Université Pierre et Marie Curie (Paris VI)
Master de Sciences et Technologie
Mention Mathématiques et Applications
1ère année

Algèbre et Théorie de Galois
2005-2006

Patrick Polo

Patrick Polo
Université Paris VI, Institut de Mathématiques,
175 rue du Chevaleret, 75013 Paris
Mél : polo@math.jussieu.fr

0 Nombres entiers et nombres algébriques entiers

Version du 23 octobre 2005

1 Nombres entiers et rationnels

1.1 Notations et définitions

On rappelle que $\mathbb{Z}$ désigne l'ensemble des nombres entiers, positifs ou négatifs, c.-à-d., $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$, et $\mathbb{Q}$ désigne l'ensemble des nombres rationnels, c.-à-d.,

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

On note $\mathbb{N} = \{0, 1, 2, \ldots\}$ l'ensemble des entiers ≥ 0. On suppose également connus l'ensemble $\mathbb{R}$ des nombres réels, et l'ensemble $\mathbb{C}$ des nombres complexes,

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\},$$

où $i^2 = -1$.

On note $\mathbb{Z}^*$, resp. $\mathbb{Q}^*$, l'ensemble des entiers, resp. rationnels, non nuls, et l'on note $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Pour tout $r \in \mathbb{Q}$, on note $|r|$ sa valeur absolue, c.-à-d.,

$$|r| = \sqrt{r^2} = \begin{cases} r & \text{si } r \geq 0; \\ -r & \text{si } r \leq 0. \end{cases}$$

On rappelle qu'un entier n est dit inversible s'il existe un entier n' tel que $nn' = 1$. Les seuls entiers inversibles sont ± 1.

Définition 1.1.1 *On dit qu'un entier p est* **premier** *s'il est non-inversible (c.-à-d., $\neq \pm 1$), et n'est divisible que par ± 1 et $\pm p$.*

Ainsi, $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$ sont des nombres premiers.

Pour tout $n \geq 1$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des entiers modulo n, c.-à-d., des classes d'équivalence pour la relation $a \equiv b$ si $a - b \in n\mathbb{Z}$. On note $\dot{a}$ ou $a + n\mathbb{Z}$ la classe de a. On rappelle que l'on peut additionner, soustraire et multiplier les entiers modulo n, par les formules :

$$\dot{a} \pm \dot{b} = \dot{\overbrace{a \pm b}}, \qquad \dot{a}\dot{b} = \dot{\overbrace{ab}} .$$

Il faut bien entendu vérifier que ces opérations sont bien définies ; ceci est supposé connu. C'est un cas particulier de construction d'un anneau quotient, construction qu'on introduira plus loin.

1.2 Division euclidienne et conséquences

Proposition 1.2.1 (Division euclidienne) *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple d'entiers (q, r) tels que $a = bq + r$ et $0 \leq r < b$.*

On appelle q et r le quotient et le reste de la division euclidienne de a par b.

Démonstration. Soit q le plus grand entier tel que $bq \leq a$ et soit $r = a - bq$. Alors $0 \leq r < b$ et $a = bq + r$. Ceci prouve l'existence. Si (q', r') est un second couple vérifiant les mêmes propriétés, alors $b(q' - q)$ égale $r - r'$ donc est de valeur absolue $< b$, et ceci entraîne $q' = q$ et $r' = r$. Ceci prouve l'unicité. □

Proposition 1.2.2 *Tout sous-groupe $\neq \{0\}$ de $\mathbb{Z}$ est de la forme $b\mathbb{Z}$, pour un $b > 0$ uniquement déterminé.*

Démonstration. Soit G un sous-groupe non-nul de $\mathbb{Z}$ et soit b le plus petit élément > 0 de G. Soit $a \in G$ arbitraire. Alors a est multiple de b. En effet, faisons la division euclidienne $a = bq + r$; alors le reste $r = a - bq$ appartient à G, et est $< b$, donc nécessairement nul. Ceci prouve que $G = b\mathbb{Z}$. De plus, b est uniquement déterminé par cette propriété. En effet, si $G = b'\mathbb{Z}$, alors il existe $n, n' \in \mathbb{Z}$ tels que $b' = nb$ et $b = n'b'$, d'où $b = n'nb$ et $1 = nn'$ (car $b \neq 0$), d'où $n = \pm 1 = n'$ et donc $b' = \pm b$. Donc, si on impose $b' > 0$ alors $b' = b$. □

Définition 1.2.3 *Soient $n_1, \ldots, n_r \in \mathbb{Z}$. L'ensemble des entiers de la forme $a_1 n_1 + \cdots + a_r n_r$, avec $a_i \in \mathbb{Z}$, est un sous-groupe de $\mathbb{Z}$. C'est le plus petit sous-groupe contenant les n_i. On l'appelle le sous-groupe engendré par $n_1, \ldots, n_r$ et on le note $\mathbb{Z}n_1 + \cdots + \mathbb{Z}n_r$.*

Définition et proposition 1.2.4 (PGCD)
Soient $n_1, \dots, n_r \in \mathbb{Z}$, non tous nuls. Le sous-groupe G qu'ils engendrent est de la forme $d\mathbb{Z}$, pour un unique $d > 0$. Alors d divise chaque n_i et, réciproquement, tout diviseur commun aux n_i divise d. On dit que d est le PGCD (plus grand commun diviseur) des n_i.

Démonstration. D'après la proposition 1.2.2, G est engendré par son plus petit élément $d > 0$, qui est de la forme

$$d = a_1 n_1 + \cdots + a_r n_r. \qquad (*)$$

Comme $n_i \in d\mathbb{Z}$, alors d divise n_i. Réciproquement, soit f un diviseur commun aux n_i. Alors $n_i = f q_i$ et l'on déduit de $(*)$ que $d = f(a_1 q_1 + \cdots + a_r q_r)$, donc f divise d. La proposition est démontrée. □

Théorème 1.2.5 (Lemme d'Euclide) *Soit p un nombre premier. Si p divise un produit ab, il divise a ou b.*

Démonstration. Supposons a non divisible par p. Alors, comme p est premier, le PGCD de p et a est nécessairement 1, donc il existe $u, v \in \mathbb{Z}$ tels que $1 = up + va$. Multipliant cette égalité par b, on obtient

$$b = upb + vab,$$

d'où on déduit que p divise b si (et seulement si) p divise ab. Le théorème est démontré. □

Par récurrence sur s, on en déduit le corollaire suivant.

Corollaire 1.2.6 *Si un nombre premier p divise un produit $a_1 \cdots a_s$, il divise l'un des a_i.*

Le Lemme d'Euclide (avec son corollaire) a des conséquences très importantes.

Théorème 1.2.7 (Euclide) *Tout entier $n \neq 0$, non inversible, (c.-à-d., $n \neq 0, \pm 1$) s'écrit de façon unique*

$$n = \varepsilon(n) p_1 \cdots p_r,$$

où $\varepsilon(n)$ est le signe de n et où les p_i sont des nombres premiers > 0 uniquement déterminés.

Démonstration. Il suffit de traiter le cas $n > 0$. Montrons par récurrence que tout entier $n \geq 2$ est produit de nombres premiers > 0. C'est bien le cas si n est premier. Sinon, l'ensemble des diviseurs d de n tels que $1 < d < n$ est non vide, donc admet un plus petit élément p, qui est nécessairement premier. Alors $n = pm$ et $1 < m < n$, donc par hypothèse de récurrence m est produit de nombres premiers > 0. Ceci prouve l'existence.

Pour montrer l'unicité, il est commode de prendre la convention qu'un produit de 0 termes (c.-à-d., un produit sur l'ensemble vide), est égal à 1. Supposons alors qu'on ait deux décompositions de l'entier $n \geq 1$ en produit de nombres premiers :

$$n = p_1 \cdots p_r = q_1 \cdots q_s. \qquad (*)$$

Montrons par récurrence sur $n \geq 1$ que $s = r$ et que, quitte à renuméroter les q_j, l'on a $q_i = p_i$ pour $i = 1, \ldots, r$.

