IV. ANNEAUX FACTORIELS, PRINCIPAUX, EUCLIDIENS

SEMAINE DU 1ER OCTOBRE

(1) Sauf mention du contraire, « anneau » signifie « anneau commutatif ».

9. Anneaux factoriels

9.1. Une motivation. — Le théorème géométrique suivant (tiré de [**Fu**, § I.6]) est un très bon exemple d'application des notions d'anneau factoriel ou principal, du théorème de transfert de Gauss, et du théorème de Bézout, qu'on va voir dans ce chapitre.

On rappelle (cf. 1.4) qu'une *sous-variété algébrique fermée* de $\mathbb{C}^n$ est l'ensemble des zéros communs d'un nombre fini de polynômes à n variables $\mathrm{F}_1, \ldots, \mathrm{F}_p \in \mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. On dit qu'une telle variété algébrique X est **irréductible** si elle est non vide et n'est pas réunion de deux sous-variétés algébriques fermées strictement plus petites.

Théorème 9.1. — *Soit* V *une sous-variété algébrique fermée irréductible de* $\mathbb{C}^2$. *Alors,* $\mathrm{V} = \mathbb{C}^2$, *ou bien* V *est formée d'un seul point* $p_0 = (x_0, y_0)$, *ou bien* $\mathrm{V} = \mathscr{V}(\mathrm{F})$, *où* $\mathrm{F} \in \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ *est un polynôme irréductible.*

Ce théorème sera démontré dans le paragraphe 9.10.

9.2. Anneaux intègres. —

Définition 9.2. — Soient A un anneau et $a \in \mathrm{A}$. On dit que a est un *diviseur de zéro* si $a \neq 0$ et s'il existe $b \neq 0$ tel que $ab = 0$.

On rappelle (cf. 3.6) que A est dit **intègre** s'il ne possède pas de diviseurs de zéros.

(1) Les chapitres I à III ont été faits pendant les semaines 1–3 ; les exemples de la section I.2 ont été ou seront traités en TD.

9.3. Divisibilité, éléments irréductibles. — Soit A un anneau commutatif. L'ensemble des éléments de $\mathrm{A} \setminus \{0\}$ inversibles pour la multiplication :

$$\{u \in \mathrm{A} \setminus \{0\} \mid \exists\, v \in \mathrm{A} \setminus \{0\} \ \text{ tel que } \ uv = 1\}$$

forme un groupe ; on le note $\mathrm{A}^\times$ ou $\mathbf{U}$. (On dit parfois que les éléments inversibles sont les *unités* de A, d'où la notation $\mathbf{U}$.)

Désormais, on suppose A **intègre**.

Définition 9.3. — On dit que $a, a' \in \mathrm{A}$ sont **associés** s'il existe un élément inversible $u \in \mathbf{U}$ tel que $a' = ua$.

Lemme 9.4. — *Soient* A *intègre et* $a, b \in \mathrm{A}$. *Les conditions suivantes sont équivalentes :*

1) *a divise b et b divise a ;*

2) *a et b engendrent le même idéal ;*

3) *a et b sont associés.*

Démonstration. — Il est clair que 3) $\Rightarrow$ 2) $\Leftrightarrow$ 1). Réciproquement, si $(a) = (b)$, il existe $\alpha, \beta \in \mathrm{A}$ tels que $b = \alpha a$ et $a = \beta b$. Alors, $b = \alpha\beta b$ et comme A est intègre il vient $\alpha\beta = 1$. Donc α et β sont inversibles. Ceci prouve le lemme. □

Définition 9.5. — Un élément $p \in \mathrm{A} \setminus \{0\}$ est dit **irréductible** s'il est non inversible, et vérifie la propriété suivante : si $p = ab$, avec $a, b \in \mathrm{A}$, alors a ou b est inversible.

Ceci équivaut à dire que $p \notin \mathbf{U}$ et que ses seuls diviseurs sont ses associés, et les inversibles.

Remarque 9.6. — Voir la section 2 pour des exemples concrets d'éléments inversibles ou irréductibles, et pour le fait que l'on a besoin de prendre en compte les éléments inversibles pour pouvoir travailler commodément avec les éléments irréductibles.

Définition 9.7. — Un idéal I de A est **principal** s'il peut être engendré par un seul élément, c.-à-d., s'il existe $a \in \mathrm{A}$ tel que $\mathrm{I} = (a)$.

Un tel a s'appelle un *générateur de* I, et d'après le lemme 9.4, a est unique à un élément inversible près.

Proposition 9.8. — *Soient* A *intègre et* I *un idéal principal non nul et* $\neq \mathrm{A}$. *Les conditions suivantes sont équivalentes :*

1) I *est engendré par un élément irréductible p ;*

2) I *est un élément maximal de l'ensemble des idéaux principaux* $\neq \mathrm{A}$ *;*

3) *tout générateur p de* I *est irréductible.*

Démonstration. — Supposons p irréductible et (p) contenu dans un idéal principal $(b) \neq \mathrm{A}$. Alors b n'est pas inversible, et il existe $a \in \mathrm{A}$ tel que $p = ab$. Comme p est irréductible, ceci entraîne que a est inversible, d'où $(b) = (p)$. Ceci prouve l'implication 1) $\Rightarrow$ 2).

Montrons que 2) $\Rightarrow$ 3). Supposons (p) maximal parmi les idéaux principaux $\neq \mathrm{A}$ et supposons $p = ab$. Alors $(p) \subseteq (a)$ et deux cas sont possibles.

Si $(a) = \mathrm{A}$, alors a est inversible et b associé à p. D'autre part, si $(a) = (p)$, alors $p = ua$, avec $u \in \mathrm{A}^\times$ (d'après le lemme), et donc $ab = p = ua$, d'où $b = u$ puisque A est intègre. Ceci montre que p est irréductible. L'implication 2) $\Rightarrow$ 3) est démontrée.

Enfin, 3) $\Rightarrow$ 1) est clair. La proposition est démontrée. □

***Théorème 9.9* (Existence d'une décomposition en facteurs irréductibles)**

Soit A *un anneau commutatif intègre* **noethérien**. *Alors, tout élément non nul et non inversible de* A *est un produit fini d'éléments irréductibles.*
(*En particulier, si* A *n'est pas un corps, il existe des éléments irréductibles.*)

Démonstration. — Si A est un corps, c.-à-d., si tout élément de $\mathrm{A} \setminus \{0\}$ est inversible, il n'y a rien à montrer. Sinon, considérons l'ensemble d'idéaux suivant :

$\mathscr{I} := \{(a) \mid a \in \mathrm{A} \setminus \{0\}$ est non inversible et n'est pas un produit fini d'éléments irréductibles$\}$
La proposition sera démontrée si on montre que cet ensemble $\mathscr{I}$ est vide.

Supposons $\mathscr{I}$ non vide. Il admet alors un élément maximal (a), où $a \in \mathrm{A} \setminus \{0\}$ n'est ni inversible ni un produit fini d'éléments irréductibles. En particulier, a n'est pas irréductible, donc il existe b, c dans A, tous deux non inversibles, tels que $a = bc$. Donc

$$(a) \subseteq (b), \qquad (a) \subseteq (c),$$

et chacune de ces inclusions est stricte. En effet, si on avait $(a) = (b)$, il existerait $d \in \mathrm{A}$ tel que $b = ad$, d'où $a = bc = adc$ et $1 = dc$ (car A est intègre), et c serait inversible, une contradiction. Donc l'inclusion $(a) \subset (b)$ est stricte, et il en est de même de $(a) \subset (c)$.

Donc, comme (a) est un élément maximal de $\mathscr{I}$, et comme b et c sont non inversibles, alors b et c sont chacun un produit fini d'éléments irréductibles, et il en est de même de leur produit $bc = a$! Ceci contredit l'hypothèse $(a) \in \mathscr{I}$, et cette contradiction montre que $\mathscr{I} = \varnothing$. Le théorème est démontré. □

Remarque 9.10. — Voir la remarque 2.43 pour un exemple d'anneau (le sous-anneau $\mathscr{A} \subset \mathbb{C}$ des entiers algébriques) dans lequel la décomposition en facteurs irréductibles n'existe pas. En fait, $\mathscr{A}$ ne possède *aucun* élément irréductible !

