, t \in A^\bullet$ quelconques, il existe toujours $r \in A^\bullet$ contenant à la fois A/s et A/t : il suffit de prendre $r = st$. On en déduit que $A/s \cap A/t$ est un sous-groupe à la fois de A/s et de A/t, puisque c'est l'intersection de deux sous-groupes de A/r ; et donc que si $x, y \in K$ appartiennent à la fois à A/s et A/t, leur somme est la même, qu'on la calcule dans A/s ou dans A/t.

Ces remarques vont nous permettre de munir K tout entier d'une structure de groupe abélien. Pour $x, y \in K$ on définit $x + y$ comme étant la somme de x et y dans n'importe quel A/r qui les contient tous les deux ; d'après ce qui précède un tel A/r existe toujours, et le résultat ne dépend pas du choix de r. Pour prouver que $x + (y + z) = (x + y) + z$ pour tous $x, y, z \in K$, il suffit de se placer dans un A/r qui les contient tous trois, et d'utiliser l'associativité de l'addition dans A/r ; la commutativité est claire, ainsi que le fait que $0/1$ est élément neutre, et que $(-a)/s$ est opposé à a/s.

5.3.8. Passons maintenant à la définition de la multiplication. Pour tous $s, t \in A^\bullet$ fixés, considérons l'application $\mathbf{Z}$-bilinéaire $(a/s, b/t) \to ab/st$ de $A/s \times A/t$ dans K. On vérifie immédiatement que ces applications sont compatibles avec les relations d'inclusion entre les A/s : si $r = cs$, on écrit $a/s = ac/r$, et $ab/st = acb/rt$, donc on a bien le même résultat que le calcul soit fait dans A/s ou dans A/r ; de même pour la deuxième variable. Donc on obtient une application $\mathbf{Z}$-bilinéaire bien définie de $K \times K$ dans K. L'associativité, la commutativité et le fait que $1/1$ soit élément neutre se vérifient immédiatement ; on a donc maintenant muni K d'une structure d'anneau commutatif, et l'application $a \to a/1$ est un homomorphisme d'anneaux qui permet d'identifier A à un sous-anneau de K.

On a $a/s = 0/1$ si et seulement si $a = 0$. Pour montrer que K est un corps, il suffit donc de montrer que tout a/s avec $a \neq 0$ est inversible ; or $a/s.s/a = as/sa = 1/1$, donc s/a est inverse de a/s.

5.3.9 Définition. — Le corps K construit ci-dessus est appelé *corps de fractions* de l'anneau intègre A, et se note $\mathrm{Fract}(A)$. Comme on l'a vu, on identifie A à un sous-anneau de $\mathrm{Fract}(A)$ par l'application $a \to a/1$.

5.3.10 Proposition. — (propriété universelle des corps de fractions) *Soit A un anneau intègre, B un anneau, et φ un homomorphisme d'anneaux de A vers B. Supposons que pour tous $s \in A^\bullet$, $\varphi(s)$ soit inversible dans B. Alors φ s'étend de façon unique en un homomorphisme d'anneaux $\overline{\varphi} : K = \mathrm{Fract}(A) \to B$; l'image de $\overline{\varphi}$ est l'ensemble des $\varphi(a)\varphi(s)^{-1}$, $a \in A$, $s \in A^\bullet$.*

Démonstration. — L'application $(a, s) \to \varphi(a)\varphi(s)^{-1}$ de $A \times A^\bullet$ vers B passe au quotient par la relation d'équivalence définie en 5.3.6. Comme les régles de calcul des expressions a/s dans K sont les mêmes que celles des expressions $\varphi(a)\varphi(s)^{-1}$ dans B, l'application $a/s \to \varphi(a)\varphi(s)^{-1}$ qui s'en déduit par passage au quotient est un homomorphisme d'anneaux.

Reste à prouver l'unicité. Mais c'est facile : si $\psi : K \to B$ est un homomorphisme d'anneaux tel que $\psi|_A = \varphi$, on a pour tous $a \in A$, $s \in A^\bullet$:

$$\psi(a/s)\varphi(s) = \psi(a/s)\psi(s) = \psi((a/s)s) = \psi(a) = \varphi(a)$$

donc $\psi(a/s) = \varphi(a)\varphi(s)^{-1} = \overline{\varphi}(a/s)$.

5.3.11 Corollaire. — (unicité du corps de fractions) *Soit L un corps contenant A, et tel que tout élément de L soit de la forme a/s, $a \in A$, $s \in A^\bullet$. Alors L est canoniquement isomorphe* à $\mathrm{Fract}(A)$.

Démonstration. — L'homomorphisme $\overline{\varphi} : \mathrm{Fract}(A) \to L$ déduit de l'injection canonique $A \subset L$ est un isomorphisme.