Si $n = 1$, alors $r = 0$ et $s = 0$, car sinon p_1 ou q_1 serait inversible, une contradiction. On peut donc supposer $n > 1$ et l'unicité établie pour tout $m < n$. Comme n est non inversible (puisque $n > 1$), alors r et s sont ≥ 1. D'après le (corollaire du) Lemme d'Euclide, p_1 divise l'un des q_i, donc, quitte à permuter les q_j, on peut supposer que p_1 divise q_1. Comme q_1 est premier, ceci entraîne $q_1 = p_1$. Alors, en simplifiant par p_1 l'égalité $(*)$, on obtient $p_2 \cdots p_r = q_2 \cdots q_s$. Par hypothèse de récurrence, appliquée à l'entier $m = n/p_1$, on conclut que $s = r$ et que l'on peut renuméroter les q_j de sorte que $q_i = p_i$ pour $i = 1, \ldots, r$. Le théorème est démontré. □

Soit $n > 0$, non inversible. D'après le théorème d'Euclide, n s'écrit de façon unique

$$n = p_1^{a_1} \cdots p_r^{a_r},$$

où les p_i sont des nombres premiers deux à deux distincts, et les a_i des entiers ≥ 1. Il est commode de numéroter les p_i de sorte que $p_1 < \cdots < p_r$. On peut "lire" sur cette écriture certaines propriétés de n. Par exemple, on a le lemme suivant.

Lemme 1.2.8 *n est un carré si et seulement si chaque a_i est pair.*

Démonstration. Si $a_i = 2b_i$ pour tout i, alors n est le carré de $p_1^{b_1} \cdots p_r^{b_r}$. Réciproquement, si $n = m^2$, on peut supposer $m > 0$, et donc $m \geq 2$ (car $n \geq 2$). Alors $m = q_1^{b_1} \cdots q_s^{b_s}$, avec $q_1 < \cdots < q_s$, et donc

$$p_1^{a_1} \cdots p_r^{a_r} = n = m^2 = q_1^{2b_1} \cdots q_s^{2b_s}.$$

L'unicité de l'écriture entraîne $s = r$ et $p_i = q_i$, $a_i = 2b_i$ pour tout i. □

Corollaire 1.2.9 (Euclide) $\sqrt{2} \notin \mathbb{Q}$.

Démonstration. Supposons $\sqrt{2} = a/b$, avec $a, b \in \mathbb{N}^*$. Alors

$$2b^2 = a^2.$$

D'après le lemme précédent, le nombre premier 2 apparaît un nombre pair, resp. impair, de fois dans le terme de droite, resp. de gauche. Ceci contredit l'unicité de la décomposition du nombre $n = a^2 = 2b^2$ en produits de facteurs premiers. Cette contradiction montre que $\sqrt{2} \notin \mathbb{Q}$. □

Remarque 1.2.10 La même démonstration montre que $\sqrt{n}$ est irrationnel si n est un entier ≥ 2 qui n'est pas un carré (en particulier si n est premier).

Définition et proposition 1.2.11 (PPCM (et PGCD))
Soient $a_1, \ldots, a_n \in \mathbb{Z}^*$ et soient $p_1, \ldots, p_r$ l'ensemble des nombres premiers > 0 qui divisent l'un des a_i. On peut donc écrire :

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

où les c_{ij} sont des entiers ≥ 0. Pour $j = 1, \ldots, r$, soient

$$M_j = \max\{c_{1j}, \ldots, c_{nj}\}, \quad m_j = \min\{c_{1j}, \ldots, c_{nj}\}.$$

Posons $M = p_1^{M_1} \cdots p_r^{M_r}$. Alors M est multiple de chaque a_i, et tout multiple commun à tous les a_i est un multiple de M. On dit que M est le PPCM (plus petit commun multiple) des a_i.
D'autre part, $d = p_1^{m_1} \cdots p_r^{m_r}$ est le PGCD des a_i.

Démonstration. Tout ceci résulte de l'unicité de la décomposition en facteurs premiers. □

Définition 1.2.12 (Valuations p-adiques) *On peut éviter, dans ce qui précède, d'avoir à "nommer" les nombres premiers qui divisent l'un des a_i, en introduisant, pour tout nombre premier p, l'application $v_p : \mathbb{Z}^* \to \mathbb{N}$ définie comme suit. Pour tout $n \in \mathbb{Z}^*$, $v_p(n)$ est l'exposant de p dans la décomposition de n en facteurs premiers ; cet exposant étant nul si p n'apparaît pas dans la décomposition (c.-à-d., $p^0 = 1$). On peut alors écrire :*

$$n = \varepsilon(n) \prod_p p^{v_p(n)},$$

le produit étant pris sur tous les nombres premiers > 0. C'est en fait un produit fini, puisqu'il n'y a qu'un nombre fini de facteurs $\neq 1$. Alors, si $a_1, \ldots, a_n \in \mathbb{Z}^*$, leur PPCM est

$$\mathrm{PPCM}(a_1, \ldots, a_n) = \prod_p p^{\max\{v_p(a_i)\}}.$$

L'application v_p s'appelle la valuation p-adique ; il est parfois commode de l'étendre en une application $\mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ en posant $v_p(0) = \infty$.

Définition 1.2.13 *On dit que des entiers $a_1, \ldots, a_n$ sont premiers entre eux s'ils n'ont pas de diviseur commun (autre que ± 1). Ceci équivaut à dire que leur PGCD est 1, et donc qu'il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que $u_1 a_1 + \cdots + u_n a_n = 1$.*

Lemme 1.2.14 *Soient $a, b \in \mathbb{Z}^*$.*

1) *a divise b si et seulement si $v_p(a) \leq v_p(b)$, pour tout p.*

2) *a et b sont premiers entre eux si et seulement si $v_p(b) = 0$ pour tout p tel que $v_p(a) > 0$.*

Démonstration. Laissée au lecteur. □

Proposition 1.2.15 (Lemme de Gauss) *Soient $a, b, c \in \mathbb{Z}$, avec a, b premiers entre eux. Si a divise bc, il divise c.*

Démonstration. Comme a, b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $1 = ua + vb$. On a donc $c = uac + vbc$. Par conséquent, si a divise bc, il divise c. □

Remarque 1.2.16 On peut aussi démontrer le Lemme de Gauss en considérant les décompositions en facteurs premiers de a, b, c et en utilisant l'unicité. On peut aussi utiliser le lemme 1.2.14.

Corollaire 1.2.17 *Tout nombre rationnel $r \neq 0$ s'écrit de façon unique*

$$r = \varepsilon(r)\frac{a}{b},$$

où $\varepsilon(r)$ est le signe de r et où $a, b \in \mathbb{N}^*$ sont premiers entre eux.

Démonstration. Sans perte de généralité, on peut supposer $r > 0$. Alors r s'écrit c/d, pour des entiers $c, d \in \mathbb{N}^*$. En simplifiant les éventuels facteurs

communs à c et d, on obtient une écriture $r = a/b$, où a et b sont premiers entre eux. Ceci prouve l'existence. Montrons l'unicité.

Supposons $a/b = a'/b'$, avec $a', b' > 0$. Alors $ab' = a'b$ et donc, d'après le Lemme de Gauss, a divise a' et b divise b'. On en déduit qu'il existe $c > 0$ tel que $a' = ac$ et $b' = bc$. Donc, si l'on suppose de plus a' et b' premiers entre eux, on obtient $c = 1$, d'où $a' = a$ et $b' = b$. Ceci prouve l'unicité voulue. □

Une conséquence immédiate du Lemme d'Euclide est que, dans $\mathbb{Z}/p\mathbb{Z}$, le produit de deux éléments non nuls est non nul. En fait, la démonstration montre qu'on a le résultat plus fort suivant.

Proposition 1.2.18 *Soit p un nombre premier. Dans $\mathbb{Z}/p\mathbb{Z}$, tout élément non nul est inversible.*

Démonstration. Soit $a \in \mathbb{Z}$ non divisible par p. Alors, le PGCD de p et a est 1, donc il existe $u, v \in \mathbb{Z}$ tels que

$$1 = up + va.$$

Par conséquent, dans $\mathbb{Z}/p\mathbb{Z}$ on a $\dot{a}\dot{v} = \dot{1}$. □

1.3 Solutions entières de $x^2 + y^2 = z^2$

Une autre conséquence du théorème d'Euclide 1.2.7 est la détermination de toutes les solutions entières de l'équation de Pythagore $x^2 + y^2 = z^2$.

Si un triplet d'entiers (a, b, c) est solution de $a^2 + b^2 = c^2$, alors les triplets $(\pm a, \pm b, \pm c)$ sont également solutions. D'autre part, on s'intéresse aux solutions non triviales, c.-à-d., telles que $ab \neq 0$. On peut donc se limiter à chercher les solutions où a, b, c sont > 0.