Remarque 9.11. — 1) Lorsqu'elle existe, on n'a pas unicité de la décomposition en facteurs irréductibles en général. Voici deux exemples :

a) Dans $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z}[\mathrm{X}]/(\mathrm{X}^2+5)$, on a

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

et l'on peut montrer que $2+i\sqrt{5}$, $2-i\sqrt{5}$ et 3 sont irréductibles mais deux à deux non associés ; voir [**Pe1**, p.II.8] et le paragraphe 9.11 plus loin.

b) Dans $\mathrm{A} = \mathbb{C}[\mathrm{X},\mathrm{Y}]/(\mathrm{X}^2-\mathrm{Y}^3)$, notons x et y les images de X et Y. On a $x^2 = y^3$, et l'on peut montrer que x et y sont irréductibles et non associés.

2) Dans les deux cas précédents, il n'est pas si facile de montrer que les éléments en question sont irréductibles et non associés. Ceci peut se faire, par exemple, en considérant la norme associée à une extension quadratique, et en étudiant les factorisations possibles de la norme $\mathrm{N}(\alpha)$ d'un élément α. Voir [**Sa**, § II.5 & IV.5] et le paragraphe 9.11 plus loin.

3) Les anneaux intègres pour lesquels la décomposition en facteurs irréductibles existe et est unique (aux inversibles près), sont appelés anneaux **factoriels** ; voir plus bas.

Définition 9.12. — Soient $a, b \in \mathrm{A}$. On dit que a et b sont **premiers entre eux** ou **sans facteur commun**, si tout diviseur commun à a et b est inversible. Ceci équivaut à dire que : A *est le seul idéal principal contenant* a *et* b.

Lemme 9.13. — *Soit* $p \in \mathrm{A}$ *irréductible et* $a \in \mathrm{A}\setminus\{0\}$. *Si* $a \notin (p)$ *alors* a *et* p *sont sans facteur commun.*

Démonstration. — Supposons que $a \notin (p)$ et qu'il existe un élément b non inversible divisant a et p. Alors, b est associé à p et il en résulte que p divise a, contredisant l'hypothèse $a \notin (p)$. Ceci prouve le lemme. □

Lemme 9.14. — *Soient* A *un anneau intègre et* p *un élément non nul de* A. *Si l'idéal* (p) *est premier, alors* p *est irréductible.*

Démonstration. — L'hypothèse que (p) soit un idéal premier, donc $\neq \mathrm{A}$, entraîne que p est non inversible.

Soient $a, b \in \mathrm{A}$ tels que $p = ab$. Comme (p) est premier, ceci entraîne, disons, que $a \in (p)$, d'où $a = p\alpha$, avec $\alpha \in \mathrm{A}$. Alors $p = p\alpha b$, et comme A est intègre il vient $\alpha b = 1$. Donc b est inversible. Ceci montre que p est irréductible. □

Notation 9.15. — On écrira $a \mid b$ (resp., $a \nmid b$) pour signifier que a divise (resp., ne divise pas) b.

9.4. Anneaux factoriels, lemmes d'Euclide et Gauss. —

Définition 9.16. — Soit A un anneau commutatif. On dit que A est **factoriel** s'il est **intègre** et vérifie les deux conditions suivantes : **existence** (E) et **unicité** (U) de la **décomposition en facteurs irréductibles**, c.-à-d.,

(E) Tout $a \in \mathrm{A} \setminus \{0\}$, non inversible, s'écrit

$$a = p_1 \cdots p_r,$$

où $r \geqslant 1$ et les p_i sont des éléments irréductibles de A ;

(U) La décomposition précédente est *unique* au sens suivant : si l'on a deux décompositions

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

où les p_i et les q_j sont irréductibles, alors $s = r$ et il existe une permutation $\sigma \in \mathrm{S}_r$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour tout $i = 1, \ldots, r$. C.-à-d., de façon plus concise, la décomposition est unique à l'ordre des termes et aux inversibles près.

Remarque 9.17. — On rappelle que (E) est satisfaite si A est noethérien (Proposition 9.9). Mais il y a aussi des exemples d'anneaux factoriels qui ne sont pas noethériens, c.-à-d., la décomposition en facteurs irréductibles peut exister sans que A soit nécessairement noethérien. Par exemple, on peut montrer que l'anneau de polynômes $\mathbb{C}[\mathrm{X}_1, \mathrm{X}_2, \ldots]$ en une infinité de variables (qui n'est pas noethérien d'après 8.9), est factoriel.

Proposition 9.18. — *Soit* A *un anneau commutatif intègre vérifiant* (E). *Les propriétés suivantes sont équivalentes.*

1) A *vérifie* (U).

2) *Pour tout élément irréductible* $p \in \mathrm{A}$, *l'idéal* (p) *est premier.*

3) A *vérifie le* **Lemme d'Euclide**, *c.-à-d., si* $p \in \mathrm{A}$ *est irréductible et divise un produit* $ab \neq 0$, *il divise* a *ou* b.

4) A *vérifie le* **Lemme de Gauss**, *c.-à-d., pour tout* $a, b, c \in \mathrm{A} \setminus \{0\}$, *si* a *divise* bc *et si* a, b *sont sans facteur commun, alors* a *divise* c.

Démonstration. — Il est clair que 2) et 3) sont équivalents. L'implication 4) $\Rightarrow$ 3) est facile. En effet, soit p irréductible divisant un produit $ab \neq 0$. Si $p \nmid a$ alors, d'après le lemme 9.13, a et p sont sans facteur commun, et l'hypothèse 4) donne alors que p divise b.

Montrons que 2) $\Rightarrow$ (U). Plus précisément, montrons que si l'on a une égalité

$$(*) \qquad p_1 \cdots p_m = u q_1 \cdots q_n,$$

où u est inversible et les p_i et q_j sont irréductibles, alors $m = n$ et il existe une permutation $\sigma \in \mathrm{S}_n$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour $i = 1, \ldots, n$. On peut supposer $m \leqslant n$.

Si $m = 0$, le terme de gauche vaut 1 et ceci entraîne $n = 0$, car sinon q_1 serait inversible, ce qui n'est pas le cas pour un élément irréductible. Supposons $m > 0$ et le résultat établi pour $m - 1$.

Il résulte de $(*)$ que l'on a

$$\overline{q}_1 \cdots \overline{q}_n = 0$$

dans l'anneau $\mathrm{A}/(p_1)$; comme ce dernier est intègre, par hypothèse, on obtient que p_1 divise l'un des q_i, donc lui est associé (puisque q_i est irréductible). Donc, quitte à changer la numérotation des q_j, on peut supposer que $p_1 = vq_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(*)$ l'égalité

$$p_2 \cdots p_m = uvq_2 \cdots q_n,$$

et le résultat cherché découle alors de l'hypothèse de récurrence. Ceci prouve que 2) $\Rightarrow$ (U).

Montrons maintenant que 1) $\Rightarrow$ 4). Supposons A factoriel et soient $a, b, c, d \in \mathrm{A} \setminus \{0\}$ tels que $ad = bc$, avec a et b sans facteur commun. Montrons que a divise c. On a des égalités

$$\begin{array}{ll} a = \alpha p_1 \cdots p_n, & d = \delta p'_1 \cdots p'_r, \\ b = \beta q_1 \cdots q_s, & c = \gamma q'_1 \cdots q'_t, \end{array}$$

avec $\alpha, \beta, \gamma, \delta$ inversibles, $n, r, s, t \geqslant 0$, et les p_i, p'_j, q_k et q'_ℓ irréductibles. On a donc une égalité

$$(**) \qquad up_1 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_1 \cdots q'_t,$$

avec u inversible. Montrons, par récurrence sur n, que ceci entraîne que $a \mid c$. Si $n = 0$, alors a est inversible et l'assertion est claire. Supposons $n \geqslant 1$ et le résultat établi pour $n - 1$.

Comme a et b sont sans facteur commun, p_1 ne peut être associé à l'un des q_j ; l'hypothèse (U) entraîne donc que p_1 est associé à un q'_k. Quitte à renuméroter les q'_k, on peut supposer que $p_1 = vq'_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(**)$ l'égalité

$$uvp_2 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_2 \cdots q'_t,$$

et le résultat cherché découle alors de l'hypothèse de récurrence. Ceci prouve que si A vérifie (E) et (U), il vérifie 4). Ceci achève la démonstration de la proposition. □

Remarque 9.19. — a) En procédant comme ci-dessus, on peut démontrer directement l'implication : A factoriel $\Rightarrow$ 3).

b) Ce qu'on appelle Lemme d'Euclide, resp. de Gauss, est l'assertion que si A est factoriel, il vérifie la condition 3), resp. 4). Pour mémoire, énonçons ci-dessous ces deux lemmes sous leur forme usuelle.