5.3.12. *Localisation.* Soit à nouveau A un anneau intègre. Dans certains cas, il est utile de considérer des "anneaux de fractions partielles" de l'anneau A, encore appelés "localisés" de A en vertu de leur interprétation en géométrie algébrique (bien sûr, pour nous le mot de localisation sera une simple terminologie.) Soit S une partie de $A^\bullet$ contenant 1 et stable par multiplication (on dira que S est une *partie multiplicative* de A.) Alors on note $S^{-1}A$ le sous-ensemble de $\mathrm{Fract}(A)$ formé des fractions de la forme a/s, $a \in A$, $s \in S$. On voit aussitôt que $S^{-1}A$ est un sous-anneau de $\mathrm{Fract}(A)$ contenant A.

Alors la prop. 5.3.10 se généralise de la façon suivante :

5.3.13 Proposition. — *Soit A un anneau intègre, S une partie multiplicative de A. Soit B un anneau, et $\varphi : A \to B$ un homomorphisme d'anneaux tel que pour tout $s \in S$, $\varphi(s)$ soit inversible dans B. Alors φ sétend de manière unique en un homomorphisme d'anneaux $\overline{\varphi} : S^{-1}A \to B$.*

Démonstration. — Exercice.

5.3.14 Exercice. — Soit $\mathbf{D}$ l'anneau des nombres décimaux, *i.e.* des nombres dont le développement décimal ne comporte qu'un nombre fini de chiffres après la virgule. Montrer qu'il existe une partie multiplicative S de $\mathbf{Z}$, que l'on déterminera, telle que $\mathbf{D} = S^{-1}\mathbf{Z}$.

5.4 Divisibilité : cas des anneaux principaux

5.4.1 Définition. — On dit qu'un anneau A est *principal*, s'il est intègre, et si tous les idéaux de A sont principaux.

Exemples. — On sait que l'anneau $\mathbf{Z}$, et l'anneau $k[X]$ des polynômes à une indéterminée sur un corps k, sont principaux (dans les deux cas, cela résulte de l'algorithme de la division euclidienne.)

5.4.2 Proposition. — *Soit A un anneau principal. Alors $p \in A^\bullet$ est irréductible si et seulement si l'idéal (p) est maximal.*

Démonstration. — Il résulte en fait de la prop. 5.3.3 que dans tout anneau intègre, p est irréductible si et seulement si (p) est maximal dans l'ensemble des idéaux principaux propres de A. Or dans un anneau principal, *tous* les idéaux sont principaux ; d'où la proposition.

5.4.3 Corollaire. — (lemme d'Euclide) *Soit $p \in A^\bullet$ irréductible, et soient $a, b \in A^\bullet$. Alors si p divise ab, p divise a ou p divise b.*

Démonstration. — La propriété du corollaire exprime le fait que $A/(p)$ est intègre, ce qui est clair puisque c'est même un corps.

5.4.4 Proposition. — *Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.*

Démonstration. — Soit $(\mathfrak{a}_n)_{n\geq 1}$ une suite croissante d'idéaux de A. Alors on vérifie immédiatement que $\mathfrak{a} = \cup_n \geq 1 \mathfrak{a}_n$ est encore un idéal, donc de la forme (a) pour un certain élément $a \in \mathfrak{a}$. Mais alors il existe $n \geq 1$ tel que $a \in \mathfrak{a}_n$; donc $\mathfrak{a} = \mathfrak{a}_n$ et $\mathfrak{a}_m = \mathfrak{a}_n$ pour tout $m \geq n$.

5.4.5 Théorème. — *Soit A un anneau principal. Alors tout $a \in A^\bullet$ possède une écriture $a = up_1 \dots p_s$ où $u \in A^\times$, $s \in \mathbf{N}$, et les p_j sont irréductibles (on dira qu'une telle écriture est une décomposition de a en produit fini d'irréductibles ; comme d'habitude, on convient qu'un produit vide est égal à 1.) Dans cette écriture, s est unique, et les p_j sont uniques à l'ordre près et à association près.*

Démonstration. — (a) Existence. Supposons que $a = a_1 \in A^\bullet$ ne soit pas produit fini d'irréductibles. Alors en particulier a n'est ni inversible, ni irréductible, et possède donc une décomposition $a_1 = a'_1 a''_1$, où a'_1 et a''_1 sont tous deux des diviseurs non triviaux de a_1. Si a'_1 et a''_1 étaient tous deux produits finis d'irréductibles, a_1 le serait aussi ; on peut donc supposer que l'un des deux, disons a'_1, n'est pas produit fini d'irréductibles, et poser $a_2 = a'_1$. Poursuivant de proche en proche, on construit une suite $(a_n)_{n\geq 1}$ d'éléments de A, telle qu'aucun a_n ne soit produit fini d'irréductibles, et telle que a_{n+1} soit un diviseur non trivial de a_n pour tout $n \geq 1$. Mais alors la suite d'idéaux principaux (a_n) est strictement croissante et infinie, ce qui contredit la prop. 5.4.4. Donc notre hypothèse est absurde, et tout $a \in A^\bullet$ possède une décomposition en produit fini d'irréductibles.