On dit qu'une solution (a, b, c) est primitive si a, b, c sont premiers entre eux. Si (a, b, c) est une solution arbitraire dont le pgcd est d, on peut écrire $(a, b, c) = (da', db', dc')$ et alors (a', b', c') est une solution primitive. Donc toute solution est multiple d'une solution primitive, et il suffit de déterminer ces dernières.

Proposition 1.3.1 (Euclide) *Les solutions entières de $a^2 + b^2 = c^2$, avec $a, b, c > 0$, sont de la forme suivante (à permutation près de a et b) :*

$$a = 2uvw, \quad b = (u^2 - v^2)w, \quad c = (u^2 + v^2)w,$$

où $u, v, w \in \mathbb{N}^*$.

Démonstration. On peut supposer a, b, c premiers entre eux. Alors a, b ne sont pas tous deux pairs. Comme le carré d'un nombre impair (resp. pair) est congru à 1 (resp. 0) modulo 4, ils ne sont pas non plus tous deux impairs, car sinon $a^2 + b^2$ serait congru à 2 modulo 4 et ne pourrait être un carré. Donc, quitte à échanger a et b, on peut supposer a pair et b, c impairs. Posons $a = 2\alpha$. Alors

$$\alpha^2 = \frac{c+b}{2}\frac{c-b}{2}.$$

Or, les entiers $(c+b)/2$ et $(c-b)/2$ sont premiers entre eux (car un diviseur premier commun diviserait b et c, d'où aussi a). On en déduit que chacun est un carré, d'où $c + b = 2u^2$ et $c - b = 2v^2$, avec $u, v \in \mathbb{N}^*$. Donc

$$b = u^2 - v^2, \quad c = u^2 + v^2, \quad a^2 = c^2 - b^2 = 4u^2v^2,$$

et $a = 2uv$ puisque $a > 0$. □

2 Entiers algébriques

2.1 Somme de deux carrés et entiers de Gauss

Quels sont les entiers qui s'écrivent comme somme de deux carrés d'entiers ? Cette question remonte au moins à Diophante d'Alexandrie, qui vécut dans une période comprise entre l'an 150 et l'an 350. Il écrivit :

> "65 s'écrit de deux façons différentes comme somme de deux carrés : $65 = 7^2 + 4^2 = 8^2 + 1^2$. Ceci est dû au fait que 65 est le produit de 13 et 5, dont chacun est somme de deux carrés."

Ceci semble indiquer que Diophante connaissait l'égalité :

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2, \qquad (\dagger)$$

que l'on peut vérifier par un calcul direct. On verra plus bas un moyen de l'obtenir. Cette égalité montre que, pour qu'un entier $n > 0$ soit somme de deux carrés, il suffit que chacun de ses facteurs premiers le soit. (On verra plus loin une condition nécessaire et suffisante). On a bien sûr $2 = 1^2+1^2$. D'autre part, comme un carré est congru à 0 ou 1 modulo 4, un nombre premier impair de la forme $4n + 3$ ne peut être somme de deux carrés. Fermat a affirmé en 1640 que tout nombre premier de la forme $4n+1$ s'écrivait de façon unique comme somme de deux carrés, mais n'a pas publié sa démonstration. La première preuve connue remonte à Euler, en 1756. Lagrange donna vers 1770 une autre preuve, simplifiée vers 1801 par Gauss. Gauss introduisit et

étudia les nombres de la forme $a+ib$, où $a,b\in\mathbb{Z}$ et $i^2=-1$, qu'on appelle entiers de Gauss.

Pour tout entier de Gauss $z=a+ib$, on définit son conjugué $\overline{z}=a-ib$, et sa norme

$$N(z):=z\overline{z}=a^2+b^2.$$

Soit $v=c+id$ un autre entier de Gauss. On a

$$zv=(a+ib)(c+id)=(ac-bd)+i(bc+ad). \tag{1}$$

On en déduit, premièrement, que $\overline{zv}=\overline{z}\overline{v}$. Ceci entraîne que la norme est multiplicative, c.-à-d.,

$$N(zv)=zv\overline{z}\overline{v}=N(z)N(v)=(a^2+b^2)(c^2+d^2). \tag{2}$$

D'autre part, (1) entraîne $N(zv)=(ac-bd)^2+(bc+ad)^2$. Comparant avec (2), on obtient l'égalité

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(bc+ad)^2. \tag{$\dagger$}$$

Si $z=a+ib$ est inversible, alors $N(z)=1$. On en déduit que les entiers de Gauss inversibles sont ±1 et $\pm i$.

Définition 2.1.1 *On dit qu'un entier de Gauss z est* **irréductible** *s'il est non inversible et si les seuls entiers de Gauss non inversibles qui le divisent sont $\pm z$ et $\pm iz$.*

Proposition 2.1.2 *Tout élément non nul et non inversible de $\mathbb{Z}[i]$ est produit d'éléments irréductibles.*

Démonstration. Montrons par récurrence sur $N(z)$ que tout élément non nul $z\in\mathbb{Z}[i]$ est inversible ou bien produit d'irréductibles. Si $N(z)=1$, alors z égale ±1 ou $\pm i$ et est inversible. Supposons $N(z)\geq 2$ et soit ξ un diviseur de z de norme minimale. Alors ξ est nécessairement irréductible, car si $\xi=uv$ alors l'égalité $N(\xi)=N(u)N(v)$ entraîne, disons, que $N(u)=N(\xi)$ et v est inversible. Posant $z=\xi\xi'$, on a $N(\xi')<N(z)$ et donc ξ' est inversible ou bien produit d'irréductibles. Ceci prouve la proposition. □

Gauss a démontré que les éléments irréductibles de $\mathbb{Z}[i]$ vérifient le Lemme d'Euclide, de sorte que la théorie de la divisibilité dans $\mathbb{Z}[i]$ est analogue à celle dans $\mathbb{Z}$. Plus précisément, Gauss a établi l'existence d'une division euclidienne dans $\mathbb{Z}[i]$.

Proposition 2.1.3 (Division euclidienne dans $\mathbb{Z}[i]$)
Soient $z, u \in \mathbb{Z}[i]$, avec $u \neq 0$. Il existe $\eta, \xi \in \mathbb{Z}[i]$ tels que $z = \eta u + \xi$, et $\sqrt{N(\xi)} < \sqrt{N(u)}$.

Démonstration. On considère les éléments de $\mathbb{Z}[i]$ dans le plan complexe $\mathbb{C} \cong \mathbb{R}^2$. Alors, pour $\alpha, \beta \in \mathbb{Z}[i]$, $\sqrt{N(\beta - \alpha)}$ est la distance euclidienne usuelle entre α et β.

Les multiples ηu, avec $\eta \in \mathbb{Z}[i]$, forment les sommets d'un quadrillage du plan, formé de carrés de côté de longueur $\sqrt{N(u)}$. Un carré arbitraire a pour quatre sommets les points :

$$\eta u, \quad (\eta + 1)u, \quad (\eta + i)u, \quad (\eta + 1 + i)u.$$

Notre élément $z \in \mathbb{Z}[i]$ appartient à (au moins) un tel carré, et la distance de z au sommet le plus proche est $\leq \sqrt{N(u)/2}$ (longueur d'une demi-diagonale). Par conséquent, il existe un multiple ηu tel que $\xi := z - \eta u$ vérifie $\sqrt{N(\xi)} < \sqrt{N(u)}$. La proposition est démontrée. □

Soient $z, z' \in \mathbb{Z}[i]$. Notons

$$\mathbb{Z}[i]z + \mathbb{Z}[i]z' := \{\eta z + \eta' z' \mid \eta, \eta' \in \mathbb{Z}[i]\};$$

cet ensemble est stable par addition, soustraction, et multiplication par un élément arbitraire de $\mathbb{Z}[i]$: c'est un **idéal** de $\mathbb{Z}[i]$, selon la terminologie introduite vers 1870 par Dedekind. Soit d un élément de $\mathbb{Z}[i]z + \mathbb{Z}[i]z'$ de norme minimale. En utilisant la division euclidienne, on montre, comme dans le cas de entiers rationnels, que tout élément de $\mathbb{Z}[i]z + \mathbb{Z}[i]z'$ est multiple de d. (En particulier, d est uniquement déterminé, à multiplication par un inversible près).