Proposition 9.20. — *Supposons* A **factoriel** *et soient* $a, b, c \in \mathrm{A} \setminus \{0\}$ *tels que* a *divise* bc*. Alors :*

(Lemme d'Euclide) *Si* a *est irréductible, il divise* b *ou* c*.*

(Lemme de Gauss) *Si* a *est sans facteur commun avec* b*, il divise* c*.*

Remarque 9.21. — Le Lemme de Gauss est **équivalent** à l'assertion $(*)$ ci-dessous :

$(*)$ Si a et b sont sans facteur commun et divisent x, alors ab divise x.

En effet, soient $a, b \in \mathrm{A}$ sans facteur commun. Supposons que A vérifie le Lemme de Gauss et que a, b divisent x. Alors x égale bc et est divisible par a. Comme a et b sont premiers entre eux, a divise c, donc $c = ad$ et $x = bad$ est divisible par ab.

Réciproquement, supposons $(*)$ vérifiée et $x = bc$ divisible par a. Alors x est divisible par ab, d'où $x = abd$, et comme A est intègre il vient $c = ad$, donc a divise c.

Corollaire 9.22 **(Lemme de Gauss)**. — *Soit* A *factoriel, soient* $a_1, \ldots, a_n \in \mathrm{A}$*, deux à deux sans facteur commun, et soit* b *un multiple commun aux* a_i*. Alors* b *est divisible par* $a_1 \cdots a_n$*.*

Démonstration. — On procède par récurrence sur n. Si $n = 2$, c'est la propriété $(*)$. Supposons $n \geqslant 3$ et le résultat établi pour $n - 1$. Par hypothèse de récurrence, il existe $c \in \mathrm{A}$ tel que

$$b = a_2 \cdots a_n c.$$

Alors, par application répétée du Lemme de Gauss, on obtient que a_1 divise c. Ceci prouve le corollaire. □

9.5. Anneaux principaux et anneaux euclidiens. —

Définition 9.23. — Soit A un anneau commutatif. On dit qu'il est **principal** s'il est **intègre** et si tout idéal de A est engendré par un élément.

Théorème 9.24 **(Théorème de Bezout)**. — *Soit* A *un anneau principal et soient* $x, y \in \mathrm{A}$ *sans facteur commun. Il existe* $a, b \in \mathrm{A}$ *tels que*

$$(*) \qquad 1 = ax + by.$$

Démonstration. — Soit $\mathrm{I} = \mathrm{A}x + \mathrm{A}y$. Comme A est principal, I est engendré par un élément d, de la forme $d = ax + by$. D'autre part, comme (d) contient x et y, alors d est un diviseur commun à x et y. L'hypothèse entraîne que d est inversible, d'où $\mathrm{A}x + \mathrm{A}y = \mathrm{A}$. Le lemme en découle. □

Corollaire 9.25. — *Soit* A *principal et soit* $p \in \mathrm{A}$ *irréductible. Alors* (p) *est maximal, donc premier.*

Démonstration. — Soit $a \in \mathrm{A}$ non divisible par p. Alors p et a sont sans facteur commun donc, d'après le théorème de Bezout, il existe $u, v \in \mathrm{A}$ tels que $up + vb = 1$. Donc $(p) + \mathrm{A}a = \mathrm{A}$, pour tout $a \notin (p)$. Ceci montre que (p) est maximal. □

Théorème 9.26. — *Soit* A *un anneau principal. Alors :*

1) A *est noethérien et factoriel.*

2) *Tout idéal premier non nul de* A *est engendré par un élément irréductible, et est un idéal maximal.*

Démonstration. — Par hypothèse, A est intègre. Comme tout idéal de A est engendré par un élément, A est noethérien. En particulier, il vérifie la condition (E), d'après la proposition 9.9.

Soit p un élément irréductible de A. D'après le corollaire précédent, l'idéal (p) est maximal, donc a fortiori premier. D'après la proposition 9.18, ceci montre que A est factoriel.

Enfin, soit (a) un idéal premier non nul de A. D'après le lemme 9.14, a est irréductible, et l'on vient de voir que dans ce cas (a) est un idéal maximal. Le théorème est démontré. □

Des exemples importants d'anneaux principaux sont fournis par les anneaux euclidiens, introduits ci-dessous.

Définition 9.27. — Soit A un anneau commutatif. On dit que A est **euclidien** s'il est **intègre** et s'il existe une application $\rho : \mathrm{A} \setminus \{0\} \to \mathbb{N}$ vérifiant la propriété suivante : pour tout $a, b \in \mathrm{A} \setminus \{0\}$, il existe $q, r \in \mathrm{A}$ tels que

$$a = bq + r, \quad \text{et } r = 0 \text{ ou bien } \rho(r) < \rho(b).$$

Proposition 9.28. — *Tout anneau euclidien* A *est principal. Plus précisément, soit* I *un idéal non nul de* A *et soit* $a \in \mathrm{I}$ *tel que* $\rho(a)$ *soit minimal. Alors* $\mathrm{I} = (a)$.

Démonstration. — Soit I un idéal non nul de A. Alors l'ensemble des $\rho(\mathrm{P})$, pour $\mathrm{P} \in \mathrm{I} \setminus \{0\}$ est un sous-ensemble non vide de $\mathbb{N}$ donc admet un plus petit élément d. Soit $\mathrm{P}_0 \in \mathrm{I}$ tel que $\rho(\mathrm{P}_0) = d$ et soit $\mathrm{P} \in \mathrm{I}$ arbitraire. Comme A est euclidien, il existe $\mathrm{Q}, \mathrm{R} \in \mathrm{A}$ tels que

$$\mathrm{P} = \mathrm{P}_0\mathrm{Q} + \mathrm{R},$$

et $\mathrm{R} = 0$ ou bien $\rho(\mathrm{R}) < \rho(\mathrm{P}_0) = d$. Or $\mathrm{R} = \mathrm{P} - \mathrm{P}_0\mathrm{Q}$ appartient à I, donc la seconde possibilité est exclue par minimalité de d. Donc $\mathrm{R} = 0$ et $\mathrm{P} = \mathrm{P}_0\mathrm{Q}$. Ceci montre que I est engendré par P_0. La proposition est démontrée. □

Exemple 9.29. — L'anneau $\mathbb{Z}$, muni de la division euclidienne usuelle, est euclidien (l'application $\rho : \mathbb{Z} \to \mathbb{N}$ étant la valeur absolue). On retrouve ainsi que, pour tout idéal $\mathrm{I} \neq (0)$ de $\mathbb{Z}$, on a $\mathrm{I} = (d)$ où d est le plus petit entier > 0 contenu dans I.

Théorème 9.30 **(Division euclidienne dans** $k[\mathrm{X}]$**).** — *Soit k un corps.*

1) $k[\mathrm{X}]$ *est intègre et, pour tout* $\mathrm{U} \in k[\mathrm{X}] \setminus \{0\}$*, on peut faire la division euclidienne par* U.

2) *Tout idéal de $k[\mathrm{X}]$ est* **principal**, *c.-à-d., engendré par un élément. Plus précisément, soit* I *un idéal non nul de $k[\mathrm{X}]$ et soit* $\mathrm{U} \in \mathrm{I}$ *un polynôme de degré minimal. Alors* $\mathrm{I} = (\mathrm{U})$*. En particulier, $k[\mathrm{X}]$ est noethérien.*

3) $k[\mathrm{X}]$ *est un anneau factoriel.*

Démonstration. — Le point 1) résulte de la proposition 7.2 et du théorème 7.3. Les points 2) et 3) en découlent, d'après la proposition 9.28 et le théorème 9.26. □

9.6. PPCM et PGCD dans un anneau factoriel. —

Remarque 9.31. — Soit A un anneau commutatif et soient $a_1, \ldots, a_n \in \mathrm{A}$. L'ensemble des multiples communs aux a_i est égal à l'idéal

$$(a_1) \cap \cdots \cap (a_n).$$

D'autre part, un élément d de A divise tous les a_i si, et seulement si, (d) contient l'idéal $(a_1, \ldots, a_n)$ engendré par les a_i.