(b) Unicité. Soit $a \in A^\bullet$. Si a est inversible, tous les diviseurs de a sont inversibles, et la seule écriture possible est celle où $s = 0$, $u = a$. Supposons a non inversible, et soient

$$a = up_1 \dots p_s = vq_1 \dots q_t$$

deux décompositions de a en produit fini d'irréductibles. On peut supposer que s est aussi petit que possible, et faire une récurrence sur s. D'après le cor. 5.4.3, tout diviseur irréductible p de a divise l'un des q_j, et est donc égal à q_j à association près. Après permutation des q_j et modification de v, on peut donc supposer que $p_1 = q_1$. Alors on simplifie par p_1, et l'on obtient : $up_2 \dots p_s = vq_2 \dots q_t$. Par hypothèse de récurrence, on a maintenant $s - 1 = t - 1$, donc $s = t$, et après permutation des q_j si nécessaire, p_j est associé à q_j pour $2 \leq j \leq s$.

5.5 Anneaux factoriels

5.5.1 Définition. — Soit A un anneau intègre. On dit que A est *factoriel*, si tout $a \in A^\bullet$ possède une décomposition en produit fini d'irréductibles (avec les mêmes conventions que dans le thm. 5.4.5), de manière unique à association et permutation des facteurs près.

Exemple. — Il résulte du thm. 5.4.5 que tous les anneaux principaux, et en particulier $\mathbf{Z}$ et les anneaux $k[X]$, où k est un corps, sont factoriels.

5.5.2 Lemme. — *Soit A un anneau intègre, $p \in A^\bullet$ non inversible. Alors les deux conditions suivantes sont équivalentes :*
(i) *(lemme d'Euclide) Pour tous $a, b, \in A$, p divise ab si et seulement si p divise a ou p divise b ;*
(ii) *(p) est premier.*
De plus, si p vérifie (i) *ou* (ii)*, alors p est irréductible.*

Démonstration. — Les conditions *(i)* et *(ii)* expriment toutes deux que l'anneau $A/(p)$ est intègre ; elles sont donc équivalentes.

Si p vérifie *(i)*, et $p = ab$ avec $a, b \in A^\bullet$, on a bien sûr $p|ab$ donc p divise a ou b ; disons p divise a. Mais on a aussi $a|p$; donc p est associé à a, et b est inversible. Ainsi p n'a pas de diviseurs non-triviaux, donc p est irréductible.

5.5.3 Proposition. — *Tout anneau factoriel vérifie les conditions équivalentes du lemme 5.5.2.*

Démonstration. — Soient $a, b \in A$ et p irréductible divisant ab. Alors il existe $c \in A$ tel que $ab = pc$. Soient $a = up_1 \dots p_s$ et $b = vq_1 \dots q_t$ des décompositions de a, b en produit fini d'irréductibles. Alors :

$$ab = uv\, p_1 \dots p_s q_1 \dots q_t$$

et en écrivant de même c en produit fini d'irréductibles, on obtient une autre décomposition de ab contenant le facteur p. De l'unicité de la décomposition il résulte que p est associé à l'un des p_i ou à l'un des q_j, ce qui entraîne bien que $p|a$ ou $p|b$.

5.5.4. *Normalisation.* Soit A un anneau factoriel. Pour se débarasser de l'ambigüité causée par les éléments inversibles, on peut procéder comme suit. Faisons choix une fois pour toutes d'un ensemble P de représentants des classes d'association d'éléments irréductibles dans $A^\bullet$. Par exemple, pour $A = \mathbf{Z}$, on a $A^\times = \{\pm 1\}$, et l'on pourra prendre pour P l'ensemble des entiers irréductibles *positifs*, *i.e.* des nombres premiers. Pour $A = k[X]$, on a $A^\times = k^\times$ (l'ensemble des polynômes constants non nuls), et l'on peut prendre pour P l'ensemble des polynômes irréductibles *unitaires*, *i.e.* ceux dont le coefficient dominant est égal à 1.