Corollaire 2.1.4 *Soient $\xi, z \in \mathbb{Z}[i]$. On suppose ξ irréductible et z non divisible par ξ. Alors il existe $u, v \in \mathbb{Z}[i]$ tels que $u\xi + vz = 1$.*

Démonstration. D'après ce qui précède, il existe $d \in \mathbb{Z}[i]$ tel que

$$d\mathbb{Z}[i] = \xi\mathbb{Z}[i] + z\mathbb{Z}[i].$$

Donc d divise ξ et z. Comme ξ est irréductible, d est inversible, ou bien produit de ξ par un inversible. Comme, par hypothèse, ξ ne divise pas z, le second cas est exclu. Donc d est inversible, d'où $d\mathbb{Z}[i] = \mathbb{Z}[i]$. Le corollaire en découle. □

Théorème 2.1.5 (Gauss) *Le Lemme d'Euclide est valable dans $\mathbb{Z}[i]$, c.-à-d., si un élément irréductible ξ divise un produit zz', il divise z ou z'.*

Démonstration. Tenant compte du corollaire précédent, la démonstration est identique à celle du Lemme d'Euclide dans $\mathbb{Z}$. □

Nous admettrons pour le moment la proposition suivante. Nous la signalons avec une $(*)$ pour indiquer qu'elle fait partie des résultats énoncés, mais non démontrés dans ce chapitre.

Proposition 2.1.6 $(*)$ *Soit $p \in \mathbb{Z}$ un nombre premier > 2. Alors, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1[4]$.*

En admettant cette proposition, voyons comment Dedekind a démontré, vers 1870, le théorème des deux carrés.

Théorème 2.1.7 *Soit $p \in \mathbb{Z}$ un nombre premier > 2. Alors $p = a^2 + b^2$, avec $a, b \in \mathbb{Z}^*$, si et seulement si $p \equiv 1[4]$.*

Démonstration. On a déjà vu que, pour une raison de congruence modulo 4, un entier congru à 3 modulo 4 ne pouvait être somme de deux carrés. On peut donc supposer $p \equiv 1[4]$. Alors, d'après la proposition, il existe un entier $m \in \{1, \ldots, p-1\}$ tel que p divise $m^2 + 1$. Or, dans $\mathbb{Z}[i]$ on a l'égalité

$$m^2 + 1 = N(m + i) = (m + i)(m - i),$$

et p ne divise aucun des facteurs de droite, car

$$\frac{m \pm i}{p} = \frac{m}{p} \pm i\frac{1}{p}$$

n'appartient pas à $\mathbb{Z}[i]$. Comme le Lemme d'Euclide est valable dans $\mathbb{Z}[i]$, on en déduit que p n'est pas irréductible. Donc, il existe $\xi, \eta \in \mathbb{Z}[i]$ non inversibles tels que $p = \xi\eta$, d'où

$$p^2 = N(p) = N(\xi)N(\eta).$$

Comme $N(\xi)$ et $N(\eta)$ sont > 1, on en déduit que $N(\xi) = p = N(\eta)$. Écrivant $\xi = a + ib$, on obtient ainsi

$$p = a^2 + b^2 = \xi\overline{\xi}.$$

De plus cette écriture est unique. En effet, l'égalité $N(\xi) = p$ entraîne que ξ est irréductible. Si $p = c^2 + d^2 = z\overline{z}$, où $z = c + id$, alors z est aussi irréductible et, quitte à changer z en $\overline{z}$, on déduit du Lemme d'Euclide que $z = \xi u$, où u est un élément inversible, c.-à-d., ± 1 ou $\pm i$. Il en résulte que $\{a^2, b^2\} = \{c^2, d^2\}$. □

Corollaire 2.1.8 *Pour qu'un entier $n \geq 2$ soit somme de deux carrés, il faut et il suffit que $v_p(n)$ soit pair, pour tout nombre premier $p > 0$ de la forme $4k + 3$.*

Démonstration. La suffisance résulte du théorème précédent, combiné avec le fait que $2 = 1^2 + 1^2$, l'égalité (†), et le fait que si $m = a^2 + b^2$ alors $mr^2 = (ar)^2 + (br)^2$.

Pour montrer la nécessité, supposons que n soit un contre-exemple minimal, c.-à-d., que $n = x^2 + y^2$ vérifie $v_p(n) = 2k + 1$ pour un nombre premier $p > 0$ congru à 3 modulo 4, et que n soit minimal pour cette propriété. Si p ne divise ni x ni y, alors dans $\mathbb{Z}/p\mathbb{Z}$ on a

$$0 = \dot{x}^2 + \dot{y}^2 = 1 + \left(\frac{\dot{y}}{\dot{x}}\right)^2,$$

donc -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, ce qui contredit la proposition 2.1.6. Par conséquent, on peut supposer que p divise x. Alors p divise y^2 et donc y (d'après le Lemme d'Euclide), et donc p^2 divise n. Mais alors $v_p(n) = 2k+1 \geq 3$ et n/p^2 est encore un contre-exemple, puisque $n/p^2 = (x/p)^2 + (y/p)^2$ et $v_p(n/p^2) = 2k - 1 \geq 1$. Ceci contredit la minimalité de n. Le corollaire est démontré. □

Remarque 2.1.9 Une démonstration plus conceptuelle du corollaire, basée sur la détermination des éléments irréductibles de $\mathbb{Z}[i]$ et de leur norme, se trouve dans [Elk], Ch.X, Ex.2.

2.2 Les anneaux de nombres $\mathbb{Z}[\sqrt{n}\,]$

Définition 2.2.1 *On dira qu'un sous-ensemble A de $\mathbb{C}$ est un* **anneau** *(de nombres), s'il contient 1 et est stable par addition, soustraction et multiplication.*

Définition 2.2.2 *Soit A un anneau de nombres. On dit qu'un élément $p \in A$ est* **irréductible** *s'il est non inversible et si les seuls éléments de A qui divisent p sont inversibles ou de la forme pu, avec u inversible.*

Ceci équivaut à dire que p est non inversible et vérifie la propriété suivante : si $p = ab$, avec $a, b \in A$, alors a ou b est inversible.

Ainsi, par exemple, l'ensemble $\mathbb{Z}[i]$ des entiers de Gauss est un anneau de nombres. De façon plus générale, 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). On peut considérer l'anneau de nombres

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

où $\sqrt{n}$ désigne l'une quelconque des racines carrées de n dans $\mathbb{C}$. Cet ensemble contient 1 et est clairement stable par addition et soustraction. Il est aussi stable par multiplication, puisque

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

C'est donc bien un anneau de nombres. Pour $u = a + \sqrt{n}\, b$, on définit, comme pour les entiers de Gauss,

$$\bar{u} = a - \sqrt{n}\, b, \qquad N(u) = u\bar{u} = a^2 - nb^2.$$

On déduit de $(*)$ que $\overline{uv} = \bar{u}\bar{v}$ et $N(uv) = N(u)N(v)$. Il en résulte que u est inversible si et seulement si $N(u) = \pm 1$. En utilisant la (valeur absolue de la) norme, on établit, exactement comme pour $\mathbb{Z}[i]$, la proposition suivante.

Proposition 2.2.3 *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. Avant de détailler ces exemples, il est utile d'introduire la définition suivante.

Définition 2.2.4 *Soit A un anneau de nombres. On dit que A est* **factoriel** *si les deux conditions ci-dessous sont satisfaites :*

1) *Tout élément de A, distinct de 0 et non inversible, est un produit fini d'éléments irréductibles.*

2) *Tout élément irréductible p vérifie le Lemme d'Euclide, c.-à-d., si p divise un produit ab, il divise a ou b.*

Exemples 2.2.5 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 $\mathbb{Z}[\sqrt{-5}\,]$, $N(a+\sqrt{-5}\,b) = a^2+5b^2$ 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 $N(a+\sqrt{-5}\,b) = a^2-5b^2$. 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 le 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

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

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].

2.3 Les anneaux $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

Soit $j = (-1 + i\sqrt{3})/2 = \exp(2i\pi/3)$; c'est une racine cubique de 1, et une racine du polynôme $X^2 + X + 1$. D'autre part, posons $\theta = (1 + \sqrt{5})/2$. C'est une racine du polynôme $X^2 - X - 1$.

Le défaut d'unicité de la factorisation dans $\mathbb{Z}[\sqrt{-3}]$ (resp., dans $\mathbb{Z}[\sqrt{5}]$) peut être pallié en élargissant cet anneau en l'anneau de nombres

$$\mathbb{Z}[j] = \{a + jb \mid a, b \in \mathbb{Z}\},$$

resp.