Définition et proposition 9.32. — *Soit* A **factoriel** *et soient* $a_1, \ldots, a_n \in \mathrm{A} \setminus \{0\}$.

1) *L'idéal* $\mathrm{I} := (a_1) \cap \cdots \cap (a_n)$ *est principal. Soit* M *un générateur de cet idéal* (M *est unique à multiplication par un inversible près, c.-à-d., tout autre générateur de* I *est associé à* M) *; alors* M *est un multiple commun aux a_i, qui divise tout multiple commun des a_i. On dit que* M *est un* **PPCM** *(plus petit commun multiple) des a_i. Par abus de notation, on écrira* $\mathrm{M} = \mathrm{ppcm}(a_1, \ldots, a_n)$.

2) *L'ensemble des idéaux principaux contenant $(a_1, \ldots, a_n)$ possède un unique élément minimal* J. *Tout générateur d de* J *est un diviseur commun aux a_i, et si f est un autre diviseur commun aux a_i, alors (f) contient* $\mathrm{J} = (d)$ *et donc f divise d. Donc, d est un diviseur commun aux a_i, qui est divisible par tout diviseur commun des a_i. Par conséquent, tout élément associé à d est un* **PGCD** *(plus grand commun diviseur) des a_i. Par abus de notation, on écrira* $d = \mathrm{pgcd}(a_1, \ldots, a_n)$.

De façon plus concrète, en décomposant chaque a_i en produits d'irréductibles, on peut écrire :

$$(\dagger) \qquad \begin{cases} a_1 = u_1\, p_1^{c_{11}} \cdots p_r^{c_{1r}}, \\ \vdots \qquad\qquad \vdots \\ a_n = u_n\, p_1^{c_{n1}} \cdots p_r^{c_{nr}}, \end{cases}$$

où $p_1, \ldots, p_r \in \mathrm{A}$ sont des éléments irréductibles deux à deux non associés, $u_1, \ldots, u_n \in \mathrm{A}$ sont inversibles, et $c_{ij} \in \mathbb{N}$. Pour $j = 1, \ldots, r$, posons

$$\mathrm{M}_j = \max\{c_{1j}, \ldots, c_{nj}\}, \quad m_j = \min\{c_{1j}, \ldots, c_{nj}\},$$

et soient

$$\mathrm{M} = p_1^{\mathrm{M}_1} \cdots p_r^{\mathrm{M}_r}, \qquad d = p_1^{m_1} \cdots p_r^{m_r}.$$

Alors M *est un générateur de* I*, donc un PPCM des a_i. D'autre part, tout diviseur commun aux a_i divise d, et donc d est un PGCD des a_i.*

Démonstration. — Soit $b \in \mathrm{A}$ un multiple commun aux a_i. Dans la décomposition (†), fixons un indice $j \in \{1, \ldots, r\}$. Alors, b est divisible par $p_j^{c_{ij}}$, pour $i = 1, \ldots, n$, donc par $p_j^{\mathrm{M}_j}$. Comme les $p_j^{\mathrm{M}_j}$ sont deux à deux sans facteur commun, il résulte du corollaire 9.22 que b est divisible par

$$\mathrm{M} := p_1^{\mathrm{M}_1} \cdots p_r^{\mathrm{M}_r}.$$

Ceci montre que M engendre l'idéal $(a_1) \cap \cdots \cap (a_n)$ et est donc un PPCM des a_i.

D'autre part, comme $a_i = u_i\, p_1^{c_{i1}} \cdots p_r^{c_{ir}}$, il résulte de l'unicité de la décomposition en facteurs irréductibles que tout diviseur de a_i est de la forme

$$a_i' = v_i\, p_1^{c'_{i1}} \cdots p_r^{c'_{ir}},$$

où v_i est inversible et $c'_{ij} \leqslant c_{ij}$ pour $j = 1, \ldots, r$. Donc, si f est un diviseur commun aux a_i, alors

$$f = v\, p_1^{c'_1} \cdots p_r^{c'_r},$$

où v est inversible et où, pour chaque $j = 1, \ldots, r$, c'_j est inférieur à c_{ij}, pour $i = 1, \ldots, n$, donc à m_j. Par conséquent, f divise

$$d = p_1^{m_1} \cdots p_r^{m_r}.$$

Ceci montre que d est un PGCD des a_i. La proposition est démontrée. □

Définition 9.33. — Soit A factoriel. On dit que $a_1, \ldots, a_n \in \mathrm{A}$ sont **premiers entre eux** *dans leur ensemble* s'ils n'ont pas de diviseur commun non inversible. Ceci équivaut à dire que leur PGCD est 1.

Remarque 9.34. — Si $a_1, \ldots, a_n$ sont *premiers entre eux deux à deux*, ils sont évidemment premiers entre eux dans leur ensemble, mais la seconde condition est strictement plus faible que la première : par exemple, les entiers $4, 6, 15$ sont premiers entre eux dans leur ensemble, mais pas deux à deux !

9.7. Corps des fractions d'un anneau intègre. — Soit A un anneau intègre. Rappelons, ou expliquons, la construction du corps des fractions de A. On considère l'ensemble C des couples (a, s), où $a \in \mathrm{A}$ et $s \in \mathrm{A} \setminus \{0\}$. De façon informelle, on pense au couple (a, s) comme à un représentant de la fraction a/s. Tenant compte de l'égalité $a/s = b/t$ si $at = bs$, on considère sur C la relation définie par

$$(a, s) \sim (b, t) \Leftrightarrow at = bs.$$

Cette relation est clairement réflexive et symétrique ; elle est aussi transitive car si $(a, s) \sim (b, t) \sim (c, u)$, alors $at = bs$ et $bu = ct$ d'où $atu = bsu = cts$, soit

$$(*) \qquad (au - cs)t = 0,$$

et comme A est intègre et $t \neq 0$, il vient $au = cs$, soit $(a, s) \sim (c, u)$. On note K l'ensemble quotient, c.-à-d., l'ensemble des classes d'équivalence, et pour tout $(a, s) \in \mathrm{C}$ on désigne par $[a, s]$ son image dans K.

On va définir sur K une structure d'anneau, déduite des lois d'addition et de multiplication des fractions :

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

C-à-d., guidés par les formules ci-dessus, on pose

$$[a, s] + [b, t] = [at + bs, st], \qquad [a, s][b, t] = [ab, st].$$

On vérifie facilement que ceci définit sur K une structure d'anneau, dont le 0 est $[0, 1]$ et l'élément unité $[1, 1]$. De plus, un élément $[a, s]$ est non-nul si et seulement si $a \neq 0$; dans ce cas on a

$$[a, s][s, a] = [as, as] = 1,$$

et donc $[a, s]$ est inversible. Ceci prouve que K est un corps. Enfin, l'application $a \mapsto [a, 1]$ est un morphisme d'anneaux de A dans K, et ce morphisme est injectif car si $[a, 1] = 0$ alors $a = 0$. On peut donc identifier A au sous-anneau de K formé des éléments $[a, 1]$, pour $a \in \mathrm{A}$. Pour $b \neq 0$, $[1, b]$ est l'inverse de $[b, 1]$. Par conséquent, si on identifie chaque élément a de A avec son image $[a, 1]$ dans K, on obtient que tout élément $[a, b]$ de K (où $b \neq 0$, est égal à la fraction $ab^{-1} = a/b$. Ceci prouve que K est « le » corps des fractions de A.

Pour le moment, les guillemets sont nécessaires car il n'est pas tout-à-fait évident que K soit uniquement déterminé par les propriétés ci-dessus. En fait, c'est bien le cas, car K vérifie la propriété universelle ci-dessous. Notons τ le morphisme $\mathrm{A} \to \mathrm{K}$, $a \mapsto [a, 1]$.

Proposition 9.35. — *Le corps* K *vérifie la propriété universelle suivante : pour tout morphisme d'anneaux* $\phi : \mathrm{A} \to \mathrm{B}$ *tel que* $\phi(a)$ *soit inversible pour tout* $a \neq 0$*, il existe un* **unique** *morphisme* $\Phi : \mathrm{K} \to \mathrm{B}$ *tel que* $\Phi \circ \tau = \phi$.