Alors tout $a \in A^\bullet$ s'écrit de façon *unique*

$$a = u \prod_{p \in P} p^{\alpha_p} \qquad \text{avec } u \in A^\times,\ \alpha_p \in \mathbf{N} \text{ presque tous nuls}$$

Pour $a = u \prod_{p\in P} p^{\alpha_p}$, $b = v \prod_{p\in P} p^{\beta_p}$ dans $A^\bullet$ on définit alors :

$$\operatorname{pgcd}(a,b) = \prod_{p \in P} p^{\gamma_p} \qquad \text{avec } \gamma_p = \min(\alpha_p, \beta_p)$$

$$\operatorname{ppcm}(a,b) = \prod_{p \in P} p^{\gamma_p} \qquad \text{avec } \gamma_p = \max(\alpha_p, \beta_p)$$

(noter que l'élément de $A^\times$ a été choisi égal à 1.) On définit de même le pgcd et le ppcm d'une famille finie d'éléments de $A^\bullet$. On dit que $a_1, \ldots, a_s \in A^\bullet$ sont *premiers entre eux* (dans leur ensemble), si $\operatorname{pgcd}(a_1, \ldots, a_s) = 1$. Pour la commodité des énoncés, on inclut dans la définition le cas $s = 1$: on a $\operatorname{pgcd}(a_1) = 1$ si et seulement si $a_1 \in A^\times$.

5.5.5. Plus généralement, soit K le corps de fractions de A. Alors tout $x \in K$ s'écrit de façon unique :

$$x = u \prod_{p \in P} p^{\alpha_p} \qquad \text{avec } u \in A^\times,\ \alpha_p \in \mathbf{Z} \text{ presque tous nuls}$$

En effet, l'existence est claire, et pour l'unicité, si on a deux écritures :

$$x = u \prod_{p \in P} p^{\alpha_p} = v \prod_{p \in P} p^{\beta_p}$$

il suffit de choisir pour chaque $p \in P$ le plus petit $\gamma_p \geq 0$ tel que $\alpha_p + \gamma_p \geq 0$, $\beta_p + \gamma_p \geq 0$ (les γ_p sont donc presque tous nuls), et de multiplier les deux membres par $\prod_{p\in P} \gamma_p$, ce qui donne :

$$u \prod_{p \in P} p^{\alpha_p + \gamma_p} = v \prod_{p \in P} p^{\beta_p + \gamma_p}$$

l'égalité ayant cette fois lieu dans A. L'unicité de la décomposition dans A donne maintenant $\alpha_p + \gamma_p = \beta_p + \gamma_p$ pour tout $p \in P$, d'où aussi $\alpha_p = \beta_p$.

5.5.6 Corollaire. — *Le groupe abélien $K^\times/A^\times$ est libre de base P (identifié à son image canonique dans $K^\times/A^\times$), et $K^\times \simeq A^\times \times \mathbf{Z}^{(P)}$.*

5.5.7. Il est immédiat de voir que la construction des anneaux de polynômes à une indéterminée, que les lecteur connaît certainement dans le cas d'un corps, s'étend en fait à un anneau de base A quelconque, intègre ou non ; nous reverrons cette construction au chapitre 6 dans le cas d'un nombre quelconque d'indéterminées. Si A est intègre de corps de fractions K, $A[X]$ s'identifie à un sous-anneau de $K[X]$ (et en particulier $A[X]$ est encore intègre.)

Nous nous proposons de montrer que si A est factoriel, $A[X]$ est encore factoriel. Pour cela, nous introduisons d'abord la notion de *contenu* d'un polynôme $f \in K[X]^\bullet$. On choisit P comme en 5.5.4. Soit $f = a_0 + a_1X + \ldots + a_mX^m \in K[X]^\bullet$, et soit J l'ensemble des $j \in \{0, \ldots, m\}$ tels que $a_j \neq 0$. On pose :

$$\mathrm{cont}\,(f) = \prod_{p \in P} p^{\gamma_p} \qquad \text{avec } \gamma_p = \min_{j \in J}\{\text{exposant de } p \text{ dans } a_j\}$$

Exemple. — Si $A = \mathbf{Z}$, $f = 6X^2 - \dfrac{9}{2}X + 12$, $\mathrm{cont}\,(f) = \dfrac{3}{2}$.

5.5.8 Proposition. — *Soit A factoriel, $f \in K[X]^\bullet$.*
(a) *$f \in A[X]$ si et seulement si* $\mathrm{cont}\,(f) \in A$.
(b) $\mathrm{cont}\,(f) = 1$ *si et seulement si $f \in A[X]$ et les coefficients de f sont premiers entre eux dans leur ensemble.*
(c) $\mathrm{cont}\,(p^\alpha f) = p^\alpha \mathrm{cont}\,(f)$ *pour tout $p \in P$ et tout $\alpha \in \mathbf{Z}$.*
(d) $\mathrm{cont}\,(f/\mathrm{cont}\,(f)) = 1$.

Démonstration. — Exercice facile.