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

Chacun de ces ensembles contient 1, et est stable par addition et soustraction, et aussi par multiplication car $j^2 = -j - 1$ (resp. $\theta^2 = \theta + 1$). Ce sont donc des anneaux de nombres. Le premier contient $\mathbb{Z}[\sqrt{-3}]$ car $i\sqrt{-3} = 2j + 1$, et le second contient $\sqrt{5} = 2\theta - 1$.

On peut montrer que $\mathbb{Z}[j]$ et $\mathbb{Z}[\theta]$ sont tous deux factoriels. Pour $\mathbb{Z}[\theta]$, on renvoie le lecteur intéressé à [Sa, Ex. V.7.a)]. Pour $\mathbb{Z}[j]$, un argument géométrique élémentaire montre l'existence d'une division euclidienne. Plus précisément, désignant par $\rho(z) = \sqrt{z\overline{z}}$ la norme d'un nombre complexe z, on a la proposition suivante.

Proposition 2.3.1 (Division euclidienne dans $\mathbb{Z}[j]$)
Soient $z, u \in \mathbb{Z}[j]$ avec $u \neq 0$. Il existe $\eta, \xi \in \mathbb{Z}[j]$ tels que $z = \eta u + \xi$, et $\rho(\xi) < \rho(u)$.

Démonstration. Les multiples $(a + jb)u$ de u forment les sommets d'une triangulation du plan formée de triangles équilatéraux de côté $\rho(u)$. Chaque point d'un triangle est à une distance $\leq \rho(u)/\sqrt{3} < \rho(u)$ du sommet le plus proche. □

Comme pour les entiers de Gauss, on en déduit, exactement comme dans la preuve du corollaire 2.1.4 et du théorème 2.1.5, le corollaire suivant.

Corollaire 2.3.2 *$\mathbb{Z}[j]$ est factoriel.*

Donc, en quelque sorte, on peut dire que le défaut de factorialité observé dans $\mathbb{Z}[\sqrt{n}]$, pour $n = -3$ et $n = 5$, provient du fait que l'on n'a pas considéré le "bon anneau", qui se trouve être, dans ce cas, l'anneau

$$\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{n}}{2}.$$

Par contre, on peut montrer que $\mathbb{Z}[\sqrt{-5}\,]$ ne peut pas être élargi en un sous-anneau A de $\mathbb{Q}[\sqrt{-5}\,] = \{a + \sqrt{-5}\,b \mid a, b \in \mathbb{Q}\}$, qui soit engendré comme $\mathbb{Z}$-module par un nombre fini d'éléments. C.-à-d., on peut démontrer la

Proposition 2.3.3 (∗) *Soit A un sous-anneau de $\mathbb{Q}[\sqrt{-5}\,]$, contenant $\sqrt{-5}$. On suppose qu'il existe $a_1, \ldots, a_r \in A$ tels que tout élément de A s'écrive $n_1a_1 + \cdots + n_ra_r$, avec $n_i \in \mathbb{Z}$. Alors $A = \mathbb{Z}[\sqrt{-5}\,]$.*

Ceci suggère les questions suivantes : que sont les anneaux $\mathbb{Z}[(1+\sqrt{n}\,)/2]$, pour $n = -3$ et $n = 5$? Pourquoi apparaissent-ils, et pourquoi le cas de $\mathbb{Z}[\sqrt{-5}\,]$ est-il différent ? La réponse à ces questions se trouve dans la notion de nombre algébrique entier, introduite par Dedekind en 1871 (voir [De]).

2.4 Entiers algébriques

Définition 2.4.1 *Soit $z \in \mathbb{C}$.*

1) *On dit que z est un* **nombre algébrique** *s'il existe un polynôme unitaire $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ dans $\mathbb{Q}[X]$ tel que $P(z) = 0$, c.-à-d., si z est racine d'une équation*

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0,$$

avec les a_i dans $\mathbb{Q}$.

2) *On dit de plus que z est un* **nombre algébrique entier**, *ou simplement un* **entier algébrique**, *s'il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ tel que $P(z) = 0$, c.-à-d., si z est racine d'une équation*

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0,$$

avec les a_i dans $\mathbb{Z}$.

Exemples 2.4.2 1) Tout entier rationnel $n \in \mathbb{Z}$ est un entier algébrique : il est racine du polynôme $X - n$.

2) Le rationnel $\frac{1}{2}$ n'est pas un entier algébrique. Plus généralement, si r est un élément de $\mathbb{Q}$ n'appartenant pas à $\mathbb{Z}$, alors r n'est pas un entier algébrique. **Exercice :** démontrer cette assertion. Indication : écrire $r = a/b$, avec a et b premiers entre eux, et supposer qu'il existe P unitaire dans $\mathbb{Z}[X]$ tel que $P(a/b) = 0$; en déduire une contradiction.

3) Pour tout $n \in \mathbb{Z}^*$, les deux racines $\pm\sqrt{n}$ du polynôme $X^2 - n$ sont des entiers algébriques. Si $n = 4k + 1$, il en est de même de $(1 + \sqrt{n}\,)/2$, qui est racine du polynôme $X^2 - X - k$.

Théorème 2.4.3 (Dedekind (1871)) *L'ensemble $\mathcal{A}$ de tous les entiers algébriques est un anneau.*

Démonstration. $\mathcal{A}$ contient 1. Soient $\alpha, \beta \in \mathcal{A}$. Par hypothèse, il existe des entiers $a_1, \ldots, a_r$ et $b_1, \ldots, b_s$ tels que

$$(*) \qquad \left\{ \begin{array}{rcl} \alpha^r & = & a_1\alpha^{r-1} + \cdots + a_r; \\ \beta^s & = & b_1\beta^{s-1} + \cdots + b_s. \end{array} \right.$$

Posons $n = rs$ et désignons par $\omega_1, \omega_2, \ldots, \omega_n$ l'ensemble des monômes

$$\alpha^i\beta^j, \qquad 0 \leq i \leq r-1,\ 0 \leq j \leq s-1,$$

en choisissant la numérotation de sorte que ω_1 soit le monôme $\alpha^0\beta^0 = 1$.

Soit η l'un des trois nombres $\alpha+\beta$, $\alpha-\beta$, ou $\alpha\beta$. On déduit des égalités $(*)$ que chacun des n produits $\eta\omega_i$ peut s'exprimer comme une combinaison linéaire

$$(E_i) \qquad \eta\omega_i = k_{i1}\omega_1 + \cdots + k_{in}\omega_n,$$

à coefficients $k_{ij} \in \mathbb{Z}$. Soustrayant $\eta\omega_i$ aux deux membres de l'égalité (E_i), on obtient que le système linéaire suivant, à coefficients dans $\mathbb{C}$,

$$\left\{ \begin{array}{rcrcrcl} (k_{11}-\eta)x_1 & + & k_{12}x_2 & + \cdots + & k_{1n}x_n & = & 0 \\ k_{21}x_1 & + & (k_{22}-\eta)x_2 & + \cdots + & k_{2n}x_n & = & 0 \\ \cdots & & \cdots & \cdots & \cdots & & \cdots \\ k_{n1}x_1 & + & k_{n2}x_2 & + \cdots + & (k_{nn}-\eta)x_n & = & 0 \end{array} \right.$$

admet la solution non nulle $x_i = \omega_i$, pour $i = 1, \ldots, n$. On en déduit que le déterminant de ce système, c.-à-d., le déterminant suivant, est nul :

$$\begin{vmatrix} k_{11}-\eta & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22}-\eta & \cdots & k_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ k_{n1} & k_{n2} & \cdots & k_{nn}-\eta \end{vmatrix} = 0.$$

En développant ce déterminant, on obtient une équation

$$\eta^n + e_1\eta^{n-1} + \cdots + e_{n-1}\eta + e_n = 0,$$

avec les e_i dans $\mathbb{Z}$. Donc η est un entier algébrique, pour $\eta = \alpha+\beta$, $\alpha-\beta$, ou $\alpha\beta$. Ceci montre que l'ensemble $\mathcal{A}$ des entiers algébriques est un anneau. Le théorème est démontré. □

Corollaire 2.4.4 *L'ensemble $\mathcal{K} = \overline{\mathbb{Q}}$ des nombres algébriques est un* **corps** (c.-à-d., un anneau dans lequel tout élément non nul admet un inverse).