Démonstration. — Si Φ existe, on a nécessairement, pour tout $a \in \mathrm{A}$, $\Phi(\tau(a)) = \phi(a)$. Alors, pour $s \neq 0$, l'égalité

$$1 = \Phi(1) = \Phi(\tau(s)\tau(s)^{-1}) = \phi(s)\Phi(\tau(s)^{-1})$$

entraîne $\Phi(\tau(s)^{-1}) = \phi(s)^{-1}$. Enfin, comme $[a, s] = \tau(a)\tau(s)^{-1}$, nécessairement Φ doit vérifier

$$\Phi([a, s]) = \phi(a)\phi(s)^{-1}. \tag{1}$$

Ceci montre que Φ, s'il existe, est nécessairement unique. Il reste à vérifier que la formule (1) définit Φ sans ambiguités. Or, si $[a, s] = [b, t]$, on a $at = bs$ d'où

$$\phi(a)\phi(t) = \phi(at) = \phi(bs) = \phi(b)\phi(s).$$

Comme $\phi(s)$ et $\phi(t)$ sont inversibles, on en déduit $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$. Ceci montre que Φ est bien définie, et la proposition est démontrée. □

Un corollaire standard de ce type de propriété universelle est que K est unique à isomorphisme unique près. C.-à-d., on a le corollaire suivant.

Corollaire 9.36. — *Soit* $\tau' : \mathrm{A} \to \mathrm{K}'$ *un autre morphisme d'anneaux tel que* $\tau'(s)$ *soit inversible pour tout* $s \neq 0$ *et vérifiant la propriété universelle ci-dessus. Alors il existe un unique morphisme* $\Phi : \mathrm{K} \to \mathrm{K}'$ *tel que* $\Phi \circ \tau = \tau'$*, et c'est un isomorphisme. En particulier,* K′ *est un corps isomorphe à* K.

Démonstration. — Par la propriété universelle de K (resp. K′) il existe un unique morphisme $\Phi : \mathrm{K} \to \mathrm{K}'$ tel que $\Phi \circ \tau = \tau'$. De même, par la propriété universelle de K′ il existe un unique morphisme $\Psi : \mathrm{K}' \to \mathrm{K}$ tel que $\Psi \circ \tau' = \tau$.

Alors, $\Psi \circ \Phi \circ \tau = \Psi \circ \tau' = \tau$, donc, par la propriété universelle de K, appliquée à $\mathrm{B}' = \mathrm{K}$ et $\tau' = \tau$, on obtient que $\Psi \circ \Phi = \mathrm{id}_{\mathrm{K}}$. On obtient de même que $\Phi \circ \Psi = \mathrm{id}_{\mathrm{K}'}$. Ceci prouve le corollaire. □

Remarque 9.37. — Cet argument montre qu'un problème universel du type ci-dessus a au plus une solution (à isomorphisme unique près). Mais il ne dit rien quant à l'existence d'une solution. Il faut donc bien construire K comme on l'a fait plus haut.

Exemples 9.38. — 1) Le corps des fractions de $\mathbb{Z}$ est le corps des rationnels

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z},\, q \neq 0 \right\}.$$

2) Soit k un corps et $\mathrm{A} = k[\mathrm{X}]$ l'anneau des polynômes à coefficients dans k ; c'est un anneau intègre (exercice !). Son corps des fractions est le corps des fractions rationnelles

$$k(\mathrm{X}) = \left\{ \frac{\mathrm{P}(\mathrm{X})}{\mathrm{Q}(\mathrm{X})} \mid \mathrm{P}, \mathrm{Q} \in k[\mathrm{X}],\ \mathrm{Q} \neq 0 \right\}.$$

On a ainsi traité, pour un anneau intègre A, le cas où l'on rend inversibles tous les éléments de $\mathrm{A} \setminus \{0\}$. Dans certaines situations, on souhaite inverser seulement une partie S des éléments de A. On verra plus loin qu'une telle construction est possible pour tout anneau commutatif A, sans hypothèse d'intégrité.

9.8. Corps des fractions d'un anneau factoriel. —

***Théorème 9.39* (Unicité de l'écriture des fractions)**. — *Soit* A *factoriel et soit* K *son corps des fractions.*

1) *Soient $x, y \in \mathrm{A} \setminus \{0\}$ et soit d un PGCD de x et y. Alors x/d et y/d sont sans facteur commun.*

2) *Tout élément $f \neq 0$ de* K *s'écrit de façon unique, aux inversibles près, $f = a/b$, avec $a, b \in \mathrm{A} \setminus \{0\}$ sans facteur commun.*

Démonstration. — 1) Écrivons $x = da$ et $y = db$. Si p était un élément non inversible divisant a et b, l'idéal (dp) contiendrait x et y et serait strictement contenu dans (d), contrairement à la définition de (d). Ceci prouve 1).

2) Soit $f \in \mathrm{K} \setminus \{0\}$. Par définition de K, il existe $x, y \in \mathrm{A} \setminus \{0\}$ tels que $f = x/y$. Soit d un pgcd de x et y ; posons $x = da$ et $y = db$. Alors a, b sont sans facteur commun, et $f = da/db = a/b$. Ceci prouve l'existence.

Montrons l'unicité, aux inversibles près. Supposons que $f = c/d$, avec c et d sans facteur commun. Alors, on a l'égalité

$$ad = bc.$$

Comme a, b (resp. c, d) sans sont facteur commun, il résulte du Lemme de Gauss que $a \mid c$ et $b \mid d$ (resp. $d \mid b$ et $c \mid a$). Par conséquent, a et c sont associés, de même que b et d. Le théorème est démontré. □

9.9. Le théorème de transfert de Gauss. — Le but de cette section est de démontrer le théorème suivant.

***Théorème 9.40* (Théorème de transfert de Gauss)**. — *Soit* A *un anneau factoriel. Alors* $\mathrm{A}[\mathrm{X}]$ *est factoriel.*

Corollaire 9.41. — *Si* A *est factoriel,* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *l'est aussi.*

Démonstration. — Le corollaire découle du théorème par récurrence sur n, vu l'isomorphisme $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \cong (\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}])[\mathrm{X}_n]$. □

Pour la démonstration du théorème, on aura besoin de notions et résultats préliminaires. Démontrons d'abord la proposition suivante. Soit K le corps des fractions de A.

Proposition 9.42. — *Soit* A *intègre et soit* $P \in A[X]$ *vérifiant l'une des deux conditions suivantes :*

i) P *est un élément irréductible de* A *;*

ii) $\deg P \geqslant 1$*, les coefficients de* P *sont sans facteur commun, et* P *est irréductible en tant qu'élément de* K[X].

Alors P *est un élément irréductible de* A[X].

Démonstration. — Supposons $P = QR$, avec $QR \in A[X]$.

1) Si P est un élément irréductible $p \in A$, alors Q et R sont de degré 0, donc appartiennent à A, et l'irréductibilité de p entraîne que Q ou R est inversible. Ceci prouve que p est irréductible dans A[X].

2) Supposons ii) vérifiée. L'irréductibilité de P comme élément de K[X] entraîne, disons, que $\deg Q = 0$. Donc Q appartient à A, et est un diviseur commun à tous les coefficients de P. Par conséquent, Q est inversible. Ceci prouve que P est un élément irréductible de A[X]. La proposition est démontrée. □

On aura besoin plus loin du lemme suivant. Soit I un idéal de A et notons IA[X] l'idéal de A[X] engendré par I. On observe que IA[X] est formé des polynômes dont tous les coefficients appartiennent à I.

Lemme 9.43. — *On a un isomorphisme de* A*-algèbres*

$$A[X]/IA[X] \xrightarrow{\sim} (A/I)[X].$$

Par conséquent, si I *est un idéal premier de* A*, alors* IA[X] *est un idéal premier de* A[X].

Démonstration. — Soit π la projection $A \to A/I$; ceci fait de A/I une A-algèbre. D'après la propriété universelle de A[X], il existe un unique morphisme de A-algèbres $\phi : A[X] \to (A/I)[X]$ tel que $\phi(X) = X$. Explicitement, pour tout $P = a_0 + \cdots + a_d X^d$, on a

$$\phi(P) = \pi(a_0) + \cdots + \pi(a_d)X^d.$$

Il est clair que ce morphisme est surjectif, et son noyau est l'idéal des polynômes dont tous les coefficients sont dans I, c.-à-d., IA[X]. Ceci prouve la première assertion. La deuxième en résulte, d'après la proposition 7.2. □

Définition 9.44 **(Contenu d'un polynôme et polynômes primitifs)**

Soit A factoriel et soit $P \in A[X] \setminus \{0\}$.