5.5.9 Théorème. — ("lemme de Gauss") *Soit A factoriel. Pour tous $f, g \in K[X]^\bullet$ on a*

$$\mathrm{cont}\,(fg) = \mathrm{cont}\,(f)\,\mathrm{cont}\,(g)$$

Démonstration. — Soient $f_1 = f/\mathrm{cont}\,(f)$, $g_1 = g/\mathrm{cont}\,(g)$. Alors en appliquant de façon répétée la prop. 5.5.8 *(c)* on a :

$$\mathrm{cont}\,(fg) = \mathrm{cont}\,(f)\,\mathrm{cont}\,(g)\,\mathrm{cont}\,(f_1g_1)$$

ce qui nous ramène à prouver que $\mathrm{cont}\,(fg) = 1$ lorsque $\mathrm{cont}\,(f) = \mathrm{cont}\,(g) = 1$, ce que nous supposerons désormais. Ecrivons :

$$\begin{aligned} f &= a_0 + a_1X + \ldots + a_mX^m && \text{avec } a_i \in A,\ \mathrm{pgcd}\,(a_0, \ldots, a_m) = 1 \\ g &= b_0 + b_1X + \ldots + b_nX^n && \text{avec } b_j \in A,\ \mathrm{pgcd}\,(b_0, \ldots, b_n) = 1 \\ fg &= c_0 + c_1X + \ldots + c_{m+n}X^{m+n} && c_k = \sum_{i+j=k} a_ib_j \end{aligned}$$

Clairement, $fg \in A[X]$; il faut donc prouver que les c_k sont premiers entre eux dans leur ensemble.

Sinon, il existe $p \in P$ divisant tous les c_k. Soit i_0 le plus petit indice i tel que p ne divise pas a_i. Alors p divise $\sum_{i=0}^{i_0-1} a_ib_{i_0-i} = c_{i_0} - a_{i_0}b_0$, et comme p divise c_{i_0} par

hypothèse, p divise $a_{i_0}b_0$; mais p ne divise pas a_{i_0}, donc d'après le lemme d'Euclide il doit diviser b_0.

Regardons maintenant $c_{i_0+1} = \sum_{i+j=i_0+1} a_i b_j$. Comme précédemment, p divise les $i_0 - 1$ premiers termes, et aussi le dernier puisque p divise b_0 ; comme il divise aussi la somme, on voit donc que p divise $a_{i_0}b_1$, et on en déduit que p divise b_1. Poursuivant ainsi de proche en proche avec les c_{i_0+j}, $0 \leq j \leq n$, on voit que p divise tous les b_j, ce qui est absurde puisque les b_j ont été supposés premiers entre eux dans leur ensemble.

5.5.10 Lemme. — *Pour tout anneau intègre A, on a $A[X]^\times = A^\times$.*

Démonstration. — Exercice.

5.5.11 Proposition. — *Si A est factoriel, les irréductibles de $A[X]$ sont :*
(a) *les éléments irréductibles de A ;*
(b) *les éléments irréductibles de $K[X]$ de contenu* 1.

Démonstration. — (a) Soit $c \in A^\bullet$, considéré comme polynôme de degré zéro. Alors si $c = fg$ est une factorisation de c dans $A[X]$, on a $\deg(c) = 0 = \deg(f) + \deg(g)$, donc $\deg(f) = \deg(g) = 0$, et $f = a$ et $g = b$ appartiennent en fait à $A^\bullet$. Comme de plus $A[X]^\times = A^\times$ d'après le lemme précédent, les factorisations non-triviales de c dans A ou dans $A[X]$ sont les mêmes ; donc c est irréductible dans $A[X]$ si et seulement si il l'est dans A.
(b) Soit maintenant $h \in A[X]^\bullet$ de degré > 0, et supposons h irréductible. En écrivant $h = \mathrm{cont}\,(h)(h/\mathrm{cont}\,(h))$, on voit que $\mathrm{cont}\,(h)$ doit être inversible, ce qui n'est possible que si $\mathrm{cont}\,(h) = 1$. Si on avait une écriture $h = fg$ dans $K[X]$, avec $\deg(f) > 0$, $\deg(g) > 0$, on aurait $\mathrm{cont}\,(f)\mathrm{cont}\,(g) = 1$ d'après le thm. 5.5.9 ; mais alors on aurait aussi $h = f_1 g_1$ avec $f_1 = f/\mathrm{cont}\,(f)$, $g_1 = g/\mathrm{cont}\,(g)$ dans $A[X]$, ce qui est absurde. Donc h est irréductible dans $K[X]$.

Réciproquement soit $h \in K[X]$ irréductible de contenu 1. Alors $h \in A[X]$; montrons qu'il est irréductible dans $A[X]$. Si $h = fg$ dans $A[X]$, l'un des deux facteurs, disons f, doit être inversible dans $K[X]$, *i.e.* de degré zéro. Mais on a $\mathrm{cont}\,(h) = \mathrm{cont}\,(f)\,\mathrm{cont}\,(g) = 1$, donc $\mathrm{cont}\,(f)$ et $\mathrm{cont}\,(g)$, qui appartiennent à A, sont inversibles dans A ; ceci n'est possible que si $\mathrm{cont}\,(f) = \mathrm{cont}\,(g) = 1$. Donc f est un élément de A de contenu 1, c'est-à-dire un élément de $A^\times$, ce qui prouve que la décomposition $h = fg$ est triviale.