Démonstration. D'abord, la même démonstration que précédemment, où cette fois les k_{ij} et les e_i sont dans $\mathbb{Q}$, montre que $\mathcal{K}$ est un anneau. Il reste à montrer que tout élément $\alpha \neq 0$ de $\mathcal{K}$ est inversible.

Soit $P \in \mathbb{Q}[X]$ un polynôme unitaire tel que $P(\alpha) = 0$, et de degré minimal pour cette propriété. Écrivons

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$

et désignons par Q le polynôme unitaire $(P - a_0)/X = X^{n-1} + \cdots + a_1$.

Alors $a_0 \neq 0$ car sinon on aurait $\alpha Q(\alpha) = 0$ et donc $Q(\alpha) = 0$, contredisant la minimalité de $n = \deg(P)$. Donc a_0 est un rationnel non nul, et l'égalité $P(\alpha) = 0$ se récrit $\alpha Q(\alpha) = -a_0$. Ceci montre que l'élément

$$-\frac{Q(\alpha)}{a_0} = \frac{-1}{a_0}\alpha^{n-1} - \cdots - \frac{a_1}{a_0},$$

qui appartient à l'anneau $\mathcal{K}$ (car $\mathcal{K}$ contient $\mathbb{Q}$ et α), est l'inverse de α. Le corollaire est démontré. □

De plus, $\mathcal{A}$ est **intégralement clos** dans $\mathbb{C}$, et $\mathcal{K} = \mathbb{Q}$ est **algébriquement clos** dans $\mathbb{C}$, c.-à-d., on a la proposition suivante.

Proposition 2.4.5 *Soient $\alpha_1, \ldots, \alpha_n$ des éléments de $\mathcal{A}$ (resp., de $\mathcal{K}$), et soit $\eta \in \mathbb{C}$ une racine de l'équation*

$$X^n + \alpha_1 X^{n-1} + \cdots + \alpha_{n-1}X + \alpha_n = 0. \tag{1}$$

Alors, $\eta \in \mathcal{A}$ (resp., $\eta \in \mathcal{K}$).

Démonstration. On va prouver la première assertion, la seconde se traitant de la même manière. Par hypothèse, il existe des entiers

$$a_{11}, \ldots, a_{1r_1}, \quad a_{21}, \ldots, a_{2r_2}, \quad \ldots \quad a_{n1}, \ldots, a_{nr_n}$$

dans $\mathbb{Z}$ tels que

$$\left\{ \begin{array}{rcl} \alpha_1^{r_1} & = & a_{11}\alpha_1^{r_1-1} + \cdots + a_{1r_1}, \\ \cdots & & \cdots \\ \alpha_n^{r_n} & = & a_{n1}\alpha_n^{r_n-1} + \cdots + a_{nr_n}. \end{array} \right. \tag{2}$$

Posons $N = n\, r_1 \cdots r_n$ et désignons, comme précédemment, par $\omega_1, \ldots, \omega_N$ les monômes

$$\eta^i \alpha_1^{i_1} \cdots \alpha_n^{i_n},$$

pour $0 \leq i \leq n-1$ et $0 \leq i_j \leq r_j - 1$, pour $j = 1, \ldots, n$; la numérotation étant choisie de sorte que $\omega_1 = 1$.

En utilisant les égalités (1) et (2), on obtient que chacun des N produits $\eta\omega_i$ peut s'exprimer comme une combinaison linéaire

$$\eta\omega_i = k_{i1}\omega_1 + \cdots + k_{iN}\omega_N,$$

à coefficients $k_{ij} \in \mathbb{Z}$. On en déduit, comme dans la preuve du théorème 2.4.3, que le déterminant suivant est nul :

$$\begin{vmatrix} k_{11} - \eta & k_{12} & \cdots & k_{1N} \\ k_{21} & k_{22} - \eta & \cdots & k_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ k_{N1} & k_{N2} & \cdots & k_{NN} - \eta \end{vmatrix} = 0.$$

En développant ce déterminant, on obtient une équation

$$\eta^N + e_1\eta^{N-1} + \cdots + e_{N-1}\eta + e_N = 0,$$

avec les e_i dans $\mathbb{Z}$. Donc η est un entier algébrique, c.-à-d., $\eta \in \mathcal{A}$. Ceci montre que l'anneau $\mathcal{A}$ est intégralement clos dans $\mathbb{C}$, et la seconde assertion de la proposition s'obtient de façon exactement analogue. □

Remarque 2.4.6 Une conséquence de la proposition précédente est que l'anneau $\mathcal{A}$ ne contient aucun élément irréductible. En effet, soit $\alpha \in \mathcal{A}$ un élément non inversible (par exemple, $\alpha = 2$), et soit β l'une des racines de l'équation $x^2 = \alpha$. Alors β appartient à $\mathcal{A}$ (d'après la proposition précédente), et β est non inversible (car sinon α le serait). Par conséquent, l'écriture $\alpha = \beta^2$ montre que α n'est pas irréductible.

La remarque précédente montre que, en un certain sens, $\mathcal{A}$ est "trop gros" pour posséder des éléments irréductibles. De façon plus précise, dans un anneau commutatif A (ou, si l'on veut, dans un sous-anneau A de $\mathbb{C}$), l'existence d'éléments irréductibles et d'une décomposition de tout élément comme produit fini d'irréductibles, est une conséquence d'une certaine propriété de "petitesse" de A, que l'on va introduire dans le paragraphe suivant.

2.5 Anneaux noethériens

Définition 2.5.1 *Soit A un anneau commutatif (ou, si l'on veut, un sous-anneau de $\mathbb{C}$).*

1) Un **idéal** *de A est un sous-ensemble non vide I de A, stable par addition et soustraction, et vérifiant la propriété suivante (stabilité par multiplication par tout élément de A) : pour tout $x \in I$ et tout $a \in A$, $ax \in I$.*

2) **Par exemple**, *pour tout $a \in A$, l'ensemble $Aa = \{ba \mid b \in A\}$ des multiples de a, est un idéal. On l'appelle l'idéal engendré par a et on le note (a). Les idéaux de ce type s'appellent les idéaux* **principaux** *de A.*

3) On dit que A est **noethérien** *si toute suite croissante d'idéaux de A est stationnaire, c.-à-d., si la propriété suivante est vérifiée : pour chaque suite croissante*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq$$

d'idéaux de A, il existe un entier n_0 tel que $I_{n_0} = I_n$ pour tout $n \geq n_0$.

La définition 3) ci-dessus peut se reformuler de la façon suivante, plus abstraite, mais extrêmement utile en pratique, et qu'il faut donc bien assimiler.

Définition 2.5.2 *Soit A un anneau commutatif (ou, si l'on veut, un sous-anneau de $\mathbb{C}$).*
1) Soit $\mathcal{I}$ un ensemble non-vide d'idéaux de A. On dit qu'un idéal I de A appartenant à l'ensemble $\mathcal{I}$ est un **élément maximal de** *$\mathcal{I}$ (pour la relation d'inclusion), s'il vérifie la propriété suivante :*

> *Si J est un idéal de A appartenant à $\mathcal{I}$ et si $I \subseteq J$, alors $I = J$. En d'autres termes, I n'est pas strictement contenu dans un idéal de A appartenant à l'ensemble $\mathcal{I}$.*

2) Considérons alors la propriété $(*)$ ci-dessous (qui porte sur l'anneau A) :

> $(*)$ **tout** *ensemble non-vide $\mathcal{I}$ d'idéaux de A admet un élément maximal, c.-à-d., étant donné un ensemble non-vide quelconque $\mathcal{I}$ d'idéaux de A, il existe au moins un idéal I de A appartenant à $\mathcal{I}$ et vérifiant la propriété : si $J \in \mathcal{I}$ et $I \subseteq J$ alors $I = J$.*

Lemme 2.5.3 *Soit A un anneau commutatif. Alors A est noethérien si, et seulement si, il vérifie la propriété $(*)$.*

Démonstration. Supposons $(*)$ vérifiée, et soit

$$(S) \qquad I_1 \subseteq I_2 \subseteq \cdots$$

une suite croissante d'idéaux de A. Considérons l'ensemble d'idéaux $\mathcal{I} = \{I_n\}_{n \geq 1}$. D'après l'hypothèse $(*)$, cet ensemble admet un élément maximal,

disons I_{n_0}. Soit $n \geq n_0$. Alors $I_n \in \mathcal{I}$ et $I_{n_0} \subseteq I_n$, et donc la maximalité de I_{n_0} dans $\mathcal{I}$ entraîne $I_{n_0} = I_n$. Ceci montre que la suite (S) est stationnaire à partir du cran n_0.