1) On note $c(P)$ et l'on appelle **contenu** de P un pgcd de ses coefficients. (Ainsi, le contenu est défini à un inversible près).

2) On dit que P est **primitif** si $c(\mathrm{P})$ est inversible, c.-à-d., si les coefficients de P sont sans facteur commun.

Remarque 9.45. — Soit $a \in \mathrm{A} \setminus \{0\}$. On voit facilement que $c(a\mathrm{P}) = ac(\mathrm{P})$.

***Théorème 9.46* (Lemme des contenus de Gauss)**. — *Soit* A *factoriel et soient* $\mathrm{P}, \mathrm{Q} \in \mathrm{A}[\mathrm{X}] \setminus \{0\}$. *On a*

$$c(\mathrm{PQ}) = c(\mathrm{P})c(\mathrm{Q}).$$

Démonstration. — On peut écrire $\mathrm{P} = c(\mathrm{P})\widetilde{\mathrm{P}}$ et $\mathrm{Q} = c(\mathrm{Q})\widetilde{\mathrm{Q}}$, où $\widetilde{\mathrm{P}}$ et $\widetilde{\mathrm{Q}}$ sont primitifs. Alors

$$\mathrm{PQ} = c(\mathrm{P})c(\mathrm{Q})\widetilde{\mathrm{P}}\widetilde{\mathrm{Q}},$$

et donc $c(\mathrm{PQ}) = c(\mathrm{P})c(\mathrm{Q})c(\widetilde{\mathrm{P}}\widetilde{\mathrm{Q}})$, d'après la remarque précédente.

Par conséquent, on peut supposer P et Q primitifs, et il s'agit de montrer que PQ l'est aussi. Supposons que ce ne soit pas le cas, et soit p un élément irréductible divisant $c(\mathrm{PQ})$.

Alors, dans l'anneau $\mathrm{A}[\mathrm{X}]/p\mathrm{A}[\mathrm{X}]$, on a $\overline{\mathrm{P}}\,\overline{\mathrm{Q}} = 0$. Mais, d'après le lemme 9.43, l'on a

$$\mathrm{A}[\mathrm{X}]/p\mathrm{A}[\mathrm{X}] \cong (\mathrm{A}/p\mathrm{A})[\mathrm{X}],$$

et cet anneau est intègre, car pA est un idéal premier de A puisque A est factoriel. Par conséquent, on a $\overline{\mathrm{P}} = 0$ ou $\overline{\mathrm{Q}} = 0$, et donc p divise tous les coefficients de P ou de Q, ce qui contredit l'hypothèse que P et Q sont primitifs. Cette contradiction montre que PQ est primitif, et le théorème est démontré. □

Corollaire 9.47. — *Soient* A *factoriel,* K *son corps des fractions, et* $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ *un polynôme irréductible de degré* $\geqslant 1$. *Alors* P *est encore irréductible dans* K[X].

Démonstration. — Comme P est irréductible et de degré $\geqslant 1$, il est primitif. Supposons $\mathrm{P} = \mathrm{QR}$, avec $\mathrm{Q}, \mathrm{R} \in \mathrm{K}[\mathrm{X}]$. On peut écrire

$$\mathrm{Q} = \frac{a}{b}\widetilde{\mathrm{Q}}, \qquad \mathrm{R} = \frac{d}{f}\widetilde{\mathrm{R}},$$

avec $\widetilde{\mathrm{Q}}, \widetilde{\mathrm{R}} \in \mathrm{A}[\mathrm{X}]$ primitifs, $a, b, d, f \in \mathrm{A}$, et $bf \neq 0$. Alors

$$bf\mathrm{P} = ad\widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}.$$

Prenant les contenus et appliquant le lemme de Gauss, on obtient :

$$bf = ad\, c(\widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}) = ad,$$

d'où $\mathrm{P} = \widetilde{\mathrm{Q}}\widetilde{\mathrm{R}}$. Comme P est irréductible dans A[X], ceci entraîne que $\widetilde{\mathrm{Q}}$ ou $\widetilde{\mathrm{R}}$ est un élément inversible de A, et donc Q ou R est un élément inversible de K. Ceci prouve que P est irréductible dans K[X]. □

Nous pouvons maintenant démontrer le théorème de transfert de Gauss. On suppose désormais A factoriel.

Montrons que A[X] vérifie (E). Considérons d'abord un élément primitif $P \in A[X]$, de degré $\geqslant 1$. Considéré comme élément de K[X], P s'écrit :

$$P = P_1^{n_1} \cdots P_r^{n_r},$$

où les P_i sont des polynômes irréductibles de K[X] de degré $\geqslant 1$. Pour chaque i, on peut écrire $P_i = (a_i/b_i)\widetilde{P}_i$, avec $a_i, b_i \in A \setminus \{0\}$ et $\widetilde{P}_i \in A[X]$ primitif. De plus, chaque $\widetilde{P}_i$ est, comme P_i, irréductible dans K[X]. Donc, d'après la proposition 9.42, chaque $\widetilde{P}_i$ est un élément irréductible de A[X]. De plus, on a l'égalité

$$(b_1^{n_1} \cdots b_r^{n_r})\, P = (a_1^{n_1} \cdots a_r^{n_r})\, \widetilde{P}_1^{n_1} \cdots \widetilde{P}_r^{n_r}.$$

En prenant les contenus et en appliquant le lemme de Gauss, on voit que $b_1^{n_1} \cdots b_r^{n_r}$ et $a_1^{n_1} \cdots a_r^{n_r}$ sont associés. Par conséquent,

$$P = u\widetilde{P}_1^{n_1} \cdots \widetilde{P}_r^{n_r},$$

avec $u \in A$ inversible, et ceci est une décomposition de P en facteurs irréductibles.

Enfin, soit $P \in A[X] \setminus \{0\}$ arbitraire. On peut écrire $P = c(P)\widetilde{P}$, où $\widetilde{P} \in A[X]$ est primitif. Alors $\widetilde{P}$ admet une décomposition comme ci-dessus, et, d'autre part, $c(P) \in A$ se décompose en produit d'irréductibles. Ceci prouve que A[X] vérifie (E).

Conséquence. Le résultat de décomposition qu'on vient de démontrer implique le résultat suivant :

(†) Soit P un élément irréductible de A[X]. Alors ou bien : *i)* $\deg P = 0$ et $P = p$ est un élément irréductible de A, ou bien : *ii)* $\deg P \geqslant 1$ et P est primitif et reste irréductible dans K[X].

En effet, soit $P \in A[X]$ irréductible. D'après ce qui précède, P s'écrit comme un produits d'irréductibles

$$P = a_1 \cdots a_r P_1 \cdots P_s$$

avec les a_i de type *i)* et les P_j de type *ii)*. Comme P est irréductible, on a $r + s = 1$ et donc $P = a_1$ ou bien $P = P_1$.

Pour montrer que A[X] est factoriel, il reste à montrer, d'après la proposition 9.18, que tout élément irréductible engendre un idéal premier. Si p est un élément irréductible de A, ceci résulte du fait que

$$A[X]/pA[X] \cong (A/pA)[X]$$

est intègre. D'autre part, soit $P \in A[X]$ un élément irréductible de degré $\geqslant 1$. Supposons que P divise un produit QR, où $Q, R \in A[X]$.

Comme P est irréductible dans K[X], qui est factoriel d'après le théorème 9.30, on peut supposer que P divise Q dans K[X]. Il existe donc $a, b \in \mathrm{A} \setminus \{0\}$ et $\mathrm{S} \in \mathrm{A}[\mathrm{X}]$ primitif tels que

$$(*) \qquad \mathrm{Q} = \frac{a}{b}\,\mathrm{SP},$$

d'où $b\mathrm{Q} = a\mathrm{PS}$. D'après le lemme des contenus, on obtient que

$$b\,c(\mathrm{Q}) = a\,c(\mathrm{PS}) = a,$$

d'où $a/b \in \mathrm{A}$. Alors $(*)$ montre que P divise Q dans A[X]. Ceci prouve que l'idéal (P) de A[X] est premier. Ceci termine la preuve du théorème de transfert de Gauss.