5.5.12 Théorème. — *Si A est factoriel, $A[X]$ est factoriel.*

Démonstration. — (a) Choisissons un ensemble P de représentants des classes d'association d'éléments irréductibles de A. Alors on peut choisir un ensemble Q de représentants de classes d'association d'irréductibles dans $K[X]$, en prenant pour Q l'ensemble des $h/\mathrm{cont}\,(h)$, où h parcourt l'ensemble des polynômes irréductibles unitaires dans $K[X]$. D'après la prop. 5.5.11, $P \coprod Q$ est un ensemble de repésentants des classes d'association d'éléments irréductibles de $A[X]$.

(b) Soit $f \in A[X]^\bullet$. Puisque $K[X]$ est principal, donc factoriel, f admet une unique écriture $f = c\prod_{h\in Q} h^{\beta_h}$, avec $c \in K^\times$, et $\beta_h \in \mathbf{N}$ presque tous nuls. Comme tous les $h \in Q$ sont de contenu 1, d'après le lemme de Gauss on a $\mathrm{cont}\,(f) = \mathrm{cont}\,(c) \in A$, donc

$c \in A$ et $c = u \prod_{p \in P} p^{\alpha_p}$, avec $\alpha_p \in \mathbf{N}$ presque tous nuls ; ceci prouve l'existence d'une décomposition de f en produit fini d'irréductibles dans $A[X]$.

Pour l'unicité, il suffit de remarquer que dans l'écriture

$$f = u \prod_{p \in P} p^{\alpha_p} \prod_{h \in Q} h^{\beta_h}$$

les α_p sont déterminés par la factorisation de cont (f) dans A, et les β_h par la factorisation de f dans $K[X]$.

5.5.13 Remarque. — Le théorème entraîne par exemple que l'anneau $\mathbf{Z}[X]$, qui n'est pas principal, est factoriel. Nous verrons au chap. 6 qu'en fait le théorème entraîne la factorialité de l'anneau $A[X_1, \ldots, X_n]$ pour tout anneau A ; en particulier $\mathbf{Z}[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]$, où k est un corps, sont factoriels pour tout $n \geq 1$.

Néanmoins, la factorialité reste un phénomène plutôt exceptionnel. La majorité des anneaux qui apparaissent en théorie algébrique des nombres (anneaux d'entiers de corps de nombres) et en géométrie algébrique (anneaux de fonctions de variétés algébriques affines) ne sont pas factoriels. L'étude des questions de divisibilité dans les anneaux d'entiers conduit à la splendide théorie des "facteurs premiers idéaux" (origine historique du mot "idéal"), inventée par Kummer dans ses travaux sur le théorème de Fermat.

5.6 Anneaux nœthériens

5.6.1. La notion d'anneau nœthérien est l'une des plus importantes de l'algèbre commutative, à cause de son ubiqüité—presque tous les anneaux que l'on rencontre en pratique sont noethériens—et de sa grande souplesse d'utilisation. C'est la principale source de résultats de finitude en algèbre.

Ils ont été nommés en l'honneur d'Emmy Nœther, mathématicienne allemande de la première moitié du vingtième siècle. Elle a fait partie de la grande école de Göttingen qui a été, de la fin du dix-neuvième siècle jusqu'à la montée du nazisme, le lieu où se sont forgées une grande partie des mathématiques d'aujourd'hui. Au centre de cette école se trouvait l'immense mathématicien David Hilbert ; ce sont d'ailleurs les études de Hilbert sur l'engendrement fini des algèbres d'invariants qui ont fourni les premiers exemples de raisonnements "nœthériens".

5.6.2 Définition. — On dit qu'un anneau A est *nœthérien*, si toute suite croissante d'idéaux de A est stationnaire.

Exemple. — Il résulte de la prop. 5.4.4 que tout anneau principal est nœthérien. En particulier, les anneaux $\mathbf{Z}$ et $k[X]$ sont nœthériens.

5.6.3 Proposition. — *Un anneau A est nœthérien si et seulement si tout idéal de A possède un ensemble générateur fini.*

Démonstration. — Supposons A nœthérien, et soit $\mathfrak{a}$ un idéal de A. Supposons que $\mathfrak{a}$ ne possède pas d'ensemble générateur fini. Alors en particulier $\mathfrak{a} \neq \{0\}$; soit $x_1 \neq 0$ dans $\mathfrak{a}$, et $\mathfrak{a}_1 = Ax_1$ l'idéal de A engendré par x_1. Puisque $\mathfrak{a}$ n'a pas d'ensemble générateur fini, on a $\mathfrak{a}_1 \neq \mathfrak{a}$; soit $x_2 \in \mathfrak{a}$, $x_2 \notin \mathfrak{a}_1$, et soit $\mathfrak{a}_2 = Ax_1 + Ax_2$. Poursuivant ainsi de proche en proche, on construit une suite strictement croissante $(\mathfrak{a}_n)_{n\geq 1}$ d'idéaux de A, ce qui est absurde.