Réciproquement, supposons A noethérien au sens de la définition 2.5.1.3), et soit $\mathcal{I}$ un ensemble non-vide d'idéaux de A. Supposons que $\mathcal{I}$ ne possède pas d'élément maximal. Soit I_1 un idéal de A appartenant à $\mathcal{I}$; comme, par hypothèse, ce n'est pas un élément maximal de $\mathcal{I}$, il existe un idéal I_2 de A appartenant à $\mathcal{I}$ et tel que $I_1 \subset I_2$ (inclusion stricte). Toujours par l'hypothèse, I_2 n'est pas un élément maximal de $\mathcal{I}$, donc il existe un idéal I_3 de A appartenant à $\mathcal{I}$ et tel que $I_2 \subset I_3$ (inclusion stricte). On construit ainsi, par récurrence, une suite strictement croissante

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

d'idéaux de $\mathcal{A}$ (appartenant à $\mathcal{I}$), et ceci contredit l'hypothèse que A est noethérien. Cette contradiction montre que si A est noethérien, il vérifie la propriété $(*)$. Le lemme est démontré. □

Comme écrit plus haut, la propriété $(*)$ est plus abstraite (et plus difficile à assimiler) mais elle est extrêmement utile dans la pratique, comme on va le voir dans le paragraphe suivant.

2.6 Éléments irréductibles dans un anneau intègre noethérien

Définition 2.6.1 *Soit A un anneau commutatif. On dit que A est* **intègre** *si le produit de deux éléments non nuls est non nul.*

Il est clair que tout sous-anneau d'un anneau intègre est intègre. Par exemple, si A est un "anneau de nombres", c.-à-d., un sous-anneau de $\mathbb{C}$, alors A est intègre.

Exemple 2.6.2 L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre, car $\dot{2} \times \dot{3} = 0$. **Exercice :** à quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ?

Définition 2.6.3 *Soit A un anneau commutatif intègre (ou, si l'on veut, un sous-anneau de $\mathbb{C}$). Un élément $a \in A$ est dit* **irréductible** *s'il est non nul, non inversible, et vérifie la propriété suivante :*

(†) **Si** $a = bc$**, alors** a **ou** b *est inversible.*

Proposition 2.6.4 *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 $A \setminus \{0\}$ est inversible, il n'y a rien à montrer. Sinon, considérons l'ensemble d'idéaux suivant :

$$\mathcal{I} := \{(a) \mid a \in A \text{ est non inversible et n'est pas un produit fini d'éléments irréductibles}\}$$

La proposition sera démontrée si on montre que cet ensemble $\mathcal{I}$ est vide.

Supposons $\mathcal{I}$ non vide. Il admet alors un élément maximal (a), où $a \in A$ 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 $d \in A$ 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 $\mathcal{I}$, 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 $(a) \in \mathcal{I}$, et cette contradiction montre que $\mathcal{I} = \emptyset$. La proposition est démontrée. □

Références citées dans ce chapitre

(les * indiquent des livres cités pour des références historiques)

[Elk], [Sa], [De]*, [St]*

1 Variétés algébriques et théorème des zéros

Version du 23 octobre 2005

Un autre moteur important pour le développement de l'algèbre commutative (la théorie des anneaux, idéaux et modules), est l'étude des variétés algébriques, c.-à-d., de l'ensemble des solutions dans $\mathbb{C}^n$ d'un ensemble fini de polynômes en n variables $P_1, \ldots, P_m$.

Commençons par le cas $n = 1$, c.-à-d., le cas des polynômes en une variable. On suppose connue la division euclidienne dans $\mathbb{C}[X]$.

3 $\mathbb{C}$ est algébriquement clos

3.1 L'énoncé du théorème

L'assertion du titre signifie que tout polynôme $P \in \mathbb{C}[X]$, non constant, admet une racine dans $\mathbb{C}$, c.-à-d., qu'il existe $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$.

Théorème 3.1.1 *$\mathbb{C}$ est algébriquement clos, c.-à-d., tout polynôme $P \in \mathbb{C}[X]$, non constant, admet une racine dans $\mathbb{C}$.*

Ce résultat est parfois appelé, surtout dans la littérature anglaise, "Théorème fondamental de l'algèbre". Dans la littérature française, il est souvent appelé "Théorème de d'Alembert". L'auteur de ces notes n'est pas compétent quant à la question de savoir si la preuve proposée par d'Alembert était complète dans tous ses détails. Quatre autres preuves ont été proposées par Gauss, dont l'une au moins était tout-à-fait complète (mais longue et compliquée), voir par exemple le livre de van der Waerden [vdW].

Nous allons donner une démonstration qui n'utilise que des méthodes élémentaires d'analyse ; elle est attribuée à Argand, en 1814 (voir [Esc, p.5]),

bien que la notion de compacité, utilisée pour assurer que le minimum est atteint, n'ait été dégagée que dans la deuxième moitié du 19e siècle (entre autre, par Weierstrass). Bref, les premières preuves simples et complètes de ce théorème datent probablement des années 1850 ou 1860. Pour une autre démonstration, plus algébrique (et un peu moins élémentaire), voir [Sa, Chap.II, Appendice].

3.2 La démonstration d'Argand

Soit $P \in \mathbb{C}[X]$ un polynôme de degré $n \geq 1$. Sans perte de généralité, on peut supposer P *unitaire*, c.-à-d., de coefficient dominant égal à 1. Écrivons

$$P = X^n + a_1 X^{n-1} + \cdots + a_n.$$

Raisonnons par l'absurde et supposons que P ne s'annule pas sur $\mathbb{C}$. Alors, en particulier, $a_n \neq 0$. Notons $|\cdot|$ la norme usuelle sur $\mathbb{C}$, c.-à-d., si $z = x+iy$ alors

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2+y^2}.$$

Comme $\lim_{|z|\to+\infty} |P(z)| = +\infty$, il existe $R > 0$ tel que

$$|z| \geq R \Rightarrow |P(z)| \geq |a_n|.$$

Explicitement, on peut prendre $R = \max\{1, 2na\}$, où $a = \max_{i=1}^n |a_i|$. En effet, pour $|z| \geq R$ et $d = 1, \ldots, n$, on a $|z^d| \geq |z| \geq 2na$ d'où

$$\left|\sum_{d=1}^n \frac{a_d}{z^d}\right| \leq \sum_{d=1}^n \frac{|a_d|}{2na} \leq \frac{1}{2}.$$

Comme $|u+v| \geq |u| - |v|$, on obtient que, pour $|z| \geq R$, on a

$$|P(z)| = |z^n| \cdot \left|1 + \sum_{d=1}^n \frac{a_d}{z^d}\right| \geq 2na(1 - \frac{1}{2}) = na \geq n|a_n|.$$

Comme le disque D de centre 0 et de rayon R est compact, la fonction continue $f : z \mapsto |P(z)|$ y atteint son minimum r_0, et $r_0 > 0$ puisqu'on a supposé que P ne s'annule pas. Comme de plus

$$r_0 \leq |P(0)| = |a_n| \leq f(z), \quad \forall z \notin D,$$

alors r_0 est le minimum de f sur $\mathbb{C}$ tout entier. Soit $z_0 \in D$ tel que $f(z_0) = r_0$. En remplaçant z par $z + z_0$ et $P(z)$ par $Q(z) := P(z_0)^{-1}P(z + z_0)$, on se ramène au cas où $z_0 = 0$ et où $Q(0) = 1$ est le minimum de $g = |Q|$ sur $\mathbb{C}$.