Corollaire 9.48. — *Soient* A *factoriel,* K *le corps des fractions de* A*, et* $\mathrm{P}, \mathrm{Q} \in \mathrm{A}[\mathrm{X}] \setminus \{0\}$.

1) *Écrivons* $\mathrm{P} = c(\mathrm{P})\widetilde{\mathrm{P}}$*, avec* $\widetilde{\mathrm{P}} \in \mathrm{A}[\mathrm{X}]$ *primitif, et soit*

$$(*) \qquad \widetilde{\mathrm{P}} = \mathrm{P}_1 \cdots \mathrm{P}_n$$

la décomposition de $\widetilde{\mathrm{P}}$ *en facteurs irréductibles de degré* $\geqslant 1$ *dans* A[X]*. Alors* $\mathrm{P}_1, \ldots, \mathrm{P}_n$ *sont les facteurs irréductibles de* P *dans* K[X].

2) *Si* P *et* Q *sont sans facteur commun dans* A[X]*, ils sont sans facteur commun dans* K[X].

Démonstration. — 1) Comme $c(\mathrm{P})$ est un élément inversible de K, P et $\widetilde{\mathrm{P}}$ ont les mêmes facteurs irréductibles (définis aux inversibles de K près). On peut supposer $n \geqslant 1$ (sinon P est un élément inversible de K). Alors, d'après le corollaire 9.47, chaque P_i est encore irréductible dans K[X] et donc $(*)$ est la décomposition de $\widetilde{\mathrm{P}}$ en facteurs irréductibles dans K[X]. Ceci prouve le point 1).

Le point 2) découle immédiatement du point 1). □

9.10. Sous-variétés algébriques fermées de $\mathbb{C}^2$. —

Proposition 9.49. — *Soient* $\mathrm{F}, \mathrm{G} \in \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ *des polynômes sans facteur commun. Alors la variété*

$$\mathscr{V}(\mathrm{F}, \mathrm{G}) := \{(x, y) \in \mathbb{C}^2 \mid \mathrm{F}(x, y) = 0 = \mathrm{G}(x, y)\}$$

est formée d'un nombre fini de points.

Démonstration. — Par hypothèse, F et G considérés comme éléments de $\mathbb{C}[\mathrm{X}][\mathrm{Y}]$ n'ont pas de facteur commun.

D'après le corollaire 9.48, F et G restent sans facteur commun dans $\mathbb{C}(X)[Y]$, qui est principal. Donc, d'après le théorème de Bézout (9.24), il existe $A, B \in \mathbb{C}(X)[Y]$ tels que

$$(*_X) \qquad AF + BG = 1.$$

Écrivons $A(X,Y) = \sum_{i=0}^{d} U_i(X)Y^i$ et $B(X,Y) = \sum_{j=0}^{f} V_j(X)Y^i$, avec $U_i, V_j \in \mathbb{C}(X)$. Soit $P \in \mathbb{C}[X]$ un dénominateur commun à tous les U_i et V_j ; alors $P(X)A(X,Y)$ et $P(X)B(X,Y)$ appartiennent à $\mathbb{C}[X,Y]$, et $(*_X)$ devient :

$$(**_X) \qquad PAF + PBG = P.$$

Échangeant les rôles de X et Y, on obtient de même qu'il existe $C, D \in \mathbb{C}(Y)[X]$ et $Q \in \mathbb{C}[Y]$ tels que $QC, QD \in \mathbb{C}[X,Y]$ et

$$(**_Y) \qquad QCF + QDG = Q.$$

Par conséquent, si $(x,y) \in \mathbb{C}^2$ est un zéro commun à F et G, alors $P(x) = 0$ et $Q(y) = 0$, et donc il n'y a qu'un nombre fini de possibilités pour x et y. Ceci montre que l'intersection

$$\mathscr{V}(F) \cap \mathscr{V}(G) = \mathscr{V}(F,G)$$

est formée d'un nombre fini de points. □

Lemme 9.50. — *Tout point $p = (x,y) \in \mathbb{C}^2$ est la variété des zéros de l'idéal maximal*

$$\mathfrak{m}_p = (X - x, Y - y).$$

Par conséquent, une sous-variété algébrique fermée irréductible de $\mathbb{C}^2$ est soit un singleton, soit de cardinal infini.

Démonstration. — Facile et laissée au lecteur. □

Théorème 9.51. — *Soit $V = \mathscr{V}(I)$ une sous-variété algébrique de $\mathbb{C}^n$. Alors :*

1) $V = \mathscr{V}(\mathscr{I}(V))$.

2) *Soit W une seconde sous-variété algébrique de $\mathbb{C}^n$. Alors*

$$\mathscr{I}(V \bigcup W) = \mathscr{I}(V) \bigcap \mathscr{I}(W).$$

3) V *est* **irréductible** *si et seulement si l'idéal $\mathscr{I}(V)$ est* **premier**.

Démonstration. — On rappelle que $\mathscr{V}(I)$ désigne la variété des zéros d'un idéal I et, si W est un sous-ensemble de $\mathbb{C}^n$,

$$\mathscr{I}(W) := \{P \in \mathbb{C}[X_1, \ldots, X_n] \mid P(w) = 0, \quad \forall\, w \in W\}$$

est l'idéal des polynômes nuls sur W. On voit immédiatement que les applications $\mathrm{I} \mapsto \mathscr{V}(\mathrm{I})$ et $\mathrm{W} \mapsto \mathscr{I}(\mathrm{W})$ sont toutes les deux *décroissantes*, c.-à-d., on a :

$$(\dagger) \qquad \begin{cases} \mathrm{I} \subseteq \mathrm{J} \ \Rightarrow \ \mathscr{V}(\mathrm{I}) \supseteq \mathscr{V}(\mathrm{J}), \\ \mathrm{V} \subseteq \mathrm{W} \Rightarrow \mathscr{I}(\mathrm{V}) \supseteq \mathscr{I}(\mathrm{W}). \end{cases}$$

Considérons $\mathrm{V} = \mathscr{V}(\mathrm{I})$. Alors on a, bien sûr, $\mathrm{I} \subseteq \mathscr{I}(\mathrm{V})$ et $\mathrm{V} \subseteq \mathscr{V}(\mathscr{I}(\mathrm{V}))$. D'après (†), on obtient :

$$\mathrm{V} = \mathscr{V}(\mathrm{I}) \supseteq \mathscr{V}(\mathscr{I}(\mathrm{V})) \supseteq \mathrm{V},$$

d'où $\mathrm{V} = \mathscr{V}(\mathscr{I}(\mathrm{V}))$. Ceci prouve 1).

Prouvons 2). Comme $\mathrm{V} \cup \mathrm{W}$ contient V et W, (†) entraîne

$$\mathscr{I}(\mathrm{V} \bigcup \mathrm{W}) \subseteq \mathscr{I}(\mathrm{V}) \bigcap \mathscr{I}(\mathrm{W}).$$

Réciproquement, soit $f \in \mathscr{I}(\mathrm{V}) \bigcap \mathscr{I}(\mathrm{W})$; alors f est nulle sur V et sur W, donc sur $\mathrm{V} \cup \mathrm{W}$, d'où $f \in \mathscr{I}(\mathrm{V} \cup \mathrm{W})$. Ceci prouve 2).

Prouvons 3). Posons $\mathrm{A} = \mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et $\mathrm{J} = \mathscr{I}(\mathrm{V})$. Supposons V irréductible et soit $f, g \in \mathrm{A} \setminus \mathrm{J}$. Alors $\mathrm{W} := \mathscr{V}(\mathrm{J} + \mathrm{A}f) \subseteq \mathscr{V}(\mathrm{J}) = \mathrm{V}$, et $\mathrm{W} \neq \mathrm{V}$ car $f \in \mathscr{I}(\mathrm{W})$ mais $f \notin \mathscr{I}(\mathrm{V}) = \mathrm{J}$. De même, $\mathrm{W}' := \mathscr{V}(\mathrm{J} + \mathrm{A}g)$ est *strictement* contenu dans V. Si l'on avait $fg \in \mathrm{J}$, alors fg serait identiquement nulle sur V et donc V serait réunion de W et W′, contredisant l'irréductibilité de V. Ceci montre que : V irréductible $\Rightarrow \mathscr{I}(\mathrm{V})$ premier.