Réciproquement, supposons que tout idéal de A possède un ensemble générateur fini, et soit $(\mathfrak{a}_n)$ une suite croissante d'idéaux de A. Soit $\mathfrak{a} = \cup_{n\geq 1}\mathfrak{a}_n$; alors on vérifie aisément que $\mathfrak{a}$ est encore un idéal de A. Soit $\{x_1, \ldots, x_s\}$ un ensemble générateur fini pour $\mathfrak{a}$. Alors il existe des entiers $n_1, \ldots, n_s$ tels que $x_j \in \mathfrak{a}_{n_j}$ pour $1 \leq j \leq s$; soit $n_0 = \max\{n_1, \ldots, n_s\}$. Alors $\mathfrak{a}_{n_0}$ contient $x_1, \ldots, x_s$, donc $\mathfrak{a} \subset \mathfrak{a}_{n_0}$, et comme l'inclusion contraire est évidente, $\mathfrak{a} = \mathfrak{a}_{n_0}$; mais alors $\mathfrak{a}_n = \mathfrak{a}$ pour tout $n \geq n_0$, ce qui prouve bien que la suite $(\mathfrak{a}_n)$ est stationnaire.

5.6.4. La proposition suivante est la principale raison de la grande abondance d'anneaux nœthériens en algèbre (contrairement au cas des anneaux factoriels) :

Proposition. — *Tout quotient d'un anneau nœthérien est nœthérien.*

Démonstration. — Soit A un anneau nœthérien, I un idéal de A, et $A' = A/I$. Soit $\mathfrak{a}'$ un idéal de A', et soit $\mathfrak{a} = \pi^{-1}(\mathfrak{a}')$, où $\pi : A \to A'$ est la surjection canonique. Alors $\mathfrak{a}$ est un idéal de A. D'après la prop. 5.6.3, l'idéal $\mathfrak{a}$ possède un ensemble générateur fini $x_1, \ldots, x_s$; alors $\pi(x_1), \ldots, \pi(x_s)$ est un ensemble générateur pour $\mathfrak{a}'$, et la conclusion résulte encore de la prop. 5.6.3.

5.6.5 Théorème. — (Hilbert) *Si A est nœthérien, $A[X]$ est nœthérien.*

Démonstration. — D'après la prop. 5.6.3, il suffit de prouver que tout idéal I de $A[X]$ possède un ensemble générateur fini. Pour tout $n \in \mathbf{N}$, soit $A[X]_n = A \oplus A.X \oplus \ldots \oplus A.X^n$ l'ensemble des polynômes de degré $\leq n$ dans $A[X]$, et soit I_n le groupe abélien $I \cap A[X]_n$ (en convenant que $A[X]_{-1} = \{0\}$). Pour tout $n \geq 0$, soit $\mathfrak{a}_n$ l'ensemble des coefficients dominants d'éléments de I_n, auxquels on adjoint zéro ; *i.e.* $\mathfrak{a}_n$ est l'ensemble des $a \in A$ tels qu'il existe $f \in I_n$ de la forme :

$$f = aX^n + \text{termes de plus bas degré}$$

Il est facile de voir que α_n est un idéal de A ; par exemple, si a et b sont dans $\mathfrak{a}_n$, on choisit f et g dans I_n tels que $f = aX^n + \ldots$, $g = bX^n + \ldots$, et on voit que $f+g = (a+b)X^n + \ldots$, donc $a+b \in \mathfrak{a}_n$; on vérifie de même que si $a \in \mathfrak{a}_n$ et $c \in A$, alors $ca \in \mathfrak{a}_n$. Par ailleurs la suite $(\mathfrak{a}_n)$ est *croissante* : en effet si $a \in \mathfrak{a}_n$ et $f = aX^n + \ldots$, on a $Xf = aX^{n+1} +$ termes de plus bas degré, et $Xf \in I_{n+1}$ puisque I est stable par multiplication par X, donc $a \in \mathfrak{a}_{n+1}$.