Observons que Q est, comme P, de degré n. Notons k l'ordre d'annulation en 0 de $Q-1$. On peut alors écrire

$$Q(X) = 1 + b_k X^k + \cdots + b_n X^n.$$

avec $b_k b_n \neq 0$. Écrivons $b_k = re^{i\theta}$, avec $r > 0$ et $\theta \in [0, 2\pi[$ et, pour $\varepsilon \in \mathbb{R}_+^*$, posons

$$z_\varepsilon = \varepsilon e^{i(\pi-\theta)/k}, \quad \text{et} \quad q(\varepsilon) = Q(z_\varepsilon).$$

Comme $e^{i\pi} = -1$, alors

$$q(\varepsilon) = 1 - r\varepsilon^k + \varepsilon^k h(\varepsilon),$$

où $h(\varepsilon) = \sum_{j=1}^n b_j z_\varepsilon^j$. Comme $\lim_{\varepsilon\to 0} h(\varepsilon) = 0$, il existe $\varepsilon_0 \in]0,1[$ tel que

$$\forall \varepsilon \leq \varepsilon_0, \qquad |h(\varepsilon)| \leq \frac{r}{2}.$$

On a alors

$$|Q(z_{\varepsilon_0})| = |1 - r\varepsilon_0^k + \varepsilon_0^k h(\varepsilon_0)| \leq 1 - r\varepsilon_0^k + \frac{r}{2}\varepsilon_0^k = 1 - \frac{r}{2}\varepsilon_0^k < 1.$$

Ceci contredit l'hypothèse que $1 = Q(0)$ était le minimum de $g = |Q|$ sur $\mathbb{C}$. Cette contradiction montre que l'hypothèse que P ne s'annule pas sur $\mathbb{C}$ est impossible. Ceci achève la démonstration du théorème.

3.3 La cas de plusieurs polynômes

Soit $P_1, \ldots, P_m \in \mathbb{C}[X]$ des polynômes en une variable, non nuls. On se demande quels sont les zéros communs à $P_1, \ldots, P_m$.

Définition 3.3.1 *On note $(P_1, \ldots, P_m)$ l'ensemble des polynômes de la forme*

$$A_1 P_1 + \cdots + A_m P_m,$$

où $A_i \in \mathbb{C}[X]$. On l'appelle **l'idéal** *engendré par $P_1, \ldots, P_m$.*

Lemme 3.3.2 *Les zéros communs à $P_1, \ldots, P_m$ sont aussi zéros communs de tous les éléments de l'idéal $(P_1, \ldots, P_m)$.*

Démonstration. C'est évident. □

Proposition 3.3.3 *Les propriétés de la division euclidienne dans* $\mathbb{C}[X]$ *entraînent qu'il existe un unique polynôme unitaire* $Q \in \mathbb{C}[X]$ *tel que l'idéal* $(P_1, \ldots, P_m)$ *soit l'ensemble des multiples* AQ*, pour* $A \in \mathbb{C}[X]$*. Par conséquent, l'ensemble des zéros communs à* $P_1, \ldots, P_m$ *est exactement l'ensemble des zéros de* Q*. Cet ensemble est non-vide ssi* $Q \neq 1$*, c.-à-d., ssi* $1 \notin (P_1, \ldots, P_m)$*.*

Démonstration. Posons $I = (P_1, \ldots, P_m)$. Soit $Q = A_1P_1 + \cdots + A_mP_m$ un élément non nul de I de degré minimum d. Quitte à multiplier Q par une constante non nulle, on peut supposer Q unitaire.

Soit $P \in I$, non nul. On peut effectuer la division euclidienne

$$P = AQ + B,$$

où $\deg B < \deg Q$. (On convient que le polynôme nul a pour degré $-\infty$). Comme $B = P - AQ$, alors $B \in I$ et la minimalité de $d = \deg Q$ entraîne que $B = 0$, d'où $P = AQ$.

Ceci montre que tout élément de I est multiple de Q. De plus, Q est l'unique polynôme unitaire de I de degré d. En effet, si Q' vérifie la même condition, alors $Q' = AQ$, et A est nécessairement de degré 0, c.-à-d., une constante, et $A = 1$ car Q et Q' sont supposés unitaires.

Comme $Q = A_1P_1 + \cdots + A_mP_m$, alors tout zéro commun aux P_i est aussi zéro de Q, et la réciproque est vraie puisque chaque P_i est un multiple QB_i de Q.

Enfin, comme $\mathbb{C}$ est algébriquement clos, cet ensemble de zéros est non vide ssi Q est non constant, c.-à-d., ssi $Q \neq 1$. □

Remarque 3.3.4 Étant donnés des polynômes $P_1, \ldots, P_m$, la détermination explicite des zéros communs (ou simplement la question de savoir si cet ensemble est non vide) est une question algorithmique non triviale. Voir par exemple le cours de P.-V. Koseleff, Introduction à l'algorithmique algébrique (MM048).

4 Le théorème des zéros

4.0 Courbes algébriques

L'ensemble des zéros dans $\mathbb{C}^2$ d'un polynôme à deux variables, non constant, $P \in \mathbb{C}[X, Y]$ s'appelle une courbe algébrique. Des exemples de courbes

algébriques sont :

$$\begin{aligned} C_1 &= \{(x,y) \in \mathbb{C}^2 \mid x^2 - y^2 = 1\}, \\ C_2 &= \{(x,y) \in \mathbb{C}^2 \mid y(x-y) = 0\}, \\ C_3 &= \{(x,y) \in \mathbb{C}^2 \mid y(x^2 - y^2 - 1) = 0\}. \end{aligned}$$

La courbe C_2 est formée de deux "morceaux" : les droites $y = 0$ et $y = x$. On peut montrer que la courbe C_1 est formée d'un seul morceau (c.-à-d., que le polynôme $X^2 - Y^2 - 1$ est irréductible), et que la courbe C_3 est formée de deux morceaux : la courbe C_1 et la droite $y = 0$. D'autre part, l'intersection de C_2 et C_3 est la droite $y = 0$, tandis que l'intersection de C_1 et C_2 est formée des deux points $(\pm 1, 0)$.

4.1 Variétés algébriques

L'analogue multidimensionnel est la notion de variété algébrique dans $\mathbb{C}^n$: c'est l'ensemble des zéros communs à une collection de polynômes en n variables $P_1, \ldots, P_m \in \mathbb{C}[X_1, \ldots, X_n]$.

Définition 4.1.1 *1) On note $V(P_1, \ldots, P_m)$ l'ensemble de ces zéros communs.*

2) On note $(P_1, \ldots, P_m)$ l'ensemble des polynômes de la forme

$$A_1 P_1 + \cdots + A_m P_m,$$

*où $A_i \in \mathbb{C}[X_1, \ldots, X_n]$, et on l'appelle l'***idéal engendré** *par $P_1, \ldots, P_m$.*

Lemme 4.1.2 *Les zéros communs à $P_1, \ldots, P_m$ sont aussi zéros communs de tous les éléments de l'idéal $(P_1, \ldots, P_m)$.*

Démonstration. C'est évident. □

On a alors le théorème fondamental suivant, qui sera démontré plus loin. Le lecteur intéressé peut en trouver une démonstration dans [BM, §VI.2] ou [Elk, §X.4].

Théorème 4.1.3 (Théorème des zéros de Hilbert)
Soit $F \in \mathbb{C}[X_1, \ldots, X_n]$ s'annulant en tout point de $V(P_1, \ldots, P_m)$. Alors il existe $r \geq 1$ et $A_1, \ldots, A_m \in \mathbb{C}[X_1, \ldots, X_n]$ tels que

$$F^r = A_1 P_1 + \cdots + A_m P_m.$$

En particulier, $V(P_1, \ldots, P_m) = \emptyset$ ssi $1 \in (P_1, \ldots, P_m)$.

Le théorème des zéros de Hilbert (1893) porte sur l'idéal engendré par $P_1, \ldots, P_m$, et sa démonstration utilise la notion d'idéal et une propriété de finitude établie par lui en 1890. Emmy Noether a ensuite découvert (en 1919) que cette propriété de finitude a des conséquences fondamentales dans la théorie des anneaux et idéaux. Ceci a donné lieu à la notion d'anneau (ou de module) noethérien, et au principe de "démonstration par récurrence noethérienne". Pour les lecteurs lisant l'allemand, voir par exemple le §1.3 de [Kru].

4.2 Vers la suite du cours

Après cet aperçu des deux motivations historiques (théorie algébrique des nombres et idéaux des anneaux de polynômes) qui ont servi de base au développement de l'algèbre commutative, on va maintenant introduire et développer les concepts qui ont été esquissés jusqu'à présent : anneaux, idéaux, modules, anneaux noethériens, anneaux euclidiens, principaux et factoriels.

Références citées dans ce chapitre

(les * indiquent des livres cités pour des références historiques)

[BM], [Elk], [Esc]*, [Kru]*, [vdW]*.

Bibliographie

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.