Réciproquement, supposons que $\mathrm{J} = \mathscr{I}(\mathrm{V})$ soit premier et que V soit réunion de deux sous-variétés algébriques fermées W et W′. Alors, d'après le point 2) l'on a

$$\mathrm{J} = \mathscr{I}(\mathrm{W}) \bigcap \mathscr{I}(\mathrm{W}') \supseteq \mathscr{I}(\mathrm{W})\mathscr{I}(\mathrm{W}').$$

Comme J est premier, ceci entraîne que J contient $\mathscr{I}(\mathrm{W})$ ou $\mathscr{I}(\mathrm{W}')$, disons $\mathscr{I}(\mathrm{W})$. Mais alors $\mathrm{W} \supseteq \mathrm{V}$ et donc $\mathrm{W} = \mathrm{V}$. Ceci prouve que : $\mathscr{I}(\mathrm{V})$ premier $\Rightarrow$ V irréductible. Le théorème est démontré. □

Corollaire 9.52. — $\mathbb{C}^n = \mathscr{V}(0)$ *est une sous-variété algébrique fermée irréductible de* $\mathbb{C}^n$.

Théorème 9.53. — *Soit* V *une sous-variété algébrique fermée irréductible de* $\mathbb{C}^2$*, de cardinal infini et distincte de* $\mathbb{C}^2$*. Alors,*

$$\mathscr{I}(\mathrm{V}) = (\mathrm{F}),$$

où $\mathrm{F} \in \mathbb{C}[\mathrm{X}, \mathrm{Y}]$ *est un polynôme irréductible (unique à multiplication par un scalaire non-nul près).*

Démonstration. — Comme $V \neq \mathbb{C}^2$, alors $\mathscr{I}(V) \neq (0)$. Soit donc E un élément non nul de $\mathscr{I}(V)$ et soit

$$E = E_1 \cdots E_n$$

sa décomposition en facteurs irréductibles. Comme $\mathscr{I}(V)$ est premier (d'après le théorème précédent), il contient au moins un des facteurs irréductibles de E, disons $F = E_1$. Soit G un élément arbitraire de $\mathscr{I}(V)$. Comme

$$V \subseteq \mathscr{V}(F) \bigcap \mathscr{V}(G),$$

il résulte de la proposition 9.49 que F et G ont un facteur commun ; donc, comme F est irréductible, on obtient que F divise G, c.-à-d., $G \in (F)$. Ceci montre que $\mathscr{I}(V) = (F)$. L'unicité de F (à un scalaire près) résulte du lemme 9.4 et du fait que les éléments inversibles de $\mathbb{C}[X, Y]$ sont les éléments de $\mathbb{C}^\times$ (d'après la proposition 7.2). □

9.11. Exemples d'anneaux noethériens non factoriels. —

***Définition 9.54* (Extensions quadratiques et normes).** — Soit $n \in \mathbb{Z}$, distinct de 1 et sans facteur carré (c.-à-d., $n = -1$ ou bien $\pm n$ est un produit de nombres premiers > 0 deux à deux distincts). Désignant par $\sqrt{n}$ l'une quelconque des racines carrées de n dans $\mathbb{C}$, considérons le sous-anneau de $\mathbb{C}$ suivant :

$$\mathbb{Z}[\sqrt{n}\,] = \{a + \sqrt{n}\,b \mid a, b \in \mathbb{Z}\}.$$

On a :

$$(a + \sqrt{n}\,b)(a' + \sqrt{n}\,b') = (aa' + nbb') + \sqrt{n}\,(ab' + ba'). \tag{1}$$

Pour $u = a + \sqrt{n}\,b$, on définit son **conjugué** $\overline{u} = a - \sqrt{n}\,b$ et sa **norme** :

$$N(u) = u\overline{u} = a^2 - nb^2. \tag{2}$$

On déduit de (1) que

$$\overline{uv} = \overline{u}\,\overline{v} \qquad \text{et} \qquad N(uv) = N(u)N(v). \tag{3}$$

Il en résulte que u est inversible si et seulement si $N(u) = \pm 1$.

Comme $\mathbb{Z}[\sqrt{n}\,]$ est noethérien, tout élément non nul et non inversible de $\mathbb{Z}[\sqrt{n}\,]$ est produit d'éléments irréductibles. Par contre, le Lemme d'Euclide, et l'unicité des facteurs irréductibles, peuvent être en défaut. C'est le cas, par exemple, pour $n = -3, -5$, ou 5.

***Exemples 9.55*.** — 1) Dans $\mathbb{Z}[\sqrt{-3}\,]$, on a $N(a + \sqrt{-3}\,b) = a^2 + 3b^2$ donc les inversibles sont ± 1 et il n'y a pas d'élément de norme 2. D'autre part, on a l'égalité suivante :

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Tous les facteurs sont de norme 4, donc irréductibles (car il n'y a pas d'élément de norme 2). Si $1 + \sqrt{-3}$ vérifiait le Lemme d'Euclide, il diviserait 2, et comme

ce dernier est irréductible, on aurait $2 = u(1+\sqrt{-3}\,)$, avec u inversible, donc $u = \pm 1$, une contradiction. Ceci montre que $\mathbb{Z}[\sqrt{-3}\,]$ n'est pas factoriel.

2) De même, dans $\mathbb{Z}[\sqrt{-5}\,]$, $\mathrm{N}(a+\sqrt{-5}\,b) = a^2+5b^2$ donc les inversibles sont ± 1 et il n'y a pas d'élément de norme 2 ou 3. D'autre part, on a l'égalité

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

Les facteurs sont de norme, respectivement, $4, 9, 6, 6$, donc sont irréductibles. Le même argument que précédemment montre que si $1+\sqrt{-5}$ vérifiait le Lemme d'Euclide, il serait égal à ± 2 ou ± 3, ce qui n'est pas le cas. Ceci montre que $\mathbb{Z}[\sqrt{-5}\,]$ n'est pas factoriel.

3) Dans $\mathbb{Z}[\sqrt{5}\,]$, on a $\mathrm{N}(a+\sqrt{5}\,b) = a^2-5b^2$. Il n'y a pas d'élément de norme ± 2. En effet, une égalité $a^2 = \pm 2 + 5b^2$ est impossible, puisque le carré d'un nombre pair (resp. impair) est congru à 0 (resp. 1) modulo 4.

D'autre part, on a l'égalité

$$(1+\sqrt{5}\,)(-1+\sqrt{5}\,) = 2 \cdot 2.$$

Les facteurs de gauche sont de norme -4, ceux de droite de norme 4, donc chaque facteur est irréductible, puisqu'il n'y a pas d'élément de norme ± 2. L'élément irréductible 2 ne vérifie pas le Lemme d'Euclide, car sinon on aurait, disons, $1+\sqrt{5} = 2u$, et

$$u = \frac{1}{2} + \frac{1}{2}\sqrt{5}$$

appartiendrait à $\mathbb{Z}[\sqrt{5}\,]$, ce qui n'est pas le cas, puisque 1 et $\sqrt{5}$ sont linéairement indépendants sur $\mathbb{Q}$. Ceci montre que $\mathbb{Z}[\sqrt{5}\,]$ n'est pas factoriel.

4) Il faut se garder de croire que l'argument précédent s'applique à $\mathbb{Z}[\sqrt{7}\,]$. Dans cet anneau, on a bien l'égalité

$$2 \cdot 3 = 6 = (1+\sqrt{7}\,)(-1+\sqrt{7}\,),$$

mais aucun des facteurs ci-dessus n'est irréductible. En effet, on a

$$\begin{array}{ll} 2 = (3+\sqrt{7}\,)(3-\sqrt{7}\,), & 1+\sqrt{7} = (3+\sqrt{7}\,)(-2+\sqrt{7}\,), \\ 3 = (2+\sqrt{7}\,)(-2+\sqrt{7}\,), & -1+\sqrt{7} = (3-\sqrt{7}\,)(2+\sqrt{7}\,). \end{array}$$

En fait, on peut montrer que $\mathbb{Z}[\sqrt{7}\,]$ est un anneau factoriel, mais la démonstration nécessite des techniques plus sophistiquées, voir par exemple [**Sa**, Ex.V.7].

TABLE DES MATIÈRES