Comme A est nœthérien, la suite $\mathfrak{a}_n$ est donc stationnaire ; *i.e.* il existe un entier m tel que $\mathfrak{a}_n = \mathfrak{a}_m$ pour tout $n \geq m$. On choisit maintenant des ensembles générateurs des $\mathfrak{a}_j$, $1 \leq j \leq m$, de la façon suivante. On part d'un ensemble générateur $\{a_1, \ldots, a_{s_0}\}$ pour $\mathfrak{a}_0$, que l'on complète si nécessaire par $\{a_{s_0+1}, \ldots, a_{s_1}\}$ en un ensemble générateur pour $\mathfrak{a}_1$, puis par $\{a_{s_1+1}, \ldots, a_{s_2}\}$ en un ensemble générateur pour $\mathfrak{a}_2$, et ainsi de suite ;

on aboutit donc à un ensemble générateur $\{a_1, \ldots, a_{s_m}\}$ de $\mathfrak{a}_m$ dont on peut extraire un ensemble générateur pour chaque $\mathfrak{a}_j$, $j \leq m$ (on pose simplement $s_j = s_{j-1}$ s'il n'y a pas lieu d'ajouter des générateurs à l'étape j, avec $s_{-1} = 0$.)

Pour chaque $i \in \{1, \ldots, s_m\}$ tel que $s_{j-1} < i \leq s_j$, on choisit $f_i \in I_j$ tel que $f_i = a_i X^j +$ termes de plus bas degré. Montrons alors que $\{f_1, \ldots, f_{s_m}\}$ est un ensemble générateur pour l'idéal I. Pour cela, soit $n \in \mathbf{N}$, et montrons par récurrence sur n que tout $f \in I_n$ appartient à l'idéal de $A[X]$ engendré par $f_1, \ldots, f_{s_m}$. Si $n = 0$ c'est facile : on a alors directement $f \in \mathfrak{a}_0$, donc il existe $a_1, \ldots, a_{s_0} \in A$ tels que $f = a_1 f_1 + \ldots + a_{s_0} f_{s_0}$.

Supposons maintenant $n > 0$, et écrivons $f = aX^n +$ termes de plus bas degré, avec $a \in \mathfrak{a}_n$. Si $n < m$, on choisit $c_1, \ldots, c_{s_n} \in A$ tels que $a = c_1 s_1 + \ldots + c_{s_n} a_{s_n}$; si $n \geq m$, on écrit de même $a = c_1 s_1 + \ldots + c_{s_m} a_{s_m}$. Alors et

$$f - \sum_i c_i X^{n - \deg(f_i)} f_i$$

appartient à I_{n-1}, puisqu'on a retranché un élément de I_n et que le coefficient de X^n dans la différence est nul ; on conclut donc par l'hypothèse de récurrence.

5.6.6 Remarque. — Nous reporterons au chapitre 6 les applications qui révèleront toute la puissance de ce théorème : nous y verrons par exemple que tout anneau engendré par un nombre fini d'éléments, ou encore toute algèbre de type fini sur un corps k, sont nœthériens.

5.6.7. Bien qu'il ne soit pas vrai, loin s'en faut, que tout anneau nœthérien soit factoriel, il y a quand même un lien entre les deux notions : en effet, dans un anneau nœthérien on a toujours l'*existence* d'une décomposition de tout élément en produit fini d'irréductibles :

Proposition. — *Soit A un anneau nœthérien intègre. Alors tout élément de A possède une décomposition en produit fini d'irréductibles.*

Démonstration. — La démonstration d'existence est exactement la même que celle du thm. 5.4.5 ; en fait, on a même seulement besoin de savoir que toute suite croissante d'idéaux *principaux* de A est stationnaire.

5.6.8 Corollaire. — *Un anneau nœthérien intègre est factoriel si et seulement si tout $p \in A^\bullet$ irréductible vérifie les conditions du lemme 5.5.2.*

Démonstration. — On sait déjà que la condition est nécessaire. Pour la réciproque, il suffit de remarquer que dans la démonstration du thm. 5.4.4, la seule propriété qui intervient est le lemme d'Euclide.

5.6.9 Exemple. — Voici un exemple simple d'anneau nœthérien intègre non factoriel. Soit A la sous-algèbre de $\mathbf{C}[X]$ engendrée par X^2 et X^3. On vérifie aussitôt que A est le sous-espace vectoriel de $\mathbf{C}[X]$ de base $(X^j)_{j \neq 1}$; la nœthérianité provient du fait que A est une $\mathbf{C}$-algèbre de type fini (comme nous l'avons dit plus haut, ceci sera vu au chapitre 6.) On vérifie aussi immédiatement que $A^\times = \mathbf{C}[X]^\times = \mathbf{C}^\times$; donc la relation

d'association dans A est la même que dans $\mathbf{C}[X]$. L'élément $p = X^2$ est irréductible dans A ; en effet, à association près son seul diviseur non-trivial dans $\mathbf{C}[X]$ est X, qui n'appartient pas à A. Soit $q = X^3$; alors p divise $q^2 = X^6 = p^3$, mais clairement p ne divise pas